REQUEST FOR PROPOSAL (RFP)

For

Request for Proposal for ICCC PROJECT (ICCC, Data Centre, OFC, ITMS etc.)

Under

SMART CITY MISSION (SCM)

in

Bhagalpur, Bihar.

VOL. II OF III

Volume II: Scope of Work

Issued By:
Chief Executive Officer
Bhagalpur Smart City Limited

Disclaimer

Bhagalpur Smart City Proposal has been selected to implement the Area Based Development(ABD) and Pan City proposals by Government of India under Smart City Mission. BSCLhas prepared this Request for Proposal (RFP) for ICCC PROJECT (ICCC, Data Centre, OFC, ITMS etc.) Under SMART CITY MISSION (SCM) in Bhagalpur, Bihar.. The RFP is a detailed document with specifies terms and conditions on which the bidder is expected to work. These terms and conditions are designed keeping in view the overall aims and objectives of the Command and Control Centre. BSCL has taken due care in preparation of information contained herein and believes it to be accurate. However, neither BSCL or any of its authorities or agencies nor any of the irrespective officers, employees, agents, or advisors gives any warranty or make any representations, express, or implied as to the completeness or accuracy of the information contained in this document or any information which may be provided in association with it.

The information provided in this document is to assist the bidder(s) for preparing their proposals. However this information is not intended to be exhaustive, and interested parties are expected to make their own inquiries to supplement information in this document. The information is provided on the basis that it is non–binding on BSCL any of its authorities or agencies, or any of their respective officers, employees, agents, or advisors. Each bidder is advised to consider the RFP as per its understanding and capacity. The bidders are also advised to do appropriate examination, enquiry and scrutiny of all aspects mentioned in the RFP before bidding. Bidders are encouraged to take professional help of experts on financial, legal, technical, taxation, and any other matters/sectors appearing in the document or specified work. The bidders should go through the RFP in details and bring to notice of BSCL any kind of error, misprint, inaccuracyoromission.

BSCL reserves the right not to proceed with the project, to alter the time table reflected in this document, or to change the process or procedure to be applied. It also reserves the right to decline to discuss the Project further with any party submitting a proposal, nor reimbursement of cost of any type will be paid to persons, entities, or consortiums submitting a Proposal.

Sd/-
Chief Executive Officer
Bhagalpur Smart City Limited (BSCL)

Definitions/Acronyms

ACRONYMS	MEANING
ABD	AREA BASED DEVELOPMENT
ACD	AUTOMATIC CALL DISTRIBUTION
AMC	ANNUAL MAINTENANCE CONTRACT
ANI	ASIAN NEWS INTERNATIONAL
ANPR	AUTOMATIC NUMBER PLATE RECOGNITION
API	APPLICATION PROGRAM INTERFACE
AQI	AIR QUALITY INDEX
ARP	ADDRESS RESOLUTION PROTOCOL
ATCS	ADAPTIVE TRAFFIC CONTROL SYSTEM
ATM	AUTOMATED TELLER MACHINE
BMS	BUSINESS MANAGEMENT SYSTEM
BoM	BILL OF MATERIAL
BSCL	BHAGALPUR SMART CITY LIMITED
CCC	CIRCUIT CROSS-CONNECT
CCTV	CLOSED CIRCUIT TELEVISION
CMM	CAPABILITY MATURITY MODEL
COTS	COMMERCIAL OFF-THE-SHELF
CSP	CLOUD SERVICE PROVIDER
CSV	COMMA SEPARATED VALUES
CTI	COMPUTER TELEPHONY INTEGRATION
DAM	Database Access Monitoring
DBMS	DATA BASE MANAGEMENT SYSTEM
DC	DATA CENTRE
DHCP	DYNAMIC HOST CONFIGURATION PROTOCOL
DMS	DOCUMENT MANAGEMENT SYSTEM
DMZ	DEMILITARIZED ZONE
DNIS	DIALED NUMBER IDENTIFICATION SERVICE
DNS	DOMAIN NAME SERVER
DOC	DOCUMENT
DoS	DENIAL OF SERVICE
DR	DISASTER RECOVERY
DRC	DISASTER RECOVERY CENTRE
DTMF	DUAL-TONE MULTI-FREQUENCY SIGNALLING
ECB	EMERGENCY CALL BOX
EMD	EARNEST MONEY DEPOSIT
EMS	ENTERPRISE MANAGEMENT SYSTEM
EPBAX	ELECTRONIC PRIVATE AUTOMATIC BRANCH EXCHANGE
ER	EQUIVALENT RELATIONAL
FAT	FINAL ACCEPTANCE TEST
FCC	FEDERAL COMMUNICATIONS COMMISSION
FMS	FACILITY MANAGEMENT SERVICES
FRS	FUNCTIONAL REQUIREMENTS STATEMENT
FTP	FILE TRANSFER PROTOCOL
FTP/SMTP	FILE TRANSFER PROTOCOL/ SIMPLE MAIL TRANSFER PROTOCOL
GIS	GEOGRAPHICAL INFORMATION SYSTEM

ACRONYMS	MEANING
GoI	GOVERNMENT OF INDIA
GPRS	GENERAL PACKET RADIO SERVICES
GPS	GLOBAL POSITIONING SYSTEM
GSM	GLOBAL SYSTEM FOR MOBILE COMMUNICATION
GST	GOODS AND SERVICES TAX
GUI	GRAPHICAL USER INTERFACE
HD	HIGH DEFINITION
HDD	HARD DISK DRIVE
HFE	HUMAN FACTORS ENGINEERING
HLD	HIGH LEVEL DESIGN
HTTPS	HYPERTEXT TRANSFER PROTOCOL SECURE
ICCC	INTEGRATED COMMAND AND CONTROL CENTRE
ICMP	INTERNET CONTROL MESSAGE PROTOCOL
ICOMC	INPUT CONTROL OUTPUT MECHANISM
ICT	INFORMATION AND COMMUNICATION TECHNOLOGY
IDS	INTRUSION DETECTION SYSTEM
IEC	INTERNATIONAL ELECTROTECHNICAL COMMISSION'S
IEEE	INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS
IETF	INTERNET ENGINEERING TASK FORCE
IGMP	INTERNET GROUP MANAGEMENT PROTOCOL
IMAP	INTERNET MESSAGE ACCESS PROTOCOL
IoT	INTERNET OF THINGS
IP	INTERNET PROTOCOL
IPF	INFORMATION PROCESSING FACILITY
IPS	INTRUSION PREVENTION SYSTEM
ISO	INTERNATIONAL ORGANIZATION FOR STANDARDIZATION
ISP	INTERNET SERVICE PROVIDER
ISWM	INTEGRATED SOLID WASTE MANAGEMENT
IT	INFORMATION TECHNOLOGY
ITDP	INSTITUTE FOR TRANSPORTATION AND DEVELOPMENT POLICY
ITIL	INFORMATION TECHNOLOGY INFRASTRUCTURE LIBRARY
ITMS	INTELLIGENT TRAFFIC MANAGEMENT SYSTEM
IVA	INTELLIGENT VIDEO ANALYTICS
IVRS	INTERACTIVE VOICE RESPONSE SYSTEM
KML	KEYHOLE MARKUP LANGUAGE
KMZ	KEYHOLE MARKUP LANGUAGE ZIPPED
KPI	KEY PERFORMANCE INDICATOR
LAN	LOCAL AREA NETWORK
LDAP	LIGHTWEIGHT DIRECTORY ACCESS PROTOCOL
LoA	LETTER OF ACCEPTANCE
MAC	MEDIA ACCESS CONTROL
MAF	MINIMUM AUDIBLE FIELD
MEITY	MINISTRY OF ELECTRONICS & INFORMATION TECHNOLOGY
MIS	MANAGEMENT INFORMATION SYSTEM
MLPP	MASTER LEASE PURCHASE PROGRAM
MPOS	MOBILE POINT OF SALE

ACRONYMS	MEANING
MSI	MASTER SYSTEM INTEGRATER
NAS	NETWORK ATTACHED STORAGE
NDSAP	NATIONAL DATA SHARING AND ACCESSIBILITY POLICY
NIT	NOTICE INVITING TENDER
NMS	NETWORK MANAGEMENT SYSTEM
NTP	NETWORK TIME PROTOCOL
O&M	OPERATION & MAINTENANCE
OEM	ORIGINAL EQUIPMENT MANUFACTURE
OFC	OPTICAL FIBER CABLE
OGC	OPEN GEOSPATIAL CONSORTIUM
ONVIF	OPEN NETWORK VIDEO INTERFACE FORUM
OS	OPERATING SYSTEM
OWASP	OPEN WEB APPLICATION SECURITY PROJECT
PA	PUBLIC ADDRESS
PDF	PORTABLE DOCUMENT FORMAT
PMO	PROJECT MANAGEMENT OFFICE
PoP	POINT OF PRESENCE
POS	POINT OF SALE
BSCL	BHAGALPUR SMART CITY LIMITED
PTZ	PAN TILT ZOOM
RACI	RESPONSIBLE, ACCOUNTABLE, CONFIRM, INFORM
RAID	REDUNDANT ARRAY OF INDEPENDENT DISKS
RFP	REQUEST FOR PROPOSAL
RLVD	RED LIGHT VIOLATION DETECTION
RTCP	REAL-TIME CONTROL PROTOCOL
RTF	RICH TEXT FORMAT
RTO	REGIONAL TRANSPORT OFFICE
RTSP	REAL TIME STREAMING PROTOCOL
SCADA	SUPERVISORY CONTROL AND DATA ACQUISITION
SCM	SMART CITY MISSION
SCP	SMART CITY PROPOSAL
SDC	STATE DATA CENTRE
SEO	SEARCH ENGINE OPTIMIZATION
SLA	SERVICE LEVEL AGREEMENT
SMF	SEALED MAINTENANCE FREE
SMS	SHORT MESSAGING SERVICE
SNMP	SIMPLE NETWORK MANAGEMENT PROTOCOL
SOP	STANDARD OPERATING PROCEDURES
SPV	SPECIAL PURPOSE VEHICLE
SRS	SYSTEM REQUIREMENT SPECIFICATIONS
SRTP	SECURE REAL-TIME TRANSPORT PROTOCOL
SSH	SECURE SHELL
SSL/TLS	SECURE SOCKETS LAYER/TRANSPORT LAYER SECURITY
SVD	SPEED VIOLATION DETECTION
SWE	SENSOR WEB ENABLEMENT
TARS	TRAFFIC ACCIDENT REPORTING SYSTEM
TCV	TOTAL CONTRACT VALUE

ACRONYMS	MEANING
TDS	TAX DEDUCTED AT SOURCE
TPA	THIRD PARTY AUDITOR
TTS	TEXT TO SPEECH
UAT	USER ACCEPTANCE TESTING
UD & HD	URBAN DEVELOPMENT AND HOUSING DEPARTMENT
UDP	USER DATAGRAM PROTOCOL
UPS	UNINTERRUPTED POWER SUPPLY
UTP	UNSHIELDED TWISTED PAIR
VAT	VALUE ADDED TAX
VLAN	VIRTUAL LOCAL AREA NETWORK
VM	VIRTUAL MACHINE
VMS	VIDEO MANAGEMENT SYSTEM
VMSB	VANCOUVER MASONIC SERVICE BUREAU
VOIP	VOICE OVER INTERNET PROTOCOL
VPN	VIRTUAL PRIVATE NETWORK
VRLA	VALVE REGULATED LEAD ACID
WAN	WIDE AREA NETWORK
XML	EXTENSIBLE MARKUP LANGUAGE

Contents

LIST OF TABLES

LIST OF FIGURES

LIST OF ANNEXURE

Introduction

1.1. Project Objectives

The key objective of this project is to establish a collaborative framework where input from different smart solutions implemented by BSCL, and other stake holders can be assimilated and analyzed on a single platform; consequently, resulting in aggregated city level information. Further this aggregated city level information can be converted to actionable intelligence, which would be propagated to relevant stakeholders and citizens in coordinated and collaborative manner. Following are the key outcomes expected to be achieved by the proposed interventions:

a) Improved visualization of ambient or emergency situation in the city and facilitation of data driven decision making

b) Efficient traffic management

c) Enhanced safety and security

d) Better management ofutilitiesand quantification ofservices

e) Asset Management

f) Disaster Managementand Emergency Response

g) Efficiency improvement in public service delivery

h) Inter-departmental coordination and collaboration for faster execution of services

i) Implementation and Integration with all existing and future services as identified by Bhagalpur Smart City Limited(BSCL) in the city including but not limited to (with provision for future escalability):

i. CCTV Surveillance System
ii. Smart Lighting
iii. Data Centre
iv. Disaster Recovery Centre
v. Integrated Command and Control Centre
vi. ICT Enabled Solid Waste Management
vii. Intelligent Traffic Management System
viii. E-Challan System
ix. Public Bike Sharing
x. Smart Water Supply System
xi. Smart Education
xii. Smart Health Management System
xiii. Intelligent Public Transport Management
xiv. Smart Pole
xv. Smart Energy Management System

1.2. Purpose of this RFP

The purpose of this Tender is for the Bhagalpur Smart City Limited (BSCL) to enter into a contract with a qualified firm for the Supply, Installation, Configuration, Integration, Commissioning, Operations and Maintenance of integrated solutions to support the command, and control centre initiative for smart city initiative of BSCL. BSCL is looking to engage a Master Service Integrator -

a) Who brings strong technology experience in smart city implementation,integration and operations through integrated and multi-agency coordination platform
b) Who can develop Standard Operating Procedures for the various components of the project and link with uses cases prepared by them
c) Who has a quality control plan in place to demonstrate that all equipment is tested and passed prior to shipping
d) Who is capable of providing high quality installations of the project equipment
e) Who is capable of maintaining and operating the complex smart city systems to provide maximum decision making support and performance of the systems
f) Who brings forth expertise for traffic management, incident and emergency management
g) Who has experience implementing city-wide ICT and surveillance system coupled with using the said systems efficiently through data analytics
h) Who will strongly build capacity of various stakeholders for efficient operations and management of the proposed solutions

This tender is designed to provide interested bidders with sufficient basic information to submit proposals meeting minimum requirements, but is not intended to limit a proposal's content or exclude any relevant or essential data. Bidders are at liberty and are encouraged to expand upon the specifications to evidence superior bid understanding and service capability.

2. Project Overview and Components

Key foundation components for BSCL Smart City considered for this RFP are as follows for implementation:

Table 1: Key Foundation Components

S.No.	Component
1.	OFC laying and Network Backbone
2.	Command & Control Centre
3.	Data Centre and DR Site
4.	ITMS
5.	Variable Message System
6.	Public Address System
7.	Emergency Call Box (ECB) System
8.	Smart Parking
9.	Environmental Monitoring System
10.	Enterprise GIS
11.	Web Portal & Mobile App
13.	CCTV Surveillance
12.	Edge based Analytics
13.	Artificial Intelligence
14.	Traffic and Transportation Management

2.1. Components & Services Scope Overview

The selected MSI shall ensure the successful implementation of the proposed ICCC solutions as well as provide capacity building support to city authorities as per the scope of services described below. Any functionality not expressly stated in this document but required to meet the needs of the BSCL to ensure successful operations of the system shall essentially be under the scope of MSI and for that no extra charges shall be admissible.Any requirement beyond the outlinedSOW will be considered after approval of ChangeRequest from BSCL on additional cost.MSI shall implement and deliver the systems and components which are described in this RFP. MSI'sscope ofworkshallincludebutwillnotbelimitedtothefollowing broadareas. Detailsofeach of these broadareas have also been outlinedin Annexures.

2.1.1. Assessment, Scoping and Survey Study

Conduct a detailed assessment, survey, gap analysis, scoping study and evelop a comprehensive project plan, including:

a) Assess existing ICT systems, Network connectivity within the city and the green-field site for the scope items mentioned in this Volume of the RFP
b) Conduct site survey for finalization of detailed technical architecture, gapanalysis, final Bill of Quantities and project implementation plan
c) Conduct site surveys to identify the need forsite preparation activities
d) Obtain site clearance obligations & other relevant permissions with the support of BSCL

2.1.2. Scope of RFP

I. Scope of this RFP includes, Design, Supply, Configuration, Installation, Implementation, Testing and Commissioning of the following primary components:

a) Integrated Command and Control Centre
b) Data Centre within ICCC Building
c) Disaster Recovery Centre (Hosted on cloud data centre of any MEITY empanelled Cloud Service Provider)
d) Smart Parking Management System
e) City Surveillance
f) Intelligent Traffic Management System

i. Adaptive Traffic Control System (ATCS)
ii. Automatic Number Plate Recognition (ANPR) System
iii. Red Light Violation Detection (RLVD) System
iv. Speed Violation Detection (SVD) System
v. Traffic Violation Cameras
vi. Variable Message Sign boards
vii. Public Address (PA) System
viii. Emergency Call Box (ECB) System

g) Environmental Monitoring Sensors
h) City Web Portal & Mobile App
i) Enterprise GIS Portal
j) Video Analytics
k) OFC laying

The detailed requirements of the above would be delineated within the subsequent sections.

II. Integration with existing and proposed ICT systems within BSCL ICT landscape, not limited to:

a) Smart Lighting
b) ICT Enabled Solid Waste Management
c) Intelligent Transportation System
d) e-Challan System
e) Public Bike Sharing
f) Smart Water Supply System
g) Smart Education
h) Smart Health Management System
i) e-Municipality
j) SCADA
k) Smart Road Network
l) e-Buses Live Tracking and Monitoring System
m) e-Toilet Monitoring System
n) ICT component of e-Library System
o) ICT component of Smart Bus Stop System

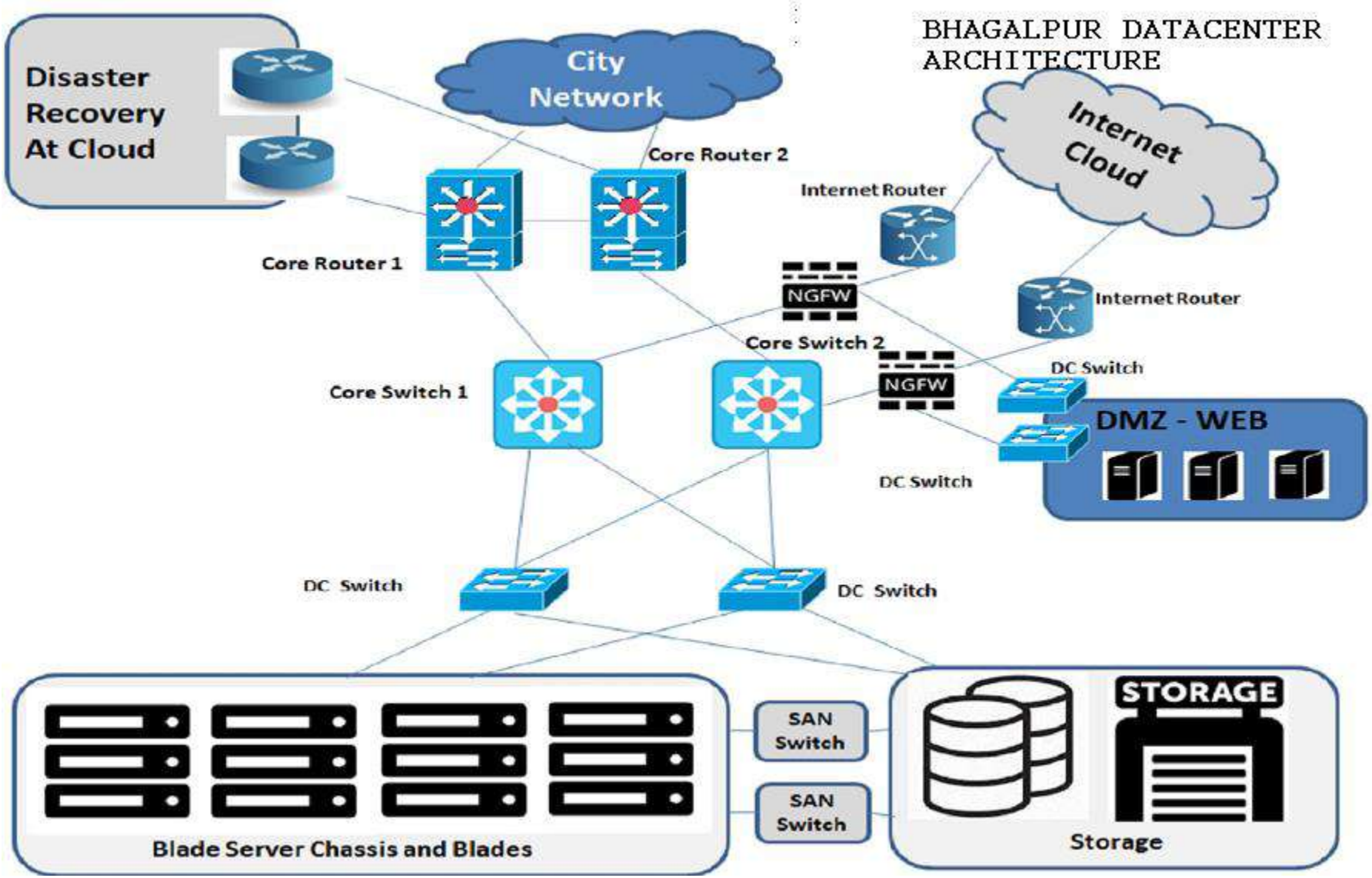
p) ICT component of Smart Parking System

2.1.3. Data Centre

Provisioning of Hardware, Network and Software Infrastructure, which includes design, supply, installation and commissioning of ICT Infrastructure at the Command and Control Centre& Data Centre. This scope consists of:

a) Site preparation services
b) IT Infrastructure including server, storage, other required hardware, application portfolio, licenses
c) Command Centre infrastructure including Video Walls, workstations, IP phones, joystick controller etc.
d) Establishment of LAN and WAN connectivity at Command Centre and DC limited to scope of infrastructure procured for the project
   Application Development and integration services for the applications

Figure 1: Data Center Architecture



2.1.4. Provisioning of City Wide Network backbone

a) Assessment of ISP service provider available in city
b) Connectivity between field device and DC and ICCC
c) Connectivity between DC & proposed DR
d) Internet Connectivity at DC
e) Network shall be sized with sufficient capacity to support redundancy and future traffic growth in order to complete traffic rerouting on the network in the event of failure without affecting overall network performance.
f) A high level Link planning and provisioning parameters like protocol, interfaces, L2 over L3 services between several components like Network, IOT etc should be planned by the MSI

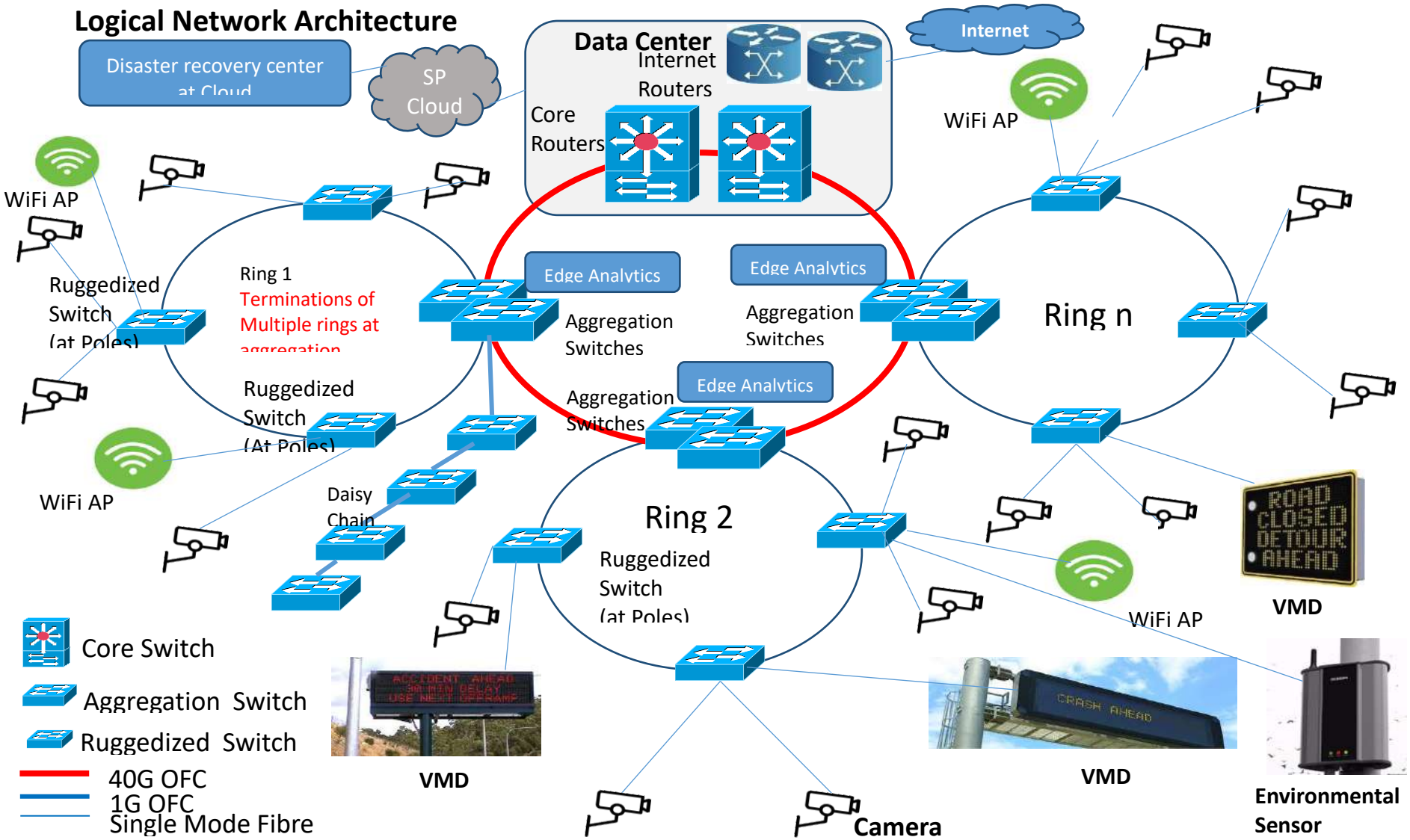


Figure 2: Logical Architecture of BhagalpurCity Wide Network

2.1.5. Capacity Building

Capacity Building for BSCL and any other department which includes preparation of operational manuals, training documents and capacity building support, including:

a) Training of city authorities, operators and other stakeholders 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 revised 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
f) Preparation of system documents, user manuals, performance manuals, Operation manuals,etc.

2.1.6. Operations and Maintenance

MSI shall also be responsible for the maintenance and management of entire systems, solutions, application deployed as part of this RFP for a period of 5 years from the Final Go-Live date of implemented solutions in an efficient and effective manner.

2.2. Component Architecture of ICCC

Indicative architecture of the components envisaged under the "Integrated Command and Control Centre" as well as the Building Blocks are as given in the figuresbelow.This component architecture is indicative in nature and is given in the RFP to bring clarity to prospective bidders on the overall scope of project and its intended use. MSI shall carry out the detail requirement analysis and finalize technical architecture. The architecture layers of the complete network of smart elements is as follows:-

a) Sensor or Field instrument layer

The sensor layer will help the city administration gather information about the ambient city conditions or capture information from the edge level devices like intelligent traffic signals, cameras, enforcement sensors, emergency call boxes, etc. BSCL city is expected to have environmentalIoT sensors installed at multiple locations across the city, to measure & report ambient conditions such as light intensity, temperature, water level (for chronic flood spots), air pollution, noise pollution and humidity for decision makers to take preventive, pro-active and execute responses in case of emergency/natural calamity.

b) Data Collection and Transmitting Layer

Controller processes the input data from the sensor which applies the logic of control and causes an output action to be generated. This signal may be sent directly to the controlled device or to other logical control functions.

The controllers function is to compare its input (from the sensor) with a set of instructions such as set point, throttling range and action, then produce an appropriate output signal. Itusually consists of a control response along with other logical decisions that are unique to the specific control application. After taking the logical decision of the information it will hand over the information to the next layer (Network Layer) which will be subsequently available at the ICCC.

c) Network/Communication Layer

The secured network layer will serve as the backbone for the project and provide connectivity to gather data from sensors and communicate messages to display devices and actuators. It will support the Wi-Fi services and other smart elements (sensors and displays) at given locations wherever applicable. The network layer will be scalable such that additional sensors, actuators, display devices can be seamlessly added.

d) Data Centre Layer

The Data Centre layer will house centralized computing power required to store, process and analyze the data to decipher actionable information. This layer includes HCI infrastructure for running complete virtualized infrastructure and physical servers, storage, ancillary network equipment elements, security devices and corresponding management tools. Similar to the network layer, it will be scalable to cater to the increasing computing and storage needs in future.

e) Security Layer

As ambient conditions, actuators and display devices are now connected through a network, security of the entire system is of paramount significance and MSI will have to provide:

i. Infrastructure Security- including policies for identity and information security policies
ii. 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.
iii. Identity and Access Management – including user authentication, authorization, SSL & Digital Signatures.
iv. Application Security- including hosting of Government Websites and other Cloud based services, adoption of Technical Standards for Interoperability Framework and other standards published by GoI for various e-Governance applications.
v. 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:

i. User/administrator audit log activity (logon, user creation, date-time of PA announcements, voice recording etc.)
ii. Secured data storage (storage of video/image/voice/location/data captured by various smart elements)
iii. SSL/TLS encryption for web and mobile application based interfaces for sensitive data transfer
iv. Protection against Denial of Serviceand Interference attacks to Wi-Fi Devices

f) Smart Application and Integration Layer

The smart applications layer 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. It will be an evolving layer with applications added and integrated as and when new applications are developed at BSCL. 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 underlying architecture components and other data from system developed by the State Government (such as police department, meteorological department, energy department, water department, irrigation department, transport organizations within BSCL, etc.) and non-government agencies.

g) Service delivery and Publishing Layer

The output field devices layer will contain display devices or bi-directional (input & output) devices connected to the network which will be used by citizens to consume - and for administrators to provide - actionable information. Such field devices include digital messaging boards, environmental data displays, etc. The Command Centrepublishes the information which will enable citizens and administrators alike to get a holistic view of city conditions. The implementation vendor will have to develop a Command Centre at the site location identified by BSCL and web/ mobile based viewing tools for understanding the ambient city conditions.

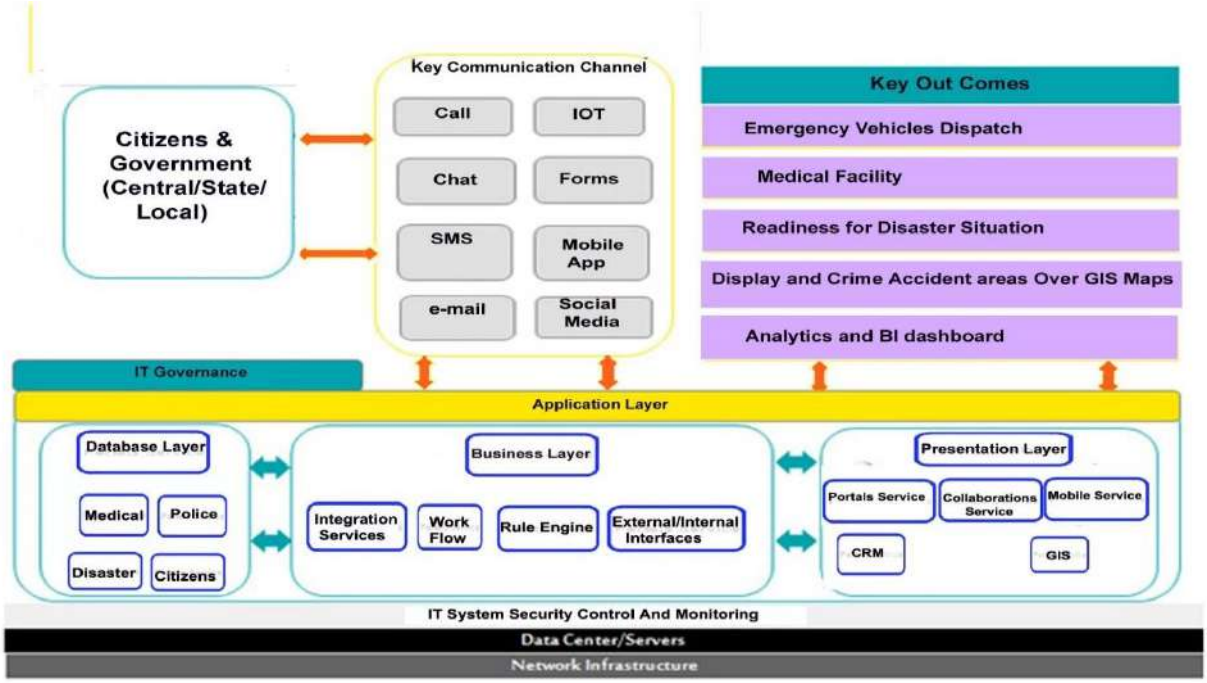


Figure 3: Indicative Architecture of ICCC

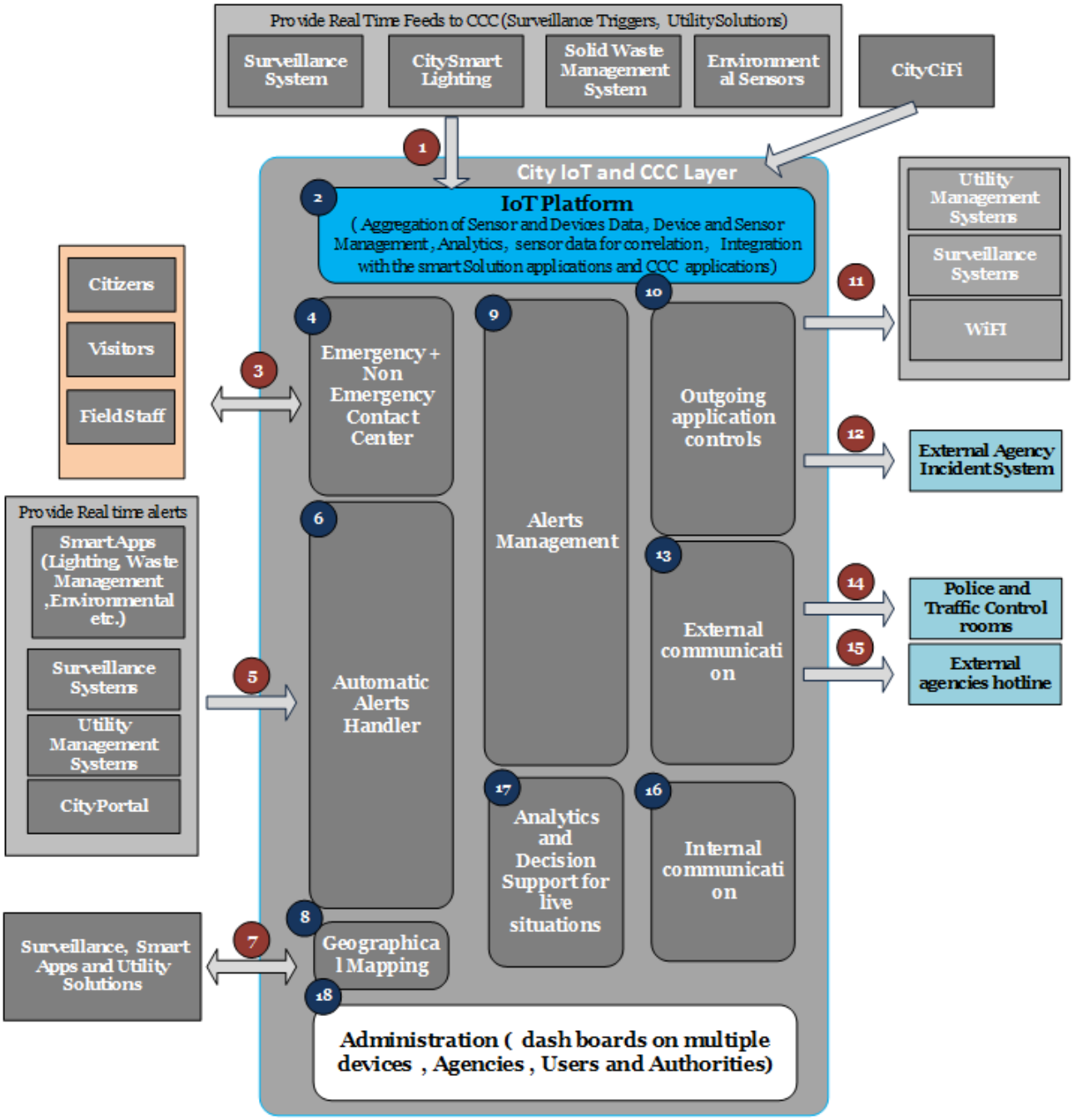


Figure 4:Building blocks of an Integrated Command and Control Center

The proposed functionality of each block, as depicted in the Figure-4, is described below (S.No. mentioned in the table below are mapped to the block numbers mentioned in the diagram):

Table 2: Description of Block Diagram of Proposed Solution.

S. No. (Mapped to ref numbers in the diagram)	Type	Description
1.	Interface	Surveillance, Smart Lighting, Environmental Sensor, Solid waste management and utility management systems will provide real time, at pre-defined frequency and on-demand feeds into the CCC.
2.	IoTFunction	Platform will do the conversion of the different form of data form devices and Sensors to a single format, Perform the device and sensor management, Correlation between different Sensors/ Devices data, Perform rule base and analytics on sensors and devices data. Integration with the Smart Solution application interface, Integration with command and Control centre Visualization and Response layer.
3.	Interface	The contact centre interface will provide citizens and field staff of various agencies with the single point where they will be able to record their grievances / feedback / incidents. This interface will enable citizens to interact with CCC through audio call, SMS, mobile interface and web interface. This will be a two-way interface enabling citizens to pass information to CCC and receive updates from CCC on the actions taken by CCC.
4.	CCC Function	The contact centre function will enable CCC to record and update both day to day incidents such as electricity break down and emergency situations such as accidents. The contact centre will receive the information from citizen and record in the database which will trigger the workflow for resolution of the incident.
5.	Interface	The Interface will enable automatic capture of the following Data: Sensor Data from the various sensor platform including IoT based Gateways deployed as a part of the Smart City Systems The systems deployed throughout the city will be monitoring the various incidents taking place as per the rules defined in the respective systems. The incidents captured automatically by these monitoring systems shall be reported into the CCC via this automated interface

S. No. (Mapped to ref numbers in the diagram)	Type	Description
		This will enable CCC to aggregate and create a centralized repository of all Data & incidents reported throughout the city either manually (as in 3 &4 above) or through this automated interface. The envisaged systems that will be generating these alerts are – a) Utility Management Systems (SCADA) b) Surveillance Systems c) Smart Mobile Apps (Mobile Interface for stakeholders to record incidents if any)
6.	CCC Function	This function within the CCC will enable it to receive the sensor data from IoT Platform and generate alerts or receive the alerts directly from other system, add relevant data to the alerts incident and pass on to next entity as per pre-defined workflow
7.	Interface	Surveillance, Smart and Utility Management Systems would use the geographical functions and geo-spatial data stored in the central GIS application for implementing their functionality that requires GIS layer. The required data and functionality exchange would be done through this system.
8.	CCC Function	This block refers to the centralized GIS layer that would be created at CCC for access by other systems.
9.	CCC Function	The incidents reported manually through contact center as well as automatically received through alerts handler shall be handled by this functional block. Further, it will enable the CCC to carry out complex event processing for data received from Sensor system directly, correlate the data through rule engine for alerts creation and will enable execution of workflow for managing the incident life cycle as per pre-defined business rules and SOPs. This will ensure consistency of response to incidents.
10.	CCC Function	The CCC will control the Surveillance, Smart and Utility Management systems via this interface enabling them to be controlled through a common interface.
11.	Interface	This interface will enable CCC to pass data to be used by various systems e.g. view triggers into various systems such as

S. No. (Mapped to ref numbers in the diagram)	Type	Description
		viewing a specific camera view into CCC, sending SMS through a SMS gateway etc.
12.	Interface	This interface will enable CCC to pass data to intimate the respective agency about incident reported in CCC e.g. creating incident in incident management system of electricity department about power failure
13.	CCC Function	This function will enable CCC to interact with external stakeholders. This block shall use tools such as Video Conferencing, Agency hot-lines etc.
14.	Interface	This interface shall enable transfer of video feeds to traffic and police control rooms
15.	Interface	This interface shall enable audio and video hotlines to agencies and offices in case of emergency situations
16.	CCC Function	The internal communication within CCC shall be managed through video conferencing and IP telephony systems
17.	CCC Function	This block will enable CCC to perform analytics on the data gathered during lifecycle of various incidents thereby enabling it to make informed changes to SoPs and business rules .
18.	CCC Function	This block will enable CCC to define the security access rights, Standard Operating Procedures, Business Rules, and Workflows , Integration with the IoT Platform for Device Provisioning and Management (Sensor System) etc. to enable the CCC to function in the desired manner

Table 3: Description of Solution Component

S. No.	Solution Component	Functional Blocks Catered
1.	CCC application	1, 2, 5, 6, 9, 10, 11, 12, 17, 18
2.	GIS application with high resolution satellite image	7, 8
3.	IoT Platform	2
4.	Video Conferencing System	13, 14, 16
5.	IP Telephony	13, 15, 16
6.	Contact centre system, appliances and work stations	3, 4
7.	Operator appliances and work stations	2
8.	SMS Gateway	13, 16

3. Survey & Design Considerations for Technical Architecture & Project Plan

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

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

b) Approach and methodology to be adopted to implement the Project (which should be in line with what has been proposed during bidding stage, but may have value additions / learning in the interest of the project)

c) Responsibility assignment matrix for all stakeholders

d) Risks that MSI anticipates and the plans they have towards their mitigation

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

f) Installation locations for field devices geo mapped to visually identify the geographical area

MSI shall conduct a comprehensive As-Is study of the existing system and infrastructure. The report shall also include the expected measurable improvements against each KPI in 'As-Is' study after implementation of smart solutions under this project. The benchmarking data should also be developed to track current situation and desired state.

MSI shall study the existing business processes, functionalities, existing systems and applications including MIS reporting requirements.

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

Additionally, MSI should provide a detailed To-Be designs specifying the following:

a) High Level Design (including but not limited to) Application architecture, Logical and physical database design, Data dictionary and data definitions, ER (Entity Relationship) diagramsand other data modeling documents and Physical infrastructure design for devices on the field.

b) Application component design including component deployment views, control flows, etc.

c) 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 Bihar.

d) Location of all field systems and components proposed at the junctions, (KML /KMZ file plotted on map) with GEO coordinates.

e) Height and foundation of Cameras, Traffic Signals and Poles for Pedestrian signals, Height and foundation of Poles, cantilevers, gantry and other mounting structures for other field devices.

f) Location of Junction Boxes.

g) Electrical power provisioning.

MSI shall also identify the customizations/ workaround that would be required for successful implementation and operation of the project. The MSI would be offering the products and solutions which meet the 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 Optimized solution which is technically superior, innovative, proven, better in terms of functionality and is cost effective. Any specified parameters mentioned in the scope/technical requirement in the RFP may be considered, if it is required for meeting current & future requirements during the contract period. The MSI is fully responsible for the specified outcome to be achieved.

The report should take into consideration following guiding principles:

a) **Transformational Nature of Smart City applications**- Applicationsshould look to fully embrace mobile adoption, online authentication, etc. to transform the processes completely and offer wider choice and no/low touch point for residents to interact directly. It is critical that project design isaligned tolarger trends anddesigned for next decade rather than past.

b) **Use of Open Standard for evolving Technology:** The entire system would be built to be open (standards, open API, plug-n-play capabilities like virtual environments, creating sandbox), components coupled loosely to allow changes in sub- system level without affecting other parts, architected to work completely within a heterogeneous compute, storage, and multi-vendor environment. Use of the latest & best available standards to avoid locking in obsolescent technologies simulated services environment can help agencies to save cost, infrastructure and time in testing multiple application integrations. Large integrated systems of Smart City operations should be designed to get the best cost and performance advantages of natural technology curve (constant

increase of speed and decrease ofcost),architecture should be open and vendor neutral, and designed forhorizontal scale. The technology shall scale linearly and shall have the provision to infuse new technologies without any disruption to running environment. It shall be support hardware agnostic and hypervisor agnostic so that we are not bind or dependent on buying a particular hardware of virtualization solution.

c) **Distributed,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.

- **Security and privacy of data** –The security services will cover the user profile management, authentication and authorization aspects of security control. This service run across all the layers since service components from different layers will interact with the security components. All public contents should be made available to all users without authentication. The service will authenticate users and allows access to other features of the envisaged application for which the user is entitled to. The system should be designed to provide the appropriate security levels commensurate with the domain of operation. Also the system will ensure data confidentiality and data integrity. The architecture must adopt an end-to-end security model that protects data and the infrastructure from malicious attacks, theft, natural disasters etc. SI must make provisions for security of field equipment as well as protection of the software system from hackers and other threats. 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 endeavor 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. The authority would carry out the Security Audit of the entire system upon handover and also at regular intervals 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).
- **Security Configuration Baseline Management (SCBM):** Automatically and constantly keep infrastructure secure via automated checks and self-healing. Logs all corrective changes for audit.

Insurance and Security - Field equipment installed through this Project would become an important public asset. During the contract period of the Project the SI shall be required to repair / replace any equipment if it is burnt/stolen/damaged/faulty due to any reason. Appropriate insurance cover from Nationalized Insurance Company must be provided to all the equipment's supplied under this project till end of O&M period. MSI has to provide copy of Insurnace Policy at the time of Go-Live for all equipments. In case of annual policy, MSI has to provide renewed policy before 15 days of expiry of previous policy.

a) 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.

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

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

d) 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.

e) 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.

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

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

h) A secure solution should be provided at the hardware infrastructurelevel, software level, and access level.

i) Authentication, Authorization & Access Control: 3 factors (User ID & Password, Biometric, and DigitalSignature) security mechanisms should be implemented to enable secure login and authorized access to portal information and services.

j) Encryption and Confidentiality of sensitive information and data of users and portal information should be ensured.

k) Appropriate mechanisms, protocols, andalgorithmsnecessary toprotect sensitive andconfirmation data and information both during communication and storage should be implemented.

l) Data security policies and standards to be used as per Government of India guidelines.

m) In order toadequately provide access tosecured information, security needs must be identified and developed at the data level. Database design must consider and incorporate data integrity requirements.

n) Role based access for all the stake holders to be implemented to access and use the system.

o) Ability to adopt other authentication mechanism such as Electronic Signature Certificates.

p) Authorization validity to be ensured for the users providing the Data tothe system. Data should be accepted only from the entity authorized.

q) Audit trails and Audit logging mechanism to be built in the system to ensure that user action can be established and can be investigated andaided (e.g. logging of IP address etc.)

r) Data alterations etc. through unauthorized channel should be prevented.

s) Industry good practice for coding of applicationso as to ensure Sustenance, Application, Vulnerability and Assessment

i. Build a complete audit trail of all activities and operations using log reports, so that errors in system – intentional or otherwise – can be traced and corrected.

ii. Access controls must be provided to ensure that the system is not tampered or modified by the system operators.

iii. The security of the field devices must be ensured with system architecture designed in a way to secure the field devices in terms of physical damage & unauthorized access.

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

v. APIs should be published and the IT systems be running on standard protocols like JSON / XML or REST etc.

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

vii. All IoT sensors deployed as part of Smart cities system should talk only to the authorized wireless network, and do not hook on to the rogue networks. The guidelines to secure Wi-Fi networks as published by Department of Telecom must be followed.

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

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

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

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

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

xiii. All the sensors in the Smart city should be connected to a completely separate network.

xiv. As various sensors use multiple protocols to communicate with the underlying network with varied security capability, the system should allow provisioning necessary authentication and encryption at the gateway or the nearest data

aggregation level if the sensor is not able to do the same.

xv. Secured Information and Event Management system - monitoring of all Smart City networks, devices and sensors to identify malicious traffic.

xvi. Activities such as anti-spoofing (no one should be able to masquerade for inappropriate access), anti-sniffing (no one should be able get data and interpret it), anti-tampering (no one should be able to put/change data which was not meant to be put/changed) should be taken care for data in transit, as well as data at rest, from internal and external threats.

t) **Sustainable & Scalable Solution-** 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 centreequipment's or other smart city components. Main technology components requiring scalability are storage, bandwidth, computing performance (IT Infrastructure).

The architecture should be scalable (cater to increasing load of internal and external users and their transactions) and capable of delivering high performance till the system is operational. In this context, it is required that the application and deployment architecture should provide for Scale-Up and Scale out on the Application and Web Servers, Database Servers and all other solution components. The data centre infrastructure shall be capable of serving at least 1000 concurrent users. The expectation is that the system should sustain at least 10 years from GO-Live. There must not be any system imposed restrictions on the upward scalability in number of field devices.

u) **Availability** - Components of the architecture must provide redundancy and ensure that are no single point of failures in the key project components. Considering the high sensitivity of the system, design should be in such a way as to be resilient to technological sabotage. To take care of remote failure, the systems need to be configured to mask and recover with minimum outage. 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 and offering system High Availability and failover. The solution should meet the minimum of following availability requirements:-

i. Load Balanced across two or more Web Server avoiding single point of failure

ii. Deployment of multiple application instances should be possible

iii. Distributed or load balanced implementation of application to ensure that availability of services is not compromised at any failure instance.

iv. Network, DC and DR should be available as per required respective up time.

v. Comply with the published e-Governance standards, frameworks, policies and guidelines available on http://egovstandards.gov.in (updated from time-to-time)

vi. Provide analytic tools build into the system that shall support automatic detection of anomalies and their quick mitigation.

v) **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 scalability of the system

w) **Interoperability** - Keeping in view the evolving needs of interoperability, especially the possibility that the solution shall become the focal point of delivery of services, and may also involve cross-functionality with the e-Government projects of other departments / businesses in future, the solution should be built on Open Standards. The SI shall ensure that the application developed is easily integrated with the existing applications. The code does not build a dependency on any proprietary software, particularly, through the use of proprietary 'stored procedures' belonging to a specific database product. The standards should:

i. comply with the published e-Governance standards, frameworks, policies and guidelines available on http://egovstandards.gov.in (updated from time-to-time); and

ii. be of leading industry standards and as per standards mentioned at Annexures.

All the personnel working on the Project and having access to the Servers / Data Center should be on direct payroll of the SI/OEM/Consortium partner. The SI 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 Command / viewing centers& Mobile Vans during post-implementation

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

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 city and approved by the Authority before resource mobilisation.

Other Integrations:

a) **Convergence -**BSCL has already initiated many projects which have state of the art infrastructure at field locations deployed under them. The ITMS Infrastructure should be made scalable for future convergence needs. Under the smart city program, BSCL has envisaged to create a state of the art infrastructure and services for the citizens of BSCL, hence it is imperative that all infrastructure created under the project shall be leveraged for maximum utilization. Hence 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 ITMS project at the field locations will be utilized to accommodate field equipment's created under the other projects of BSCL. The procedure for utilization of the infrastructure will be mutually agreed between the BSCL and MSI.

Sub-contracting / Outsourcing shall be allowed only for the work which is mentioned in the relevant clauses of Volume I of this RFP with prior written approval of BSCL. However, even if the work is sub-contracted / outsourced, the sole responsibility of the work shall lie with MSI. 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 toBSCL.

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

c) **SMS Gateway Integration-** SI 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.

d) **Application Architecture**

i. The applications designed and developed for the departments concerned must follow best practice and industry standards. In order to achieve the high level of stability and robustness of the application, the system development life cycle must be carried out using the industry standard best practices and adopting the security constraints for access and control rights. The various modules / application should have a common Exception Manager to handle any kind of exception arising due to internal/ external factors. The standards should (a) at least comply with the published e-Governance standards, frameworks, policies and guidelines available on http://egovstandards.gov.in (updated from time-to-time); and(b) be of leading industry standards and as per standards mentioned at Annexures 23-30.

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

SI shall design and develop the Smart City System as per the Functional and System requirement specifications.

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

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

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

i. Front end web portal in English and local language

ii. 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.

iii. Storage of entered data in local language using UNICODE (version 6.0 or later) encoding standard.

iv. Retrieval & display in local language across all user interfaces, forms and reports with all browsers compliant with Unicode version 6.0 and above.

v. Facility for bilingual printing (English and the local language)

d) 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:

   i. Feature to use the master data for the auto-populating the forms and dropdowns

   ii. 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

   iii. Creation of the "output" of the service, i.e. Certificate, Order etc.

   iv. Automatic reports

      - of compliance to citizen charter on delivery of services
      - delay reports

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.

   i. SI shall ensure using Digital signatures/e-Authentication(Aadhar Based) to authenticate approvals of service requests etc.

f) e-Transaction & SLA Monitoring Tools

   i. The SI should be able to measure and monitor the performance of the deployed infrastructure and all SLAs set out in this RFP. More importantly, it should be possible to monitor in REALTIME, the number of citizens touched through e-Services each day, month and year, through appropriate tools and MIS reports.

   ii. The Infrastructure management and Monitoring System shall be used by SI to monitor the infrastructure (both IT and Non-IT) hosted at the Data center and DR site.

   iii. For monitoring of uptime and performance of IT and non IT infrastructure deployed, the SI shall have to provision for monitoring and measurement tools, licenses, etc. required for this purpose.

g) The Smart City Application should have roadmap to integrate with key initiatives of State namely Portal Services, Citizen Contact Centre, Certifying Authority etc.

h) Complete mobile enablement of the Smart City System.

3.1. Commencement of Works

Site Clearance obligations & other relevant permissions –
Prior to starting the site clearance, MSI shall carry out survey of field locations as specified in RFP, for buildings, structures, fences, trees, existing installations, etc. The BSCL 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 BSCL before executing the plan.

3.2. Existing Traffic Signal System

The unused infrastructure of existing traffic signal systems including the aspects, controllers etc. will be dismantled and replaced with the new systems where required, which are proposed and required under the scope of the ITMS. The dismantled infrastructure shall be delivered at the BSCL designated location without damage at no extra cost.

3.3. Road Signs

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

3.4. Electrical Works and Power Supply

MSI shall directly interact with electricity board for provision of mains power supply at all desired locations for ITMS field solution. MSI shall be responsible to submit the electricity bill including connection charge, meter charge, recurring charges etc. to the electricity board directly. MSI shall have to submit the challan of bill submission to BSCL. BSCL will reimburse the amount submitted to MSI after verification in next billing cycle.

3.5. Lightning-Proof Measures

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

Earthing System

All electrical components are to be earthed 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 earthed through the cable glands. The entire applicable IT infrastructure i.e. signal junction or command centre shall have adequate earthing. Further, earthling should be done as per Local/State/National standard in relevance with IS standard.

a) 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. BSCL shall provide the necessary space required to prepare the earthing pits.

b) All metallic objects on the premises that are likely to be energized by electric currents should be effectively grounded.
c) 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.
d) The earth connections shall be properly made.
e) 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.
f) Provide separate Earthing pits for Servers, & UPS as per the standards.
g) The metallic housing of electronic equipment/junction box/panel shall be connected to the earthing system.
h) The active electronic parts of an electronic equipment system shall be connected to the earthingsystem.

3.6. Junction Box, Poles and Cantilever

h) MSI shall provide the Junction Boxes, Posts and Cantilever to mount the field sensors, cameras, traffic sensors, traffic light aspects, active network components, controller and power backup (UPS/Alternate energy sources) at all field locations, as per the specifications given in the RFP.
i) Junction Box needs to be appropriately sized in-order to accommodate the systems envisaged at the Junctions, and MSI should design the Junction box for 1.5 times the actual size required for utilization under the ITMS project.
j) Additional 50% space in the Junction Box shall be utilized by BSCL to accommodate any future requirements under other projects.
k) Junction Box for UPS with Battery bank needs to be considered separately. Bidder may propose solar based solutions to power the equipment. In this case, raw power can be used as backup supply whenever solar power is not able to meet the requirement.
l) It should be noted that MSI would have designed the Junction box keeping in mind the scalability requirements of ITMS project, and the additional 50% volume needs to considered over and above such requirement.
m) 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.

3.7. Cabling Infrastructure

a) MSI shall provide standardized cabling for all devices and subsystems.
b) 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.
c) 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.
d) Cabling must be carried out per relevant BIS standards. All cabling shall be documented in a cable plan by MSI.

3.8. Integrated Command& Control Centre (ICCC)

a) The vision of the Command and Control (ICCC) is to have an integrated view of all the smart initiatives undertaken by BSCL with the focus to serve as a decision support engine for city administrators in day-to-day operations or during exigency situations. ICCC involves leveraging on the information provided by various departments and providing a comprehensive response mechanism for the day-to-day challenges across the city. ICCC shall be a fully integrated solution that provides seamless traffic management, incident – response management, collaboration and geo-spatial display. This platform is expected to integrate various urban services devices at the street layer so that urban services applications can be developed on top of this platform independent of the technology that is used in the devices. The platform should be able to integrate with any type of sensor platform being used for the urban services irrespective of the technology used.

b) The platform should be able to normalize the data coming from different devices of same type (i.e. lighting sensors from different OEMs, energy meters from different OEMs etc.) and provide secure access to that data using data API(s) to application developers.

c) ICCC shall facilitate the viewing and controlling mechanism for the selected field locations in a fully automated environment for optimized monitoring, regulation and enforcement of services. The smart city operations center shall be accessible by operators and concerned authorized entities with necessary authentication credentials. Various smart elements are able to use the data and intelligence gathered from operations of other elements so that civic services are delivered lot more efficiently and in an informed fashion. ICCC should be able to integrate with various Utility systems such as Water/SCADA, Power, Gas, ITMS, Parking, Sewerage/ Drainage system, Disaster Mgmt. System etc.

d) MSI has to integrate all smart components of the project at Command and Control Centre with an integrated operations and dashboard application that will integrate various Smart City components implemented in this project and in future.

e) As part of this RFP, MSI shall ensure that redundancy and fault tolerance is considered at the ICCC components level in the actual deployment.

f) High Availability / Up Time Targets for ICCC operations are identified as follows:
   i. Availability Target (24Hr operation): 99.741%
   ii. Maximum Downtime Tolerated per Day: 6 minutes
   iii. Maximum Downtime Tolerated per Week: 42 minutes

3.9. Integrated City Operation Platform

3.9.1. Urban Services and Data APIs

a) **Live data** and **visual feed** from diverse sensors should be connected to the platform

b) **Normalized APIs:** for listed domain (Parking, Outdoor Lighting, Traffic, Environment, Urban mobility etc.) to monitor, control sensor and/or actuators functionality

   For example, Lighting APIs: Vendor agnostic APIs to control Lighting functionality

c) **Cross APIs Integration:** Enabling contextual information (API-API Bi-directional) and correlation across domains and verticals (Multiple vendor and Multi-sensor in future)

3.9.2. Platform Functionality

a) **API management and gateway:** Provides secure API lifecycle, monitoring mechanism for available APIs
b) **User and subscription management:** Provides different tier of user categorization, authentication, authorization, and services based on the subscriptions
c) **Application management:** Provides role-based access view to applications
d) **Enabling analytics:** Time shifted and real-time data available for big data and analytics
e) **Domain and/or Insight reports**- Parking occupancy, energy reports, AQI report (environmental pollution)

3.9.3. Video Analytics at Edge of the City

While Intelligent Video Analytics (IVA) is great at extracting key information, in many safety, security, or failure prevention scenarios, the speed of reaction is equally critical to effectively address the situation. For example, the response to a major multivehicle accident at rush hour may involve rapidly dispatching police, ambulances and fire trucks, changing road signs to reroute traffic away from the area, and automatically archiving the pre-roll and post-roll footage as police evidence.

Sending every bit of video data from the thousands of cameras at edge back to a traditional data center or cloud for processing is often:

a) Too slow leading to a high latency of reaction
b) Too expensive due to the high bandwidth needed for all the video feeds
c) At a high risk of corruption or snooping when sent over a public network

Artificial Intelligence (AI) enabled Surveillance brings below distinct advantages, all at the same time.

a)Enables super-human levels of understanding and accuracy.
b) Edge based AI Analytics saves transmission bandwidth & storage costs, is easy for installation hence saves deployment costs.

Continuous learning to stay updated with city's changing video feeds and delivering unprecedented accuracy levels.However, Video analytics at edge as well as server is jointly required for the quick and efficient city operations as the edge analytics alone cannot provide reference with historic video data processed and stored at the server. The advanced analytics system should be supported by continuous learning abilities. MSI should be able to implement the analytics on edge / server (in selected cases) as per city requirement and increase accuracy

of analytics every 4 months via continuous learning. This will personalize analytics for Bhagalpur Smart City and mandate the feature of continuous learning for city's betterment.

The MSI is expected to propose edge / hybrid/server based analytics solution based on the use cases. The bidder must provide as many use cases as possible from the camera and native VMS to ensure seamless and easy functioning but is free to offer third party products and solutions that meet the requirements of the RFP focussing on the outcome, future scalability, security, reliability and adherence to SLAs and best practices in the industry.

3.10. GIS Mapping

GIS city map which shall be a common platform across all the solutions including City Wi-Fi, City Surveillance, Smart Lighting, solid waste management, Environmental sensor etc. across City/ Region of Interest. The GIS solutions shall also be responsible for appropriate geo referencing & geo tagging on the map covering all relevant assets like Surveillance Camera , Wi-Fi Hotspots, bin locations, street poles, Environmental sensor , Lighting etc.

GIS Maps Features

a) GIS maps shall be comprehensive and detailed up to Complete Road Network, Building Foot Prints and Land use level. Solution shall ensure that the GIS Map provides complete Spatial and Attribute Information Pertaining to All the features of the city as various digital vector layers and allows for zoom in/out, searching, and retrieving information capabilities.

b) GIS system of City would provide the following details include the following data with attributes:

i. Road Network
   - City Arterial Roads
   - Streets

ii. Administrative boundaries
   - District and Sub District Boundary
   - Town and Ward Boundaries

iii. Building footprints and names

iv. Points of Interest data to include:

   - Health services (Hospitals, Blood Banks, and Diagnostics center, Ambulance Services, Other Medical Services, etc.)
   - Community services (fire stations, police stations, banks, ATMs, post offices, educational facilities, Govt. Buildings etc.)
   - Business Centres (Shopping malls, markets, commercial complexes etc.
   - Transportation (bus stops/Terminus, parking areas, petrol bunks, metro stations, seaports, airports,Railway Stations etc.)
   - Recreation facilities (Restaurants, theatres, auditoriums etc.)
   - Other utilities such as travel and tourism facilities, religious places,burial grounds, solid waste locations etc.
   - Local landmarks with locally called names.

v. Land-Cover
   - Green areas
   - Open Areas
   - Water bodies

- Built up Areas

vi. Address layers (Pin code, Locality, Sub-locality, House numbers/names)

vii. Geo referencing of all the assets pertaining to the aforementioned solutions as required shall be provided by the SI

viii. All data procured shall be imported into a central database.

ix. System Functionalities:

- The system shall have capability to perform attribute or spatial queries on data from selected sources.
- The system shall support Android, IOS and Windows Mobile platform,
- The system shall support clipping and/or downloading of raster and vector data by authorised users.
- The system shall support server side Geo-processing
- The application shall have standard and modern map navigation tools of pan and zoom.

x. The application shall support client requests to print the spatial data. The system shall be able to support industry-standard data types, Industry-standard data formats, unlimited file size or database size, unlimited number of files or tables, and unlimited number of users.

- The system shall support geocoding and reverse geocoding
- The system shall allow the users to perform advanced spatial analysis like geocoding, routing, buffering and attribute based analysis.
- The System shall have optimal route planning and real time ETA leading to greater per vehicle productivity
- The application shall have standard and modern map navigation Tools
- The system shall have the facility wherein the user can opt to view in 2D or 3D environment.
- The system shall be compatible with Google Maps, Bing™ Maps, ESRI Geodatabase, Micro Station, AutoCAD, MGE, FRAMME, G/Technology, ODBC source.
- GIS system should support designs creation for network expansions, Integration with SCADA, ERP systems, billing system, Metering system (smart meters), 3rd party Network Management systems for specific spatial analysis.
- The System shall support hierarchical legends, and watermarks.
- The application shall allow users to views the data with different symbology styles like differentiating feature records based on attributes or types, dynamic label generation with conflict detection, and translucency of all raster data and area color fill.
- The system shall allow the user to find Address/Location
- The system shall be able to consume real-time enterprise published spatial data. It shall be able to consume the third-party published OGC web-services.

xi. Application shall be OGC compliant for database and shall provision conversion to other database formats.

xii. GIS base maps shall be installed on work stations at Command control Centreand City Command and Control Center. GIS maps and data replication shall happen from central system remotely.

xiii. Provide GIS engine that shall allow operators to get an overview of the entire system and access to all the system components dynamically. GIS engine shall enable dynamic view of the location and status of resources and objects/sensors. System shall enable authorized user to open a new incident and to associate the incident with its geographic location automatically, via GIS display.

4. Other Expectation and Consideration from MSI

4.1. Expectations from MSI/SI

a) SI shall engage early in active consultations with the Authority, City Police and other key stakeholders to establish a clear and comprehensive project plan in line with the priorities of all project stakeholders and the project objectives.

b) Study the existing fiber duct (if any) layout in the city and existing network to understand the existing technology adopted in each of the following areas (not limited to):

i. Surveillance Infrastructure – CCTV Cameras, Data communication, monitoring, control room and Infrastructure

ii. Other Smart City initiatives envisaged

c) SI shall assess existing infrastructure's current ability to support the entire solution and integrate the same with the proposed solution wherever applicable and possible.

d) SI shall judiciously evaluate the resources and time planned for undertaking the current state assessment, given the overall timelines and milestones of the project.

e) SI shall be responsible for supply of all the Products/equipment such as optical fiber cable, Network, Hardware, Software, Devices, etc. as indicated (but not limited to) in the tentative Bill of Materials included in the RFP and their appropriate quantity & capacity.

f) SI shall be responsible for supply of passive components indicated in the Bill of Materials section of the RFP viz. Housings, Fiber Patch Cords, Racks etc. Civil work required for the site shall be undertaken by the SI.

g) Validate / Assess the re-use of the existing infrastructure if any within Authority site.

h) Supply, Installation, and Commissioning of entire solution at all the locations.

i) SI has to provide Enterprise version for all Open source software. No community version will be accepted.

j) SI shall provide the bandwidth required for operationalizing each smart city initiative till the time Authority's own fiber is laid by the SI as part of the scope of work of this RFP. The bandwidth requirement shall be analyzed and procured by the SI at its own cost / risk.

k) SI shall Install and commission connectivity across all designated locations.

l) SI shall establish high availability, reliability and redundancy of the network elements to meet the Service Level requirements.

m) SI shall be responsible for planning and design of the access network architecture (access controllers, backhaul connectivity, routers, switches, etc.) to meet the technical, capacity and service requirements for all smart city initiatives.

n) SI shall be responsible for up-gradation, enhancement and provisioning additional supplies of network (including active / passive components), hardware, software, etc. as requisitioned by Authority.

o) SI shall ensure that the infrastructure provided under the project shall not have an end of life within 24 months from the date of bidding.

p) SI shall ensure that the end of support is not reached during the concurrency of the contract and 5 years thereafter.

q) SI shall ensure compliance to all mandatory government regulations as amended from time to time.

r) The SI shall ensure that all the peripherals, accessories, sub-components required for the functionality and completeness of the solution, including but not limited to devices, equipment, accessories, patch cords (fiber), cables, software, licenses, tools, etc. are provided according to the requirements of the solution.

s) Authority shall not be responsible if the SI has not provisioned some components, sub-components, assemblies, sub-assemblies as part of Bill of Materials in the RFP. The SI shall have to provision these & other similar things to meet the solution requirements at no additional cost and time implications to Authority.

t) All the software licenses that the SI proposes shall be perpetual software licenses along with maintenance, upgrades and updates for the currency of the contract. The software licenses shall not be restricted based on location and Authority shall have the flexibility to use the software licenses for other requirements if required.

u) The SI shall ensure there is a 24x7 comprehensive onsite support for duration of the contract for respective components to meet SLA requirement. The SI shall ensure that all the OEMs have an understanding of the service levels required by Authority. SI is required to provide the necessary MAF (Manufacturer Authorization Form) as per the format provided in the RFP in support of OEMs active support in the project.

v) Considering the criticality of the infrastructure, SI is expected to design the solution considering the RFP requirement of no single point of failure with high level of redundancy and resilience to meet the network uptime requirements.

w) SI shall be responsible for periodic updates & upgrades of all equipment, cabling and connectivity provided at all locations during the contract period.

x) Although,BSCL will facilitate to provide all Government approvals like, for Pollution Clearance, Fire Audit & Clearance, Right of Way, etc., but MSI has to bear the cost/fees for the same (if any)

y) SI shall be responsible for setting up / building / renovating the necessary physical infrastructure including provisioning for network, power, rack, etc. at all the locations.

z) SI is expected to provide following services, including but not limited to:

   i. Provisioning hardware and network components of the solution, in line with the

proposed authority's requirements.

ii. Size and propose for network devices (like Router, switches, security equipment including firewalls, IPS / IDS, routers, etc. as per the location requirements with the required components/modules, considering redundancy and load balancing in line with RFP.

iii. Size and provision the WAN bandwidth requirements across all locations considering the application performance, data transfer, DR and other requirements for smart city initiatives.

iv. Size and provision the internet connectivity for Service Provider network and Network Backbone.

v. Size and provision for bandwidth as a service for operations of CCTV surveillance till operationalization of network backbone.

vi. Liaise with service providers for commissioning and maintenance of the links.

vii. Furnish a schedule of delivery of all IT/Non-IT Infrastructure items.

viii. All equipment proposed as part of this RFP shall be rack mountable.

ix. Authority may at its sole discretion evaluate the hardware sizing document proposed by the SI. SI needs to provide necessary explanation for sizing to the Authority.

x. Complete hardware sizing for the complete scope with provision for upgrade.

xi. Specifying the number and configuration of the racks (size, power, etc.) that shall be required at all the locations.

xii. The SI shall provide for all required features like support for multiple routing protocols, congestion management mechanisms and Quality of Service support.

xiii. SI shall ensure that all networking active equipment (components) are Simple Network Management Protocol (SNMP) V3 compliant and are available for maintenance/management through SNMP from the date of installation by a Network Monitoring System.

4.2. Inception Phase

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

a) Define an organized set of activities for the project and identify the interdependence between them
b) 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 BSCL office or off site at MSI premises
c) Establish and measure resource assignments and responsibilities
d) Highlight the milestones and associated risks
e) Communicate the project plan to stakeholders with meaningful reports
f) Measure project deadlines and performance objectives
g) Project Progress Reporting. During the implementation of the project, MSI should present weekly reports. This report will be presented in the Steering Committee meeting to BSCL. The report should contain at the minimum the under mentioned:

i. Results accomplished during the period (weekly)
ii. Cumulative deviations from the schedule date as specified in the finalized Project Plan
iii. Corrective actions to be taken to return to planned schedule of progress
iv. Plan for the next week
v. Proposed revision to planned schedule provided such revision is necessitated by reasons beyond the control of MSI
vi. Support needed
vii. Highlights/lowlights
viii. Issues/Concerns
ix. Risks/Show stoppers along with mitigation

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

4.3. Requirement Phase

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 BSCL and its representatives. While doing so, MSI at least is expected to do following:

a. MSI shall conduct a detailed survey and prepare a gap analysis report, detailed survey report of the physical and field infrastructure requirements. MSI shall duly assist the department in preparing an action plan to address the gaps.

b. MSI shall study and revalidate the requirements given in the RFP with BSCL and submit as an exhaustive FRS document. MSI shall develop the FRS and SRS documents.

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

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

e. MSI must get the sign off from user groups formed by BSCL.

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

g. Prior to starting the site clearance, MSI shall carry out survey of field locations for buildings, structures, fences, trees, existing installations, etc.

h. 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 such as poles, cantilevers, cabling, aspects etc. should be reused to derive economies for the project with prior approval of BSCL. The dismantled infrastructure shall be delivered at the BSCL designated location without damage at no extra cost.

i. 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 BSCL

guidelines. Road signs, street name plate, etc. damaged by MSI during their operation shall be repaired or replaced by MSI at no additional cost.

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

4.4. Design Phase

MSI shall make a detailed Design document for proposed the solution as per the Design Considerations detailed in Section – 5,6,7,8 and all Annexures. Separate design for ICCC should be made based on both layouts as provided at Annexure – 2 & 3.

4.5. Development Phase

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, 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): Following needs to be adhered for the proposed software products:
   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. 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. MSI shall report any exceptions to license terms and conditions at the right time to BSCL. However, the responsibility of license compliance solely lies with MSI. Any financial penalty imposed on BSCL during the contract period due to license non-compliance shall be borne by MSI.
   iv. As per requirement of complex solution implementation MSI has to ensure that OEM owned/certified resources& MSI best technical resources are deployed in this project.
   v. The OEM should provide the specific design (OEM Low Level Design, Core Implementation) support expertise to make sure that their supplied technology & products work as per the design objectives.
   vi. OEM to design and implement the complete security policy and workflow as per industry best practice in consultation with Customer to meet their Business requirements.
   vii. MSI should provide the overall program management and OEM to ensure that the solution which may include multiple technologies from various OEM, to work together seamlessly as per the design goals. The seamless integration with all devices would be SIs responsibility for the respective products offered.
   viii. MSI shall also supply any other tools & accessories required to make the integrated solution complete as per requirements. For the integrated solution, MSI shall supply:

b) Software & licenses.
c) Supply tools, accessories, documentation and provide a list of the same. Tools and accessories shall be part of the solution.
d) 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 BSCL regularly :
    i. Functional Requirement Specification (FRS)
    ii. High level design of whole system
    iii. Low Level design for whole system / Module design level
    iv. System Requirements Specifications (SRS)
    v. Any other explanatory notes about system
    vi. Traceability matrix
    vii. RACI Matrix
    viii. Technical and product related manuals
    ix. Installation guides
    x. User manuals
    xi. System administrator manuals
    xii. Toolkit guides and troubleshooting guides
    xiii. Other documents as prescribed by BSCL
    xiv. Quality assurance procedures
    xv. Change management histories
    xvi. Version control data
    xvii. SOPs, procedures, policies, processes, etc. developed for BSCL
    xviii. Programs
        - Entire source codes as applicable
        - 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 and updated during entire project duration. The entire documentation will be the property of BSCL.)

4.6. Integration Phase

The Command and control Centre should be integrated with feeds of all tracks/component deployed under this BSCL Project. 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 to enable city for better decision management and planning.

4.7. Pilot Deployment

a) MSI shall conduct Pilot deployment and testing for meeting BSCL's business requirements before rolling out the complete system. The pilot will be run for four weeks to study any issues arising out of the implementation. MSI shall also review health, usage and performance of the system till it is stabilized during pilot deployment. Based on BSCL'sfeedback for incorporating changes as required and appropriate, MSI shall train staff involved in the Pilot implementation.
b) Pilot shall be demonstrated to the BSCL's representatives. If for any reason the Pilot is found to be incomplete, these will be communicated to the MSI in writing on the lapses that need to be made good. A one-time extension will be provided to the MSI for making goodon the lapses pointed out before offering the system to Client for review. Failure to successfully demonstrate the Pilot may lead to termination of the contract with no liability to Client.

4.8. Go-Live Preparedness and Go-Live

a) MSI shall prepare and agree with BSCL, the detailed plan for Go-Live (in-line with BSCL's implementation plan as mentioned in RFP).
b) MSI shall define and agree with BSCL, the criteria for Go-Live.
c) 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 BSCL team on the same.
f) Go-live of the application shall be done as per the finalized and agreed upon Go-Live plan.

4.9. Handholding and Training

In order to strengthen the staff, structured capacity building programmes shall be undertaken for identified resources of BSCL, UD&HD and stakeholder departments. It is important to understand the training needs to be provided to each and every staff personnel of ICCC. These officers shall be handling emergency situations with very minimal turnaround time. The actual number of trainees will be provided at design stage.

a) MSI shall prepare and submit detailed Training Plan and Training Manuals to BSCL for review and approval.
b) Appropriate training shall be carried out as per the User Training Plan prepared in detail stating the number of training sessions to be held per batch of trainees, course work for the training program, coursework delivery methodologies and evaluation methodologies in detail.
c) MSI shall also be responsible for full capacity building. Training and capacity building shall be provided for all individual modules along with their respective integrations.
d) MSI shall be responsible for necessary demonstration environment setup including setup of cameras, sensors and application solutions to conduct end user training. End user training shall include all the equipment including but not limited to all the applications and infrastructure at ICCC, DC, field locations etc. End user training shall be conducted at a centralized location or any other location as identified by BSCL with inputs from the MSI.
e) MSI shall conduct end user training and ensure that the training module holistically

covers all the details around hardware and system applications expected to be used on a daily basis to run the system.

f) MSI shall impart operational and technical training to internal users on solutions being implemented to allow them to effectively and efficiently use the ICCC system.
g) MSI shall prepare the solution specific training manuals and submit the same to BSCL for review and approval. Training Manuals, operation procedures, visual help-kit etc. shall be provided in Hindi & English language.
h) MSI shall provide training to selected officers of the purchaser covering functional, technical aspects, usage and implementation of the products and solutions.
i) MSI shall ensure that all concerned personnel receive regular training sessions, from time to time, as and when required. Refresher training sessions shall be conducted on a regular basis.
j) An annual training calendar shall be clearly chalked out and shared with the BSCL along with complete details of content of training, target audience for each year etc.
k) MSI shall update training manuals, procedures, manuals, deployment/installation guidelines etc. on a regular basis (Quarterly/ Biannual) to reflect the latest changes to the solutions implemented and new developments.
l) MSI shall ensure that training is a continuous process for the users. Basic intermediate and advanced application usage modules shall be identified by the MSI.
m) Systematic training shall be imparted to the designated trainees that shall help them to understand the concept of solution, the day-to-day operations of overall solution and maintenance and updating of the system to some extent. This shall be done under complete guidance of the trainers provided by the MSI.
n) Time Schedule and detailed program shall be prepared in consultation with BSCL and respective authorized entity. In addition to the above, while designing the training courses and manuals, MSI shall take care to impart training on the key system components that are best suited for enabling the personnel to start working on the system in the shortest possible time.
o) MSI is required to deploy a Master Trainer who shall be responsible for planning, designing and conducting continuous training sessions.
p) The master trainer shall demonstrate a thorough knowledge of the material covered in the courses, familiarity with the training materials used in the courses, and the ability to effectively lead the staff in a classroom setting. If at any stage of training, the BSCL feels that on-field sessions are required, the same shall be conducted by the MSI.
q) If any trainer is considered unsuitable by BSCL, either before or during the training, MSI shall provide a suitable replacement without disrupting the training plan.
r) Training sessions and workshops shall comprise of presentations, demonstrations and hands-on mandatorily for the application modules.
s) BSCL shall be responsible for identifying and nominating users for the training. However, SI shall be responsible for facilitating and coordinating this entire process.
t) MSI has to ensure that training sessions are effective and the attendees shall be able to carry on with their work efficiently. For this purpose, it is necessary that effectiveness of the training session is measured through a comprehensive feedback mechanism. MSI shall be responsible for making the feedback available for the BSCL/authorized entity to review and track the progress, In case, after feedback, more than 40% of the respondents suggest that the training provided to them was unsatisfactory or less than satisfactory then the SI shall re-conduct the same training at no extra cost.

Types of Trainings:

Following training needs is identified for all the project stakeholders:

a) Functional Training

i. Basic IT skills
ii. Web portal, Mobile App, Enterprise GIS, ITMS, Smart Parking, environmental sensors, Data Analytics, ANPR, Smart Solutions etc.
iii. Software Applications (Command and Control Centre)
iv. Networking, Hardware Installation
v. Centralized Helpdesk
vi. Feed monitoring

b) Administrative Training

i. System Administration Helpdesk, BMS Administration etc.
ii. Master trainer assistance and handling helpdesk requests etc.

c) Senior Management Training

i. Usage of all the proposed systems for monitoring, tracking and reporting,
ii. MIS reports, accessing various exception reports

d) Post-Implementation Training

i. Refresher Trainings for senior officials
ii. Functional/Operational training and IT basics for new operators
iii. Refresher courses on System Administration
iv. ChangeManagementprograms

4.10. Operations and Maintenance

MSI will operate and maintain all the components of the ICCC System for a period of five (5) years after Final Go-Live date. During O&M phase, MSI shall ensure that service levels are monitored on continuous basis; service levels are met and are reported to BSCL. After Go-Live, if any system/sub-system/appliance that is deployed during the O&M phase must be added in the System only after proper induction procedures are followed including hardening and security testing. MSI needs to implement suitable Performance Improvement Process (PIP) in the project.

PIP program applies to all the processes of ICCC project. MSI need to submit its detailed approach for PIP in its technical proposal. Every process and procedure implemented in this project must be reviewed and updated by MSI at least on annual basis from the Go-Live Date. All the manpower engaged for O&M support of the project should be citizens ofIndia.MSI will ensure that at no time shall any data of ICCC System be ported outside the geographical limits of the country. Some broad details of O&M activities are mentioned at later sections.

4.10.1. Applications Support and Maintenance

Application support includes, but not limited to, production monitoring, troubleshooting and addressing the functionality, availability and performance issues, implementing the system change requests etc. The MSI shall keep the application software in good working order; perform changes and upgrades to applications as requested by the BSCLteam. All tickets related to anyissue/complaint/observation about the system shall be maintained in an ITIL compliant comprehensive ticketing solution. Key activities to be performed by MSI in the application support phase are as follows:

a) Compliance to SLA

MSI shall ensure compliance to SLAs as indicated in this RFP and any upgrades/major changes to the software shall be accordingly planned by MSI ensuring the SLA requirements are met at no additional cost to the BSCL.

b) Annual Technology Support

MSI shall be responsible for arranging for annual technology support for the OEMproducts to BSCLprovided by respective OEMs during the entire O&M phase.

c) Application Software Maintenance

i. MSI shall provide unlimited support through onsite team/telephone/Fax/E-mail/VideoConferencing/installation visit as required
ii. MSI shall address all the errors/bugs/gaps in the functionality in the solution implemented by the MSI (vis-à-vis the FRS, BRS and SRS signed off) at no additional cost during the O&M phase.
iii. All patches and upgrades from OEMs shall be implemented by the MSI ensuring customization done in the solution as per the BSCL's requirements are applied. Technical upgrade of the installation to the new version, as and when required, shall be done by the MSI. Any version upgrade of the software / tool / appliance by MSI to be done after taking prior approval of BSCL and after submitting impact assessment of such upgrade.
iv. Any changes/upgrades to the software performed during the support phase shall subject to the comprehensive and integrated testing by the MSI to ensure that the changes implemented in the system meets the specified requirements and doesn't impact any other function of the system. Release management for application software will also requireBSCL's approval. A detailed process in this regard will be finalized by MSI in consultation with BSCL.
v. Issue log for the errors and bugs identified in the solution and any change done in the solution shall be maintained by the MSI and periodically submitted to the BSCL.

vi. MSI, at least on a monthly basis, will inform BSCLabout any new updates/upgrades available for all software components of the solution along with a detailed action report.

vii. In case of critical security patches/alerts, the MSI shall inform about the same immediately along with his recommendations. The report shall contain MSI'srecommendations on update/upgrade, benefits, impact analysis etc. The MSI shall need to execute updates/upgrades though formal change management process and update all documentations and Knowledge databases etc. For updates and upgrades, MSI will carry it out free of cost by following defined process.

d) Problem identification and Resolution

i. Errors and bugs that persist for a long time, impact a wider range of users and is difficult to resolve becomes a problem. MSI shall identify and resolve all the application problems in the identified solution (e.g. system malfunctions, performance problems and data corruption etc.).

ii. Monthly report on problem identified and resolved would be submitted to BSCLalong with the recommended resolution.

e) Change and Version Control

All planned or emergency changes to any component of the system shall be through the approved Change Management process. The MSI needs to follow all such processes (based on industry ITSM framework). For any change, MSI shall ensure:

i. Detailed impact analysis
ii. Change plan with Roll back plans
iii. Appropriate communication on change required has taken place
iv. Proper approvals have been received
v. Schedules have been adjusted to minimize impact on the production environment
vi. All associated documentations are updated post stabilization of the change
vii. Version control maintained for software changes

The MSI shall define the Software Change Management and Version control process. For any changes to the solution, MSI has to prepare detailed documentation including proposed changes, impact to the system in terms of functional outcomes/additional features added to the system etc. MSI shall ensure that software and hardware version control is done for entire duration of MSI's contract.

a) Maintain configuration information

MSI shall maintain version control and configuration information for application software and any system documentation.

b) Training

MSI shall provide training to BSCLpersonnel whenever there is any change

in the functionality. Training plan has to be mutually decided with BSCL.

c) Maintain System documentation

MSI shall maintain at least the following minimum documents with respect to the ICCCSystem:

i. High level design of whole system
ii. Low Level design for whole system / Module design level
iii. System Requirements Specifications (SRS)
iv. Any other explanatory notes about system
v. Traceability matrix
vi. Compilation environment

MSI shall also ensure updation of documentation of software system ensuring that:

i. Source code is documented
ii. Functional specifications are documented
iii. Application documentation is updated to reflect on-going maintenance and
iv. Enhancements including FRS and SRS, in accordance with the defined standards
v. User manuals and training manuals are updated to reflect on-going
vi. Changes/enhancements
vii. Standard practices are adopted and followed in respect of version control and management.

a) All the project documents need to follow version control mechanism. MSI will be required to keep all project documentation updated and should ensure in case of any change, the project documents are updated and submitted to BSCL by the end of next quarter.
b) For application support MSI shall keep dedicated software support team to be based at MSIlocation that will single point of contact for resolution of all application related issues. This team will receive all the application related tickets/incidents and will resolve them. In its technical proposal MSI need to provide the proposed team structure of application support including number of team members proposed to be deployed along with roles and skills of each such member. Application support team shall be employees of MSI.
c) Any software changes required due to problems/bugs in the developed software/application will not be considered under change control. The MSI will have to modify the software/application free of cost. This may lead to enhancements/customizations and the same needs to be implemented by the MSI at no extra cost.
d) Any additional changes required would follow the Change Control Procedure. BSCLmay engage an independent agency to validate the estimates submitted by the MSI. The inputs of such an agency would be taken as the final estimate for efforts required. MSI to propose the cost of such changes in terms of man month rate basis and in terms of Function point/Work Breakdown Structure (WBS) basis in the proposal.

4.10.2. ICT Infrastructure Support and Maintenance

ICT infrastructure includes servers, storages, back up, networking, load balancers, security equipment, operating systems, database, enterprise management system, help desk system and other related ICT infrastructure required for running and operating the envisaged system. MSI shall prepare documentation/policies required for certifications to include Policies, Historic Alarms, Routing etc. Manuals to be updated periodically.MSI should also prepare and manage all the Policies. These includes Backup and Restore Policies, Storage Policies, Retention Policies, Firewall Policies, and Secure domain Policies etc. MSI should prepare all the SOPs which include BPNM, Workflow, SOP handling, degraded operations, Mayday SOPs etc.

MSI shall define, develop, implement and adhere to IT Service Management (ITSM) processes aligned to ITIL framework for all the IT Services defined and managed as part of this project.

4.10.3. Warranty support

a) MSI shall provide comprehensive and on-site warranty for 5 years from the date of Final Go-Live for the infrastructure deployed on the project. MSI need to have OEM support for thesecomponents and documentation in this regard need to be submitted to BSCLon annual basis.
b) MSI shall provide the comprehensive & onsite manufacturer's warranty in respect of properdesign, quality and workmanship of all hardware, equipment, accessories etc. covered by theRFP. MSI must warrant all hardware, equipment, accessories, spare parts, software etc.procured and implemented as per this RFP against any manufacturing defects during thewarranty period.
c) MSI shall provide the performance warranty in respect of performance of the installedhardware and software to meet the performance requirements and service levels in the RFP.
d) MSI is responsible for sizing and procuring the necessary hardware and software licenses asper the performance requirements provided in the RFP. During the warranty period MSI shall replace or augment or procure higher-level new equipment or additional licenses/hardware at no additional cost to the BSCL in case the procured hardware or software is not enough or is undersized to meet the service levels and the project requirements.
e) During the warranty period MSI shall maintain the systems and repair/replace at the installedsite including all consumables, at no charge to BSCL, all defective components that are brought to the MSI's notice.
f) The MSI shall carry out Preventive Maintenance (PM) of all hardware and testing for virus, ifany, and should maintain proper records at each site for such PM. The PM should be carried out at least once in six months as per checklist and for components agreed with BSCL.
g) The MSI shall carry out Corrective Maintenance for maintenance/troubleshooting of supplied hardware/software and support infrastructure problem including network (active/passive) equipment, security and rectification of the same. The MSI shall also maintain complete documentation of problems, isolation, cause and rectification procedures for

building knowledge base for the known problems in centralized repository, accessible to BSCLteamas well.

h) MSI shall monitor warranties to check adherence to preventive and repair maintenance terms and conditions.

i) The MSI shall ensure that the warranty complies with the agreed technical standards, security requirements, operating procedures, and recovery procedures.

   i. 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.
   ii. Any 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).
   iii. The MSI shall introduce a comprehensive Assets Management process & appropriate tool to manage the entire lifecycle of every component of ICCCsystem.

4.10.4. Maintenance of ICT Infrastructure at DC and ICCC

a) Management of DC andICCC

MSI need to deploy requisite mix of L1, L2 and L3 resources (on 24X7 basis) for management of entireICCCSystem including ICT infrastructure deployed at DC and ICCC.All resources deployed in the project should be employees of MSI and be Indian citizens. All theL1 and L2 resources proposed for the project need to be dedicated for the project. Any change in the team once deployed will require approval from BSCL. It is expected that resources have proven track record and reliability. Considering the criticality of the project, BSCL may ask for security verification (Police verification) of every resource deployed on the project and MSI need to comply the same before deployment of the resource at the project. At all times, the MSI need to maintain the details of resources deployed for the project to BSCL and keep the same updated. Detailed process in this regard will be finalized between BSCL and MSI. The MSI shall maintain an attendance register for the resources deployed. Attendance details of the resources deployed also need to be shared with BSCLon monthly basis. BSCLreserves the right to interview resourcesdeployed for Operations and maintenance and assess the suitability of the resource for the role. Incase a resource is not found suitable, MSI will change the resource on request of BSCL. MSI shall comply with this.

The scope of work for infrastructure and maintenance includes the following:

   i. DC operations to be in compliance with industry leading ITSM frameworks like ITIL, ISO
   ii. ISO 20000 & ISO 27001
   iii. Ensure compliance to relevant SLA’s

iv. 24x7 monitoring & management of availability & security of the infrastructure and assets
v. Perform regular hardening, patch management, testing and installation of software updates issued by OEM/vendors from time to time after following agreed process
vi. Ensure overall security – ensure installation and management of every security component at every layer including physical security
vii. Prepare documentation/policies required for certifications included in the scope of work
viii. Preventive maintenance plan for every quarter
ix. Performance tuning of system as required
x. Design and maintain Policies and Standard Operating Procedures
xi. User access management
xii. Other activities as defined/to meet the project objectives
xiii. Up-dation of all Documentation.

During operations phase the MSI needs to submit proof of renewal of support for all IT infrastructure products and other system software's for whom it is mandated to have OEM support.

This needs to be submitted on an annual basis and needs to be verified before release of 2nd quarter payment of each year.

b) System Maintenance and Management

i. MSI shall be responsible for tasks including but not limited to setting up servers, configuring and apportioning storage space, account management, performing periodic backup of data and automating reporting tasks, and executing hardware and software updates when necessary. It shall be noted that the activities performed by the MSI may also be reviewed by BSCL.
ii. MSI shall provision skilled and experienced manpower resources to administer and manage the entire system at the Data Center.
iii. On an ongoing basis, MSI shall be responsible for troubleshooting issues in the IT infrastructure solution to determine the areas where fixes are required and ensuring resolution of the same.
iv. MSI shall be responsible for identification, diagnosis and resolution of problem areas pertaining to the IT Infrastructure and maintaining the defined SLA levels.
v. MSI shall implement and maintain standard operating procedures for the maintenance of the IT infrastructure based on the policies formulated in discussion with BSCL and based on the industry best practices/frameworks. MSI shall also create and maintain adequate documentation/checklists for the same.

vi. MSI shall be responsible for managing the user names, roles and passwords of all the relevant subsystems, including, but not limited to servers, other devices, etc. MSI shall be required to set up the directory server. Logs relating to access of system by administrators shall also be kept and shall be made available to BSCL on need basis.

vii. MSI shall implement a password change mechanism in accordance with the security policy formulated in discussion with BSCL and based on the industry best practices/frameworks like ISO 27001, ISO 20000 etc.

viii. The administrators shall also be required to have experience in latest technologies so as to make provision for the existing and applicable infrastructure on a requirement based scenario.

c) System Administration

i. 24*7*365 monitoring and management of the servers in the DC.

ii. MSI shall also ensure proper configuration of server parameters and performance tuning on regular basis. MSI shall be the single point of accountability for all hardware maintenance and support the ICT infrastructure. It should be noted that the activities performed by theMSI may be reviewed by BSCL.

iii. MSI shall be responsible for operating system administration, including but not limited to management of users, processes, preventive maintenance and management of upgrades including updates, upgrades and patches to ensure that the system is properly updated.

iv. MSI shall also be responsible for installation and re-installation of the hardware(s) as well as the software(s) in the event of system crash/failures.

v. MSI shall also be responsible for proactive monitoring of the applications hosted

vi. MSI shall appoint system administrators to regularly monitor and maintain a log of the monitoring of servers to ensure their availability to BSCL at all times.

vii. BSCL shall undertake regular analysis of events and logs generated in all the sub systems including but not limited to servers, operating systems etc. The system administrators shall undertake actions in accordance with the results of the log analysis. The system administrators shall also ensure that the logs are backed up and truncated at regular intervals.MSI shall refer to CERT-In Guidelines so as to ensure their alignment with the practices followed.

viii. The system administrators shall adopt a defined process for change and configuration management in the areas including, but not limited to, changes in servers, operating system, applying patches, etc.

ix. The system administrators shall provide hardening of servers in line with the defined security policies. Validation of hardening configuration will be carried out quarterly and deviations must be tracked through SLA reporting.
x. The system administrators shall provide integration and user support on all supported servers, data storage systems etc.
xi. The system administrators shall be required to trouble shoot problems with web services, application software, server relationship issues and overall aspects of a server environment like managing and monitoring server configuration, performance and activity of all servers.
xii. The system administrators should be responsible for documentation regarding configuration of all servers, IT Infrastructure etc.
xiii. The system administrators shall be responsible for managing the trouble tickets, diagnosis of the problems, reporting, managing escalation, and ensuring rectification of server problems as prescribed in Service Level Agreement.
xiv. The administrators will also be required to have experience in latest technologies so as to provision the existing and applicable infrastructure on a requirement based scenario.

d) Storage Administration

i. MSI shall be responsible for the management of the storage solution including, but not limited to, storage management policy, configuration and management of disk array, SANfabric/switches, tape library, etc. It should be noted that the activities performed by the MSImay be reviewed by BSCL.
ii. MSI shall be responsible for storage management, including but not limited to management of space, SAN/NAS volumes, RAID configuration, LUN, zone, security, business continuity volumes, performance, etc.
iii. The storage administrator will be required to identify parameters including but not limited to key resources in the storage solution, interconnects between key resources in the storage solution, health of key resources, connectivity and access rights to storage volumes and the zones being enforced in the storage solution.
iv. The storage administrator will be required to create/delete, enable/disable zones in the storage solution.
v. The storage administrator will be required to create/delete/modify storage volumes in the storage solution.
vi. The storage administrator will be required to create/delete, enable/disable connectivity and access rights to storage volumes in the storage solution.
vii. To facilitate scalability of solution wherever required.
viii. The administrators will also be required to have experience in technologies such as virtualization and cloud computing so as to

provision the existing and applicable infrastructure on a requirement based scenario.

e) Database Administration

i. MSI shall be responsible for monitoring database activity and performance, changing the database logical structure to embody the requirements of new and changed programs.
ii. MSI shall be responsible to perform physical administrative functions such as reorganizing the database to improve performance.
iii. MSI shall be responsible for tuning of the database, ensuring the integrity of the data and configuring the data dictionary.
iv. MSI will follow guidelines issued by BSCL in this regard from time to time including access of data base by system administrators and guidelines relating to security of data base.
v. Database administration should follow the principle of segregation of duties to ensure no single DBA can update production tables/data singularly.
vi. In addition to restrictions on any direct change in Data by any administrator, the Databases shall have Auditing features enabled to capture all activities of administrators.

f) Backup/Restore/Archival

i. MSI shall be responsible for implementation of backup & archival policies as finalized withBSCL. The MSI is responsible for getting acquainted with the storage policies of BSCLbefore installation and configuration. It should be noted that the activities performed by theMSI may be reviewed by BSCL.
ii. MSI shall be responsible for monitoring and enhancing the performance of scheduled backups, scheduled regular testing of backups and ensuring adherence to related retention policies.
iii. MSI shall be responsible for prompt execution of on-demand backups of volumes and files whenever required by BSCLor in case of upgrades and configuration changes to the system.
iv. MSI shall be responsible for real-time monitoring, log maintenance and reporting of backup status on a regular basis. MSI shall appoint administrators to ensure prompt problem resolution in case of failures in the backup processes.
v. MSI shall undertake media management tasks, including, but not limited to, tagging, cross-referencing, storing, logging, testing, and vaulting in fire proof cabinets (onsite and offsite asper the detailed process finalized by during project implementation phase).
vi. MSI shall also provide a 24 x 7 support for file and volume restoration requests at the Data Centre.

g) Network monitoring

i. MSI shall provide services for management of network environment to maintain performance at optimum levels on a 24 x 7 basis. It should be noted that the activities performed by the MSI may be reviewed by BSCL.
ii. MSI shall be responsible for creating and modifying VLAN, assignment of ports to appropriate applications and segmentation of traffic.
iii. MSI shall also be responsible for break fix maintenance of the LAN cabling within DC/ICCCetc.
iv. MSI shall also provide network related support and will coordinate with connectivity service providers of BSCL/other agencies who are terminating their network at the DC/ICCCforaccess of system.

h) Security Management

i. Regular hardening and patch management of components of the ICCC System as agreed with BSCL
ii. Performing security services on the components that are part of the BSCL environment as per security policy finalized with BSCL
iii. IT Security Administration – Manage and monitor safety of information/data
iv. Reporting security incidents and resolution of the same
v. Proactively monitor, manage, maintain & administer all security devices and updateengine, signatures, and patterns as applicable.
vi. Managing and monitoring of anti-virus, anti-malware, phishing and malware for managedresources.
vii. Ensuring 100 percent antivirus coverage with patterns not old more than period agreed onany given system
viii. Reporting security incidents and co-ordinate resolution
ix. Monitoring centralized pattern distribution (live update) and scan for deficiencies
x. Maintaining secure domain policies
xi. Secured IPsec/SSL/TLS based virtual private network (VPN) management
xii. Performing firewall management and review of policies on at-least quarterly basis during first year of O&M and then after at-least on half-yearly basis
xiii. Resolution of calls for security notifications, system alerts, vulnerabilities in hardware/software and alerting BSCLas appropriate
xiv. Performing patch management using software distribution tool for all security applications including content management system, antivirus and VPN

xv. Providing root cause analysis for all defined problems including hacking attempts
xvi. Monthly reporting on security breaches and attempts plus the action taken to thwart the same and providing the same to BSCL
xvii. Maintaining documentation of security component details including architecture diagram, policies and configurations
xviii. Performing periodic review of security configurations for inconsistencies and redundancies against security policy
xix. Performing periodic review of security policy and suggest improvements
xx. Reviewing logs daily of significance such as abnormal traffic, unauthorized penetration attempts, any sign of potential vulnerability. Security alerts and responses. Proactive measures in the event a problem is detected
xxi. Policy management (firewall users, rules, hosts, access controls, daily adaptations)
xxii. Modifying security policy, routing table and protocols
xxiii. Performing zone management (DMZ)
xxiv. Sensitizing users to security issues through regular updates or alerts –periodic updates/Help BSCLissuance of mailers in this regard
xxv. Performing capacity management of security resources to meet business needs
xxvi. Rapidly resolving every incident/problem within mutually agreed timelines
xxvii. Testing and implementation of patches and upgrades
xxviii. Network/device hardening procedure as per security guidelines from BSCL
xxix. Implementing and maintaining security rules
xxx. Performing any other day-to-day administration and support activities

i) Other Activities

i. MSI shall ensure that it prepares configuration manual for OS, appliances, middleware, all tool, servers/devices and all equipment's and the same need to be submitted to BSCL, any changes in the configuration manual need to be approved by BSCL. Configuration manual to be updated periodically.
ii. MSI shall maintain data regarding entitlement for software upgrades, enhancements, refreshes, replacements and maintenance.
iii. If the Operating System or additional copies of Operating System are required to be installed/reinstalled/un-installed, the same should be done as part of O&M.
iv. MSI should carry out any requisite adjustments/changes in the configuration for implementing different versions of Application Software.

v. Updates/Upgrades/New releases/new versions: The MSI shall provide from time to time the Updates/Upgrades/new releases/new versions of the software and operating systems as required. The MSI should provide free upgrades, updates & patches of the software and tools to BSCLas and when released by OEM.

vi. MSI shall provide patches to the software as part of IT infrastructure, operating system, databases and other applications.

vii. Software License Management: The MSI shall provide for software license management and control. MSI shall maintain data regarding entitlement for software updates, enhancements, refreshes, replacements, and maintenance.

viii. Data backup/recovery management services

ix. All other activities required to meet the project requirements and service levels.

x. It is responsibility of the MSI to scale up the Operations & Maintenance (O&M) team as and when required to ensure smooth project execution throughout the project duration.

4.10.5. Compliance to SLA

a) MSI shall ensure compliance to uptime and performance requirements of project solution as indicated in the SLA (as per Volume III of RFP) table of RFP and any upgrades/major changes to the ICCC System shall be accordingly planned by MSI for ensuring the SLA requirements.

b) MSI shall be responsible for measurement of the SLAs at the ICCC System level swell as at the user level with the help of the enterprise monitoring tool on a periodic basis.

c) Reports for SLA measurement must be produced BSCL officials as per the project requirements.

4.11. 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, MSI will ensure that the entire Project is developed in compliance with the applicable standards.

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

Table 4:Standards & Certifications for Compliance

S.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 fordocumentation

c) Apart from the above MSI need to ensure compliance of the project with Government of India IT security guidelines including provisions of:
   i. The Information Technology Act, 2000 and amendments thereof and
   ii. Guidelines and advisories for information security published by CERT-In/MeitY (Government of India) issued till the date of publishing of tender notice. Periodic changes in these guidelines during project duration need to be complied with.

d) While writing the source code for application modules 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:
   i. The name of the module
   ii. The date when module was created
   iii. A description of what the module does
   iv. A list of the calling arguments, their types, and brief explanations of what they do
   v. A list of required files and/or database tables needed by the module
   vi. Error codes/Exceptions
   vii. Operating System (OS) specific assumptions
   viii. A list of locally defined variables, their types, and how they are used
   ix. 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
   i. Proper and consistent indentation
   ii. Inline comments
   iii. Structured programming
   iv. Meaningful variable names
   v. Appropriate spacing
   vi. Declaration of variable names
   vii. Meaningful error messages

f) Quality Audits
   i. BSCL, at its discretion, may also engage independent auditors to audit any/some/all standards/processes. MSI shall support all such audits as per calendar agreed in advance. The result of the audit shall be shared with MSI who has to provide an effective action plan for mitigations of observations/non-compliances, if any.
   ii. MSI should comply with all the technical and functional specification provided in various sections in this RFP document.

4.12. 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. MSI may propose further detailed Acceptance criteria which the BSCL will review. Once BSCL provides its approval, the Acceptance criteria can be finalized. In case required, parameters might be revised by BSCL 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:

Table 5: Various Testing envisaged for the project

Type of Testing	Responsibility	Scope of Work
System Testing	✓ MSI	▪ MSI to perform System testing ▪ MSI to prepare test plan and test cases and maintain it. BSCL may request MSI to share the test cases and results ▪ Should be performed through manual as well as automated methods ▪ Automation testing tools to be provided by MSI. BSCL doesn't intend to own these tools
Integration Testing	✓ MSI	▪ MSI to perform Integration testing ▪ MSI to prepare and share with BSCL the Integration test plans and test cases ▪ MSI to perform Integration testing as per the approved plan ▪ Integration testing to be performed through manual as well as automated methods ▪ Automation testing tools to be provided by MSI
Performance andLoad Testing	✓ MSI ✓ BSCL/ Third Party Auditor(to monitor the performance testing)	▪ MSI to do performance and load testing. ▪ Various performance parameters such as transaction response time, throughput, and page loading time should be taken into account. ▪ Load and stress testing of the Project to be performed on business transaction volume ▪ Test cases and test results to be shared with BSCL ▪ Performance testing to be carried out in the exact same architecture that would be set up for production ▪ MSI need to use performance and load testing tool at the time of Go-Live and at the end of every 6 months during O&M Phase. ▪ BSCLif required, could involve third party auditors to monitor/validate the performance testing. Cost for such audits to be paid by BSCL
Security Testing (including Penetration and Vulnerability testing)	✓ MSI ✓ BSCL/ Third Party Auditor (to monitor the security testing)	▪ 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, datacenter, security monitoring system deployed by MSI. ▪ Solution shall pass vulnerability and penetration testing for roll out 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. ▪ MSI should carry out security and vulnerability testing on the developed solution. ▪ Security testing to be carried out in the exact same environment/architecture that would be setup for production. ▪ Security test report and test cases should be shared with BSCL

Type of Testing	Responsibility	Scope of Work
		▪ Testing tools if required, to be provided by MSI. ▪ During O&M phase, penetration testing to be conducted on yearly basis and vulnerability assessment to be conducted on half-yearly basis. ▪ BSCL 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 BSCL
User Acceptance Testing of Project	✓ BSCLor BSCLappointed third party auditor	▪ BSCL/BSCL appointed third party audit or to perform User Acceptance Testing ▪ MSI to prepare User Acceptance Testing test cases ▪ UAT to be carried out in the exact same environment/architecture that would be set up for production ▪ MSI should fix bugs and issues raised during UAT and get approval on the fixes from BSCL/third party auditor before production deployment ▪ 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. BSCL does not intend to own the tools.

b. MSI shall work in a manner to satisfy all the testing requirements and adhere to the testing strategy outlined. MSI must ensure deployment of necessary resources and tools during the testing phases. 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 MSI meets all the requirements specified in the RFP. MSI shall take remedial action based on outcome of the tests.

c. 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 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 BSCL directly. All tools/environment required for testing shall be provided by MSI.

e. STQC/Other agencies appointed by BSCL 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 MSI.

4.13. Factory Testing& Pre-Despatch Inspection

a) Successful MSI shall have to submit Factory Test Certificate for all the ICCC, DC & ICT Equipment (Active & Passive) before the actual supply of the items.MSI has to provide MAF (OEM warranty certificate) for all the ICCC, DC & ICT Active Equipment.
b) BSCL reserve the right to visit the OEM premises for Pre-Despatch Inspection of all the ICCC, DC & ICT Active Equipment through the Technical team at the cost of MSI. All the supply for the approved quantity will happen after clearance of such Technical team.
c) Technical Committee can ask for 72 hours Burn-in test of all the Desktops, Workstations, Servers and its associated accessories.

4.14. Final Acceptance Testing

The final acceptance shall cover 100% of the BSCL Project, after successful testing by the BSCL; a Final Acceptance Test Certificate (FAT) shall be issued by the BSCL to MSI.

Prerequisite for Carrying out FAT activity:

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

The FAT shall include the following:

a) All hardware and software items must be installed at respective sites as per the specification.
b) Availability of all the defined services shall be verified.
c) MSI shall be required to demonstrate all the features / facilities / functionalities as mentioned in the RFP.
d) MSI shall arrange the test equipment required for performance verification, and will also provide documented test results.
e) MSI shall be responsible for the security audit of the established system to be carried out by a certified third party as agreed by BSCL.
f) Any delay by 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 BSCL and MSI. In the event MSI is not able to complete the installation due to non-availability of bandwidth from the bandwidth service providers, the Supplier and BSCL may mutually agree to redefine the Network so that MSI can complete installation and conduct the Final Acceptance Test within the specified time.

5. Detailed Scope of Work with Specifications

5.1. Integrated Command & Control Centre (ICCC)

5.1.1. Command & Control Centre Application

It is envisaged that the city will implement multiple Smart City use cases over a period of time. The potential example Smart City use cases are-

a) Smart Parking
b) Smart Traffic Management
c) Public Safety and Safe City Operations
d) Connected Public Transport
e) Environmental Monitoring
f) Smart Waste Management

ICCC will be able to provide and transfer information and data to Patna command centre as and when required.Master Command Centre in Patna will be able to access any control from Bhagalpur Command Centre as and when required. Patna(Hub) will be have seamless integration with Bhagalpur (Spoke) Command and Control Centre

5.1.2. Functional & Technical Requirements for ICCC Platform

S.N.	Description	
1.	Integration platform of aggregation of information in form of data	i. The City will be using various device vendors for various urban services. Various Solutions and technologies of smart elements will be used for deployment and each will be generating data in their own format. This Smart City platform should be able to define its own data model for each urban service like parking, waste, lighting, transport etc. and map data from different device vendors to the common data model. ii. Application development and analytics applications should be able to use of various data formats. iii. Open platform to normalize the data to provide secure access to that data using data API(s) to application developer. iv. This data must be exposed to all type of application eco system using secure APIs. v. The attributes of the API key(s) must restrict / allow access to relevant data from specified domain, sensor andsolution identified. vi. The platform should be open/able to integrate with any type of sensor platform being used for the urban services irrespective of the technology used.

S.N.	Description	
		Agnostics to sensor technologies such as LoRA, ZigBee, GPRS, Wi-Fi, IP Camera. vii. The platform should be open and allow the manufacturers of the sensors to develop integrations themselves using SDKs without affecting the northbound applications and existing integration The platform should have the ability and provision to write adaptors, which interface with the sensors or sensor management software. viii. The Command & Control solution should adhere to the principles & guidelines of open standards published by GoI. ix. Platform should support fault tolerance, load balancing and high availability. x. 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. xi. The platform should be able to convert the data coming from different devices of same type for correlation between various sources.
2.	Distributed Architecture	The platform should support distributed deployment of functions (workflows & policies) across city's network and compute infrastructure with centralized management and control
3.	Device Abstraction method	The platform should neutralize the device data for M2M communication.
4.	GIS Map Support and Location identifier and mapper	System should support Esri, map box, Open street and other GIS applications. a) Map services and geospatial coordinates: provides the geographical coordinates of various assets and locations of the city b) Geospatial calculation: calculates distance between two, or more, locations on the map Location-based tracking: locates and traces devices on the map and provide real time attributes on map when required. The solution shall integrate with GIS and map information and be able to dynamically update information on the GIS maps to show status of resources.

S.N.	Description	
5.	Service management	Performs service management like ID, EVENT Management etc.
6.	Developer Program tools	Middleware ICCC Platform should provide Developer Program tools that help City to develop / integrate new applications, and/or use solution SDK/APIs to enhance or manage existing solution.
7.	API Repository / API Guide	i. Neutral data APIs should be available for the various solutions implemented to monitor, control sensor and/or actuators to provide functionality to enable app developers to develop apps on this platform. ii. API Repository and user guide should be publically available for other OEM/manufactures to do further development of interfaces without any cost. iii. Cross collaboration APIs enables contextual information and correlation across domains and verticals (Multiple vendor and Multi-sensor in future) to be provided.
8.	Authentication, Authorization	System should support standard Authentication, Authorization protocols
9.	Data plan Functionalities	Live data and visual feed from diverse sensors connected to the platform
10.	Platform upgrade and maintenance	Facility for securely access the ICCC platform remotely for platform updates / upgrades and maintenance for the given duration. Platform should be able to be deployed on a public cloud for disaster recovery.
11.	Platform functionality, API Management	i. Provides secure API lifecycle, monitoring mechanism for available APIs as API management. ii. Provides different tier of user categorization, authentication, authorization, and services based on the subscriptions/type of user. iii. Provides role-based access view to applications. iv. Historical and real-time data available for big data and analytics at any point of time. v. Enables the City and its partners to define a standard data model for each of the urban services solutions using API's.
12.	ICCC Operation	i. The solution should be implemented and compliant to industry open standard commercial-off-the-shelf (COTS) applications that are customizable. ii. The solution shall also provide an integrated user

S.N.	Description		
			interface for all the smart solution elements implemented.
		iii.	The solution should provide operators and managers with a management dashboard that provides a real time status and is automatically updated when certain actions, incidents and resources have been assigned, pending, acknowledged, dispatched, implemented, and completed with clear identification code.
		iv.	The solution shall provide the "day to day operation", "Common Operating Picture" and situational awareness to the centre and participating agencies during these modes of operation.
		v.	It shall improve visibility for large and geographically distributed environments.
		vi.	It shall provide complete view of all solutions in an easy-to-use and intuitive GIS-enabled graphical interface with a powerful workflow and business logic engine.
		vii.	It shall provide a uniform, coherent, user-friendly and standardized interface.
		viii.	It shall provide possibility to connect to workstations and access visualization layer and dashboards via web browser
		ix.	Role based filtering should be allowed.
		x.	The solution should allow creation of hierarchy of incidents and be able to present the same in the form of a parent-child structure for analysis purposes.
		xi.	It shall be possible to combine the different views onto a single screen or a multi-monitor workstation.
		xii.	The solution should maintain a comprehensive audit trail of read and write actions performed on the system for PSC when required.
		xiii.	The solution should provide ability to extract data in various formats for publishing and reporting.
		xiv.	The solution should have functionality to attach reference documents and other artifacts' to incidents and other entities.
		xv.	The solution is required to issue, log, track, manage

S.N.	Description		
			and report on all activities underway during these modes of operation: • anticipation of incident • incident or crisis • recovery
13.	Integration capabilities	i. ii. iii.	This platform is expected to integrate various urban services devices at the street level sensors or instruments so that urban services applications can be developed on top of this platform independent of the technology that is used in the devices. Platform should be able to integrate devices using their APIs in to this platform by writing appropriate integration adaptor. Platform should support on the fly deployment, add/modify/removal of Sensors without shut down and auto detect of sensors.
14.	Edge Computing support for future	i. ii. iii. iv. v. vi. vii. viii.	Ability to support standard edge appliance to connect industrial protocol devices, provides secure connection deployed infrastructure. Provides remote management including, self-registration, and local administrative interface. ICCC platform should support edge computing where, local processing of events, contextualization, transformation, analytics, decisions and controls happens on edge device. ICCC platform should allow toset or change the behaviour on the edge through policies. Edge computing should learn the behaviour as analysing the data to create better decisions with time. Share the outcomes with other edges when required. Provide centralized Device Management from sensor. Provide management tools to view, analyse and report on the edge configurations. Edge software should be open to use on any sensors and devices or protocols. Same software blueprint should be deployed and running on all edges. Data and Configurations can be different from edge to edge based on requirement.

S.N.	Description	
15.	Trending Service	System should provide trends in graphical representation from data sources over a period of time. Trends should allow to monitor and analyse device performance over time.
16.	Policies and Events	i. System should allow policy creation to set of rules that control the behavior of infrastructure items. Each policy should a set of conditions that activate the behavior it provides based on pre-defined threshold. System should allow Default, Time-based, Event-based and Manual override polices creation. For example, an operator might enforce a "Lane close/ Electricity shout down " policy manually based on event. ii. System should provision to defines a set of conditions that can be used to trigger an event-based policy.
17.	Notifications, Alerts and Alarms	i. System should generate Notification, Alert and Alarm messages based on event, issue that should be visible within the Dashboard and to the respective authority over Mobile App if required. ii. All system messages (notifications, alerts and alarms) should always visible from the Notifications view, which provides controls that operator can use to sort and filter the messages that it displays. iii. Systems should deliver message to a set of subscribers. The Notification service should support min two types of notification methods – Email notification and Short Messaging Service (SMS) notification and any other mode available.
18.	Users and roles	i. Users access the platform for various tasks, such as adding new locations, configuring new devices, managing adapters, and so on. However, not all users can perform all tasks. Each user should be associated with one or more roles and each role is assigned a certain set of permissions for batter access and responsibility. ii. These roles and permissions define the tasks that a user can perform. Additionally, system should assign one or more locations to each role so that the

S.N.	Description	
		user can perform tasks at the assigned locations only. iii. The platform should allow different roles to be created and assign those roles to different access control policies. iv. System should support LDAP to be used as an additional data store for user management and authentication.
19	Reports	i. The platform should have capability to provide access to real time data and historical data from various connected devices for reporting and analytics. ii. System should allow dashboard to generate reports and have provision to add reports in favourites list and have provision to send reports automatically based on predefined rules.
20	Standard Operating Procedure	i. 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 based on use cases defined as per city and solution requirement. ii. Integrated Command & Control Center platform should provide for authoring and invoking un-limited number of configurable and customizable standard operating procedures in multiple languages through graphical, easy to use tooling interface. It should have: iii. Ability to edit the SOP, including adding, editing, or deleting the activities. iv. Ability of automatically logging the actions, changes, and commentary for the SOP and its activities, so that an electronic record is available for after-action review. v. Ability to add comments to or stop the SOP (prior to completion). vi. Ability to define the following activity types: vii. **Automation Activity** – Based on predefined rule and threshold, activity initiates and tracks a particular work flow and select a predefined flow order from the list.

S.N.	Description		
		viii.	**Manual Activity** – Based on the emergency event or any other circumstances activity that is done manually by the owner with details of event.
		ix.	**If-Then-Else Activity** - Conditional activity that allows branching based on specific criteria.
		x.	**Notification Activity** - Activity that displays a notification window that contains an email template for the activity owner to complete, and then sends an email notification.
		xi.	**SOP trigger** - An activity that launches another standard operating procedure.
21	Collaboration/Correlation	i.	The CCC platform should have ability or should be able to integrate with a third-party tool to bring multiple stake holders on to a common voice conference call for virtual meeting and groups as a standard operating procedure in response configured events.
		ii.	Ability to view on computer or hand-held devices.
		iii.	Ability to notify the users using email, sms etc.
		iv.	Ability to bring in multiple stake holders automatically into a common collaboration platform in response to a SOP defined to handle a particular event.
		v.	The platform should allow stakeholders to share content relevant to the issue in the collaboration space.
		vi.	The ICCC platform user/operator should be able to interface with the Multiparty Conf. Unit (section 5.1.14) & Video Conferencing (section 5.1.13) invoke a conferencing session . It should be possible to include all stakeholders in the collaboration space.
		vii.	The platform should allow information's related to smart city devices (cameras, lights, various sensors etc.) to be added to the collaboration spaces. It should also allow the operator to acquire data from such devices and take actions based on the decisions made in the collaboration space, subject to access privileges for each user and device.
		viii.	The platform should allow stakeholders to participate in the web conferencing session

S.N.	Description	
22	Analytics Engine	i. Artificial intelligence-based ICCC analytics platform module to maximize business value through advanced machine learning capabilities. The machine learning capabilities aid in automating policies that result in better asset and infrastructure management. ii. Analytics engine should be flexible to integrate with other city and government software applications. iii. Solution should be robust, secure and scalable. iv. Data Analytics should have minimum below capabilities; a) Advanced Predictive Analytics b) Ability to integrate with other cities and government software applications c) Ability to predict insights consuming data from cities infrastructure d) Able to predict with measurable accuracy of at least >70% or better v. Ability to have a visualization platform to view historic analytics vi. Ability to discover, compare, and correlate data across heterogeneous data sources to unravel the patterns that are previously hidden. a) Connect to a variety of data sources b) Analyse the result set c) Visualize the results d) Predict outcomes vii. Ability to support multiple Data Sources. All standard data sources should be supported from day 1. viii. Able to provide analysis of data from a selected data source(s). ix. Able to define arithmetic and aggregation operations that result in the desired output. x. Able to provide capability to check analysis with multiple predictive algorithms.
23	Analytics Engine Visualizations	i. Analytics Engine should provide visualizations dashboard. ii. In the visualization workspace it should allow to change visual attributes of a graph.

S.N.	Description	
		iii. User should not be allowed to alter the graph/visualization definition. iv. In the visualizations workspace, user should able to do the following operations: a) Change the graph/visualization type b) Print the graph c) Export the graph d) Narrow down on the value ranges e) Toggle the axis labels f) Integrate with other 3rd party applications seamlessly
24	**Infrastructure components/API security:**	i. Platform should support user encrypted storage volumes. Restrict inbound access from public network only on secure ports via DMZ proxy instances. SSH access is restricted with secure key-pair and from designated jump hosts alone. User management and authentication is tied to Corporate SSO. ii. Platform should have appropriate technical controls in place to prevent attacks that target virtual infrastructure iii. Access to the platform API(s) should be secured using API keys. iv. Software should support security standards: O-Auth 2.0, HTTPS over SSL, and key management help protect the data across all domains. **v.** Should support security features built for many of its components by using HTTPS, TLS for all its public facing API implementations. For deployment where CCC Software API(s) exposed to application eco system, API Management, API security features and API Key management functions are required.
25	Performance Monitoring Tool	Performance monitoring tool shall include following functionalities i. Identify infra and/or application components between the user and backend servers that is causing the problems ii. Providing key performance indicators iii. Identify the inter-dependencies between application &infra components iv. Able to provide network/ system node causing the

S.N.	Description	
		problem v. Provide email, SMS and/or mobile alert mechanism if performances falls below predefined thresholds vi. Performance monitoring shall not adversely affect the performance of the platform
26.	Database monitoring	Platform should provide files and traps for database monitoring for DB health checksto monitor : i. Memory allocation, usage and contention ii. Disk I/O usage iii. CPU usage for a particular transition iv. Number of buffers, buffer size and usage v. Active locks and locks contention, including waiting time vi. Active users and status of their operations vii. List of users (complete or selected) with their access rights
27.	Video Display and integration capabilities	i. 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. ii. Should support SDK level integration with the proposed VMS and the ICCC operator must be able to fully control the VMS fuctions. iii. Integrate and assess inputs from different sources such as CCTV, Video Analytics, and sensors further to assist with actionable intelligence. iv. ICCC operator should be able to control the PTZ cameras and call functions like PAN/Tilt/Zoom etc. directly from the ICCC interface. v. Display module should have capability to control multi-screened display wall in sync with operator console vi. The system should dynamically reduce the bit rate and bandwidth for each stream based on the viewing resolution at the remote location vii. If the remote station is viewing with 352 x 240 (CIF), the stream to remote viewing location should not be using HD bandwidth, but dynamically should change to lower bandwidth

S.N.	Description		
		iii.	If the remote viewing station is viewing this camera in full screen 1080P, then it should dynamically increase the bandwidth to provide HD experience
		ix.	Smart City Operations Center should use dynamic channel coverage specifically for video stream function for efficient bandwidth usage for multiple operation center and only transmits video stream required to display on monitor to maximize bandwidth efficiency and should support minimum 16 camera feeds in single display
		x.	Platform shall process and transmit video streams adaptive to each video requests from a display server to optimize network bandwidth usage.
		xi.	Platform shall be able to transmit video streams in remote locations.
		xii.	Regardless of the numbers or the types of video input, platform shall be able to batch process and transmit multiple Full HD / HD video streams at all times.
		iii.	Platform shall be able to distribute real-time video streams to both display server and main operating server without any loss in original video quality
28	Forensic Investigation Feature	i.	Analysis in ICCC would be Graphical User Interface for search, replay and to simultaneously search and replay recorded video feeds, recorded telephone systems, VOIP, Screen recording, GPS data on GIS maps, conventional and digital radio channels as well as trunked radio communications. All communications regarding a specific incident should be replayed together in the sequence in which communications occurred on a synchronized timeline to support time coded playback of event. The solution should support event logs including operator's onscreen activities, voice &video events, etc. for further analysis, training and similar activities.
		ii.	The software must allow simple and quick search based on frequently used search parameters.
		iii.	The software must be capable of displaying multimedia search results graphically arranged by time of recording to allow a full view of the incident picture.
		iv.	The software must be capable of replaying an unlimited number of multimedia channels in synchronized mode. The software must allow the

S.N.	Description	
		user the capability of selecting and replaying part of a call, transmission, and video in either single item selection or when selecting multiple items. v. The software should support upload of incident related information into a single folder. The information should include: recordings made by the system as well as other related files - documents, photos, video clips, etc. The software must present the Incident folder storage usage. vi. The software must enable remote access to information for authorized users. This could be used by investigators, for example, in order to review evidentiary material in an organized manner rather than replay it from CD or DVD. vii. The distribution process and created incident folders must support an authentication mechanism to ensure the integrity of the incident information including audio and video recording as well as files such as: documents, photos, video clips, etc. The software must enable traceability of actions history taken on any of the incident information items. viii. The software system should provide detailed incident reporting and debriefing with time-coded playback of incident data on a single timeline. ix. It should allow synchronized playback - Exactly as it happened for post-mortem analysis and review. x. It should enable the authorities to find gaps in the incident handling and improve or rewrite SOPs. xi. CCC should have facility of integrating operator screen recording, Police (100), Fire (101) and xii. Health (102/108) Services (whenever they are available). Coordination with these agencies is critical. The integration shall be for recording of all the data types of the above services as well as for real time transactions and response. The CCC should also be able to group locations and connect surveillance systems to respond quickly to any emergency. xiii. The suite of software modules would be required to be scaled up to support any number of cameras, control rooms and client operators and would have multiple redundancy and security level options.
29.	Operational Requirements for Forensic Investigation	i. Forensic Investigation room shall be equipped with one video wall/TV, four workstations, IP telephone and at least five operators. ii. The forensic operators shall have facility to see live as well as playback videos of any camera. They shall keep a special watch on few selected cameras. iii. Video analytics software shall run on selected camera feeds to be further investigated by forensic operators.

S.N.	Description	
		iv. Forensic operators shall be equipped with software for: a) Examination of authenticity of uploaded photos and videos b) The system shall support for any standard image format (jpeg, tiff, bmp, png) and raw format from digital cameras. c) The system shall have filters to allow comparison of the results between two images, with user customizable configuration and optional post processing parameters d) The system shall have filter results saved in a cache folder for speedy subsequent analysis, with export analysis output as plain text, HTML, or TSV, with multiple file analysis table directly to spreadsheets for further processing. e) The system shall have automatic analysis of the format of all images in a folder to find suspicious files (triage), automatic comparison of the format of all files in a folder with the analyzed image, automatic comparison of the quantization tables of all files in a folder with the analyzed image. f) The system shall support search for similar images and images from a certain specific camera on Google Images. Supports advanced image features filtering. g) The system shall support search for images from a certain camera on Flickr. Supports advanced image features filtering.Reverse Image search engine Integration, The system shall support search for similar images on TinEye like reverse image search engine to make use of image identification technology rather than keywords, metadata or watermarks. ➢ Repair and recover videos ➢ Match photographs ➢ Provide forensic video enhancement of video evidence for identifying suspects, h) The system should take input from any standard video format (avi, flv, 3gpp, wmv, mov), also without the need of the codec installed on the system. Expandable by system codecs. i) The system should Convert proprietary surveillance video files to a standard AVI format like H264 j) The system should have screen capture utility to capture playback from DVR console display or proprietary player to avoid conversion and downscale issues

S.N.	Description	
		k) Provide recorded and archived media to authorized persons l) Transfer the evidence into a format that can be used for legal purposes etc. m) Post analysis of video provided through secondary source through various attributes like identified object, size, color etc. n) The system should allow automatic generation of a report containing all the scientific methodology and details of the processing steps, settings, and the bibliographic references to the algorithms in HTML format. o) The system should allow to track areas, people, objects through static, dynamic, and custom tracking. p) The system should allow display of Instant results like: add, configure, move, and modify an unlimited number of filters, in real time even while playing video. User can apply real-time, non-destructive image adjustments that don't require re-rendering as changes are applied. q) The system should Verify alteration of image and video files in saved projects using hash function, displaying Hash Code specific to saved files r) The system should display current image morphological and statistical features. s) The sytem shall reduces the noise integrating current and previous frames and avoiding halos on moving objects, reduces the noise integrating current and previous frames, reduces the noise by creating an image which is the average of all the frames, merges all frames to improve the resolution of the image v. Forensic operators shall also have access to recorded voice communications of dial 100 control room and radio gateway. vi. Forensic Analyst/Operator shall have following roles and responsibilities: a) Examine, enhance and authenticate digital and analogue CCTV video evidence for both criminal and civil litigation b) Assist the police in respect of preparation of evidence for legal and judicial purpose in court. c) Providing recorded and archived media to authorized persons. d) Transfer the evidence into a format that can be used for legal purposes e) Provide Forensic video enhancement of video evidence for identifying suspects.

S.N.	Description	
		f) Attending and examining scenes of crimes g) Repair and recovery of evidence h) Pixelizes, darkens or blurs an area of interest in a video (witness protection) i) Juxtaposes or overlays original and enhanced image for comparison j) Corrects the blur of objects which are out of focus (big blur) k) Corrects the blur of objects out of focus with blind deconvolution (little blur) l) Corrects the blur caused by air turbulence at long distances m) Non linear blur shall be supported.

5.1.3. Functional & Technical Requirements for Contact Centre

S.N.	Minimum Requirements
1.	The contact center solution shall include VoIP based EPBAX, IVRS, Automatic Call Distribution (ACD), Voice Logger Server among other hardware and software. Using the contact center solution, citizens can contact city administrator through the emergency communications system or through the contact center helpline number including Dial 100/112.
2.	Solution should be designed and implemented for minimum to 30 agents
3.	IVRS should be modular and scalable in nature for easy expansion without requiring any change in the software.
4.	The contact center solution should be able to route voice/ VOIP calls from centralized Interactive Voice Response System (IVRS) to respective call center (s).
5.	The callers should be able to access the various services through state-of-art centralized integrated Interactive Voice Response System (IVRS).
6.	IVRS should support various means of Alarm indications in case of system failures, e.g. Functional error, missing voice message prompt, etc., and shall generate error Logs. Also to identify other required services from IVR solution.
7.	IVRS shall be able to get information /text/data from databases, convert to voice, and speaks it back to the caller in relevant/desired language, including English and Hindi both.
8.	Solution should provide pre-integration with industry standard IVRS servers and enhance routing & screen pop by passing forward the information. Interactive Voice Response System (IVRS) should - a. play welcome messages to callers Prompts to press and collect DTMF digits b. be able to integrate with backend database for self-service, as and when required c. Offer GUI based tool to be provided for designing the IVR and ACD call flow. d. support Voice XML for ASR, TTS, and DTMF call flows e. be able to Read data from HTTP and XML Pages be able to run outbound campaigns
9.	Automatic call distribution (ACD) solution should - a. be able to route the call to any remote call center agent using IP phones b. have an ability to queue or hold the call for an agent if none is immediately available

	c. have an ability to keep the callers informed as to the status of the call and providing information to callers while they wait in queue d. be able to perform prioritized call routing e. be highly available with hot standby and seamless failover in case of main server failure f. support skill based routing and it should be possible to put all the agents in to a single skill group and different skill groups g. Support routing of incoming calls based upon caller input to menus, real-time queue statistics, time of day, day of week, ANI, dialed number etc. h. support call routing based on longest available agent, circular agent selection algorithms i. Maintain log of all services offered which can be used for audit and analysis purpose. j. 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 k. allow agents to chat with other Agents or supervisor from the Agent desktop software l. allow supervisor to see the real-time status of agents, supervisors should be able to make agent ready or logout from the supervisor desktop m. support Queuing of calls and playing different prompts depending on the type of call and time in the queue
10.	System shall provide for 100% recording of calls using a call logger. The recording shall contain detailed call information and the solution must provide advanced searching capabilities.
11.	Solution should have automatic identification ofincoming number based on landline and mobile number mapping. The recording shall be secure with AES Rijndael 256-bit encryption. The system shall have maker checker profile with MD5 finger printing.
12.	Solution should support call recording mapped to incident tickets
13.	Solution should offer customizable agent and supervisor desktop layout
14.	Solution should offer Inbound and outbound capability
15.	Solution should provide facilities for outbound calling list management, and software based predictive or preview dialing
16.	The agent's desktop shall have an application which shall fulfill the following functionalities : i. It should provide consistent agent interface across multiple media types like fax, SMS, telephone, email, and web call back. ii. The agent's desktop should have a "soft-phone" – an application that enables standard telephony functions through a GUI. iii. It should provide the agents with a help-desk functionality to guide the agents to answer a specific query intelligently. iv. It should also provide an easy access to agents to previous similar query which was answered successfully. v. It should also be possible to identify a request to be a similar request made earlier. vi. It should be possible for agents to mark a query as complex/typical and put in to database for future reference by other agents. vii. It should be possible for agents to escalate the query.
17.	System should be able to integrate with e–mail / SMS gateway so that appropriate messages can be sent to the relevant stakeholders after the interaction and any updates thereon.

18.	Should intelligently and automatically responds to email inquiries or routes inquires with skills based routing discipline to agents
19.	Live data reporting gadgets
20.	Multiline support
21.	Speed dial in IP phones
22.	Solution should provide CTI services such as: i. CTI link should allow a computer application to acquire control of the agent resources on the IP EPABX & change state of the agent phone through commands on the CTI link. ii. CTI link should pass events & information of agent states & changes in agent states as well as incoming calls to the computer applications. iii. CTI link should allow a computer application to take control of the call flow inside the IP EPABX & also allow the computer application to decide the most suitable action / agent for an incoming call. iv. automatic display (screen pop) of information concerning a user/customer on the call agent v. screen prior to taking the call based on ANI, DNIS or IVR data vi. Synchronized transfer of the data and the call to the call centre agent vii. Transfer of data corresponding to any query raised by any agent regarding a query raised by ➢ a caller whose call is being attended by the agent ➢ Call routing facilities such as business rule based routing, skills-based routing etc.
23.	Supervisor Module - The call centre should provide a graphical console application program for the supervisor's workstation. This position shall facilitate the following features:- i. Any supervisor shall be able to monitor or control any group in the call Centre ii. It shall show the live activity of each agent in details as well as in a summarized fashion including information like total number of calls received, calls answered, average response time etc. iii. Supervisor console shall also graphically display live status of the call session summary, number of call waiting in the queue, call traffic etc. iv. Live status of the group shall be shown, including waiting calls and calls being answered currently. v. Access to the supervisor console shall be restricted. vi. It shall be possible for a supervisor to attend calls whenever necessary.
24.	Reporting: i. System to provide report of IVR Application Performance Analysis, Call by Call details for all the calls, Traffic analysis reports etc. ii. Reporting platform to support Agent level reports, Agent login, logout report, report on agent state changes iii. Queue reports, Abandon call reports all the reports should be summary, tabular and detailed report format to be available for the agents. iv. Reporting platform to support custom reports using a combination of the Crystal Reports Developer's Toolkit and SQL stored procedures. v. 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.
25.	Solution should offer audit trail with the following features -

	i. Solution should have a comprehensive audit trail detailing every user activity including system/security administrators with before and after image ii. Audit trails presented by the system shall be very detailed with all the related fields, such as User ID, time log, changes made before and after, Machines ID etc. iii. It shall have the facility to generate security report(s) and audit the whole process from logs reports at any future date. The system shall have complete audit trail of any changes to the system e.g. alert generated, system configuration etc. iv. System shall not allow audit log to be deleted and any attempts to delete must be logged. v. System shall have at a minimum following standard reports: ➢ List of users, user privileges and status ➢ User sign-off and sign-on ➢ User violation – unsuccessful logon attempts ➢ User additions, amendments and deletions with before & after image

5.1.4. Functional & Technical Requirements for Video Display Wall

Sr.No	**Parameters**	Minimum Technical Requirements
1	**Configuration**	Video Wall cubes of 70"(± 5 %) diagonal in a 5(C) x 2(R) configuration complete with base stand
2	**Cube & Controller**	Cube & controller, Software should be from the same manufacturer
3	**Native Resolution**	Full HD (1920x 1080)
4	**Light Source Type**	Laser light source using Direct RGB laser diode with a life time of 100000 hrs.
		Individual cube should be equipped with multiple laser banks and each laser bank should have an array of diodes. Single or multiple diode failure should not impact image display on the screen
5	**Brightness of Projection engine**	1600 Lumens or better
6	**Brightness of Cube**	Minimum 500nits and should be adjustable for lower or even higher brightness requirements
7	**Brightness Uniformity**	≥ 95 %.Automatic and continuous calibration system should be provided to maintain uniformity in color and brightness using integrated color sensor or equivalent
8	**Dynamic Contrast**	1000000:1 or more

9	**Dust Prevention**	Should be designed to prevent dust entering into the engine
10	**Heat dissipation**	390 BTU/Hr (Eco Mode)
11	**Pixel clock**	330 MHz
12	**Control**	IP based control to be provided
13	**Remote**	IR remote control or IP based control should also be provided for quick access
14	**Screen to Screen Gap**	Less than 0.2mm Gap between 2 screens
15	**Screen Support**	screen should not be expanding or shrinking due to variations in humidity and temperature or any other climatic conditions
16	**Control BD Input terminals**	Minimum one port of each DVI, HDMI, Display Port. All ports should be future ready to take 4HD input
17	**Power Consumption**	Power Consumption for each VDU/Rear Projection Modules should be less than 150 Watts
18	**Power Supply**	Redundancy should be provided for Power supply.
19	**Cooling Inside Cube**	Any advanced cooling mechanism
20	**Cube Depth**	700mm or less
21	**Source Redundancy**	Redundancy should be provided for DVI Inputs
22	**Maintenance Access**	Cube should be accessible from the front/rear side for maintenance.
23	**Cube control &Monitoring**	Video wall should be equipped with a cube control & monitoring system. It should provide options to view remotely on remote devices such as mobile, laptop, etc through IE.
		Should be able to control & monitor individual cube, multiple cubes and multiple video walls
		Should provide a virtual remote on the screen to control the video wall
		System should have a quick monitor area to access critical functions of the video wall

		User should be able to add or delete critical functions from quick monitor area
		User should be able to define the error messages as informational, serious or warning messages
		Automatically notify the error to the administrator or user through a pop up window and email
		Status log file should be downloadable as per user convenience
24	**Sharing & Collaboration**	It should be possible to share the layouts over LAN/WAN Network with Display in Meeting room or on Remote Workstations connected on LAN/WAN Network

5.1.5. Functional & Technical Requirements for Video Wall Controller

Sr.No	Parameters	Minimum Technical Requirements
1	Functionality	The Controller should be able to make all the 10 cubes behave as one logical area. It should be possible to display any or all the inputs on the video wall in any desired configuration. Should be possible to increase the number of inputs if desired at a later stage
2	Architecture	Should be based on Server architecture/Distributed architecture
3	Operating System	Windows 10 /others (-64 bit)
4	RAM	16GB or higher
5	HDD	1 TB or higher
6	RAID	RAID should be provided
7	Chip	Intel Xeon or better
8	Power Supply	Dual Redundant Power Supply
9	Outputs	32 DP/DVI outputs to the cubes
10	Inputs	6 DVI Inputs, Dual LAN
11	Chassis	19" rack mount industrial chassis
12	Wall Management Software	Software to be provided to manage the layout on the display. Should be able to record the video wall screen .Can use proven technology from the market

5.1.6. Functional & Technical Requirements for Monitoring Workstations

S.N	Parameters	Minimum Technical Requirements
1	Processor	Latest generation 64bit, 3.4 Ghz, 8 Core Xeon or better Processer with Intel C612 or latest chipset
2	Motherboard	OEM Motherboard
3	RAM	Minimum 16GB DDR4 RAM expandable to 128 GB
4	Graphics card	Minimum Graphics card with 2 GB video memory (non-shared) with 3 HDMI/mini display ports for connecting three different monitors simultaneously.
5	Monitor	Three Monitors of 24" Curved TFT LED, with Minimum 1920 x1080 resolution, Minimum input of 1xDP, 1x HDMI, Energy star 5.0/BEE star certified
6	HDD	Min. 1 TB Hard Drive@7200rpm
7	Other Accessories	Line/Mic IN, Line- out/Speaker Out (3.5 mm), Minimum 6 USB ports (out of that 2 in front), 104 keys minimum OEM keyboard, USB Optical OEM mouse,
8	PTZ joystick controller	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
9	Operating System	Pre-loaded Windows 10 (or latest) Professional 64 bit, licensed copy All Utilities and driver software, bundled in CD/DVD/Pen-drive media.
10	Antivirus feature	Advanced antivirus, antispyware, desktop firewall and encryption as required.
11	Network Interface Port	1G Port

5.1.7. Functional and Technical Specification of PTZ Joy Stick

S.No.	Minimum Technical Requirements
1	The Digital Keyboard (Joystick) shall be fully functional, multipurpose keyboard used for controlling of connected PTZ Camera.
2	Digital Keyboard shall include an integral variable speed Pan/Tilt/Zoom joystick and shall be able to select PTZ Camera.
3	Digital Keyboard shall support RS-232/RS-485 or Ethernet or USB port connectivity and shall be supplied along requisite interface units.
4	The Digital Keyboard (Joystick) should be ONVIF compliant and supports all features/ functionality of the VMS and NVR.

5.1.8. Functional and Technical Specification of LED Display (55 inches)

S. No.	Parameter	Minimum Specification
1.	Technology	LED Based
2.	Screen Size	Minimum 55 inches diagonally
3.	Resolution	Full high definition (1920 x 1080)
4.	Viewing Angle	150 Degree or better
5.	Input	The display should have one VGA/DVI and one HDMI/DP input
6.	Operations	24x7
7.	Aspect Ratio	16:09
8.	USB	One USB port
9.	Energy Star	5.0/BEE star certified & BIS approved
10.	Certifications	Safety: UL/ cUL / CB / TUV, EMC, FCC / CE.

5.1.9. Functional & Technical Requirements for Desktops

S.No	Parameters	Minimum Technical Requirements
1.	Processor	Intel Core i7-latest generation (3.0 Ghz) or higher
2.	Memory	8 GB DDR4 RAM @ 2400 MHz. One DIMM Slot must be free for future upgrade
3.	Motherboard	OEM Motherboard
4.	Hard Disk Drive	Minimum 1 TB Hard Disk @7200 RPM or higher
5.	Audio	Line/Mic In, Line-out/Speaker Out (3.5 mm)
6.	Network port	10/100/1000 Mbps auto-sensing on-board integrated RJ-45 Ethernet Port
7.	Wireless Connectivity	Wireless LAN - 802.11b/g/n/
8.	USB Ports	Minimum 4 USB ports, including 2xUSB 3.0 Ports
9.	Display Port	Minimum 1 Display Port (HDMI/VGA) port
10.	Keyboard	104 keys Heavy Duty Mechanical Switch Keyboard (USB Interface) with 50 million keystrokes life per switch. Rupee Symbol to be engraved.
11.	Mouse	Optical with USB interface (same make as of desktop)

12.	Monitor	Minimum 21.5" diagonal LED Monitor with 1920x1080 or higher resolution. (Same make as desktop). Must be TCO05 certified.
13.	Operation System and Support	Pre-loaded Windows 10 (or latest) Professional 64 bit, licensed copy All Utilities and driver software, bundled in CD/DVD/Pen-drive media.
14.	Certification for Desktop	Energy Star 5.0 or above / BEE star certified

5.1.10. Functional & Technical Requirements for Ceiling Speakers

S.No.	Minimum Technical Requirements
1.	The ceiling speakers shall have high power with extended frequency responses.
2.	The ceiling speakers shall have wide, controlled constant directivity dispersions for optimum coverage.
3.	The ceiling speakers shall have output of at least 15W peak. They shall have in-built amplifiers or shall be supported by an external amplifier.
4.	The ceiling speakers shall have a conical coverage pattern .
5.	The ceiling speakers shall be in a White colour to match the ceiling and surrounding interior design.
6.	The ceiling speaker shall have a diameter not greater than 8.5".
7.	MSI shall quantify and space speakers to provide full audio coverage within the command centre room and conference room.
8.	The ceiling speakers shall follow the manufacturer recommendation for connectivity.
9.	The Ceiling Speakers shall automatically adjust the output audio level based on ambient noise. This may require either in-built noise sensors with the ceiling speakers or an independent ambient noise monitoring system.

5.1.11. Functional & Technical Requirements for IP Phones

S.No.	Parameter	Minimum Technical Requirements
1.	Display	2 line or more, Mono chrome display for viewing features like messages, directory
2.	Integral switch	10/100 mbps for a direct connection to a10/100BASE-T Ethernet network through an RJ-45interface
3.	Speaker Phone	Yes
4.	Headset	Wired, Cushion Padded Dual Ear-Speaker, Noise Cancelling headset with mouthpiece microphone, port compatibility with IP Phone
5.	VoIP Protocol	SIP V2 VoIP supported
6.	POE	IEEE 802.3af or better and AC Power Adapter (Option)
7.	Supported Protocols	SNMP, DHCP, DNS

S.No.	Parameter	Minimum Technical Requirements
8.	Codecs	G.711, G.722, G.729 including handset and speakerphone
9.	Speaker Phone	Full duplex speaker phone with echo cancellation Speaker on/off button, microphone mute
10.	Volume control	Easy decibel level adjustment for speaker phone, handset and ringer
11.	Phonebook/ Address book	Minimum 100 contacts
12.	Call Logs	Access to missed, received, and placed calls. (Minimum 20 overall)
13.	Clock	Time and Date on display
14.	Ringer	Selectable Ringer tone
15.	Directory Access	Able to integrate with LDAP standard directory
16.	QoS	QoS mechanism through 802.1p/q

5.1.12. Functional & Technical Requirements for CTI System

S.No.	Minimum Technical Requirements
1.	IP based Computer Telephony Integration (CTI) 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
2.	The single IP PBX system should be scalable to support up to 500stations(any mix/percentage of Analog/IP) to achieve the future capacity
3.	The system should be based on server gateway architecture with external server running on Windows / Linux OS. No card based processor systems should be quoted
4.	The voice network architecture and call control functionality should be based on SIP
5.	The call control system should be fully redundant solution with no single point of failure & should provide 1:1 redundancy.
6.	The communication server and gateway should support IP V6 from day one so as to be future proof
7.	The entire solution (IP PBX, its hardware, IP Phones, Voice Gateway, IVR Logger) should be from a single OEM
8.	Support for call-processing and call-control
9.	Should support signaling standards/Protocols – SIP, MGCP, H.323, Q. Sig
10.	Voice Codec support - G.711, G.729, G.729ab, g.722
11.	The System should have GUI support web based management console Security
12.	The protection of signaling connections over IP by means of authentication, Integrity and encryption should be carried out using TLS
13.	System should support MLPP feature
14.	Proposed system should support SRTP for media encryption and signaling encryption by TLS

15.	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
16.	The administrator logging on to the call control server needs to authenticate by suitable mechanism such as User Login Information and Passwords/ Radius Server
17.	Voice gateway to be provided with 3 PRI card scalable to 6 PRI on same gateway in future for PSTN (PRI) line termination.

5.1.13. Functional & Technical Requirements for Video Conf. Unit

S.No	Parameters	Minimum Specifications
1	Protocols	The system should be able to call any H.323 and SIP endpoint directly or indirectly. It should be possible to share content via BFCP and H.239 Endpoint should support the latest video coding standard eitherH.263, H.264, H.265/MJPEG/H.264 Hi Profile or better. It should support Audio coding G.722, G.722.1, G.711, MPEG 4 AAC - LC or LD.
2	Network	Endpoint should support bit rate up to 8 Mbps or more on IP (H.323and SIP) Minimum 2 X Gigabit Ethernet: Should support 10/100/1000 BASET
3	Main Video Resolution	Shall work in high definition video resolution of 1080p @60fps for live video for both Transmit and receive
4	Camera	Codec should support 2 cameras Zoom: Minimum 10x (optical) or better
5	Video Inputs	Minimum 1 HDMI inputs and 1 DVI input for connecting PC / laptop
6	Video Outputs	Minimum 2 x HDMI or similar or better to connect two displays. Additional Outputs are desirable.
7	Audio Inputs	It should support minimum 2 Omnidirectional / Directional Microphones. 2 microphones to be supplied from day one with the system.
8	Encryption	AES 128 bit or more, TLS, SRTP, HTTPS or similar or better
9	User Interface	Intuitive touch panel/Remote Control to operate the entire system

5.1.14. Functional & Technical Requirements for Multiparty Conf. Unit

Functional & Technical Requirements for Multiparty Conference Unit (Video and Audio Conferencing Bridge with Secure VC over Internet)

S.No	Minimum Requirements
1.	The Bridging should be running on the standard Intel servers on standard Virtualized platforms. The hardware, software and virtualization software should be procured.
2.	From day one the bridge must provide 6 full HD video ports @1080p 30 fps and 30 audio conference ports.
3.	All necessary hardware to support the above capacity needs to be supplied from day one. Bridge must have a redundant power supply.
4.	All the ports must be able to connect different sites at different bandwidths and protocols.
5.	H.264 AVC standard must be supported at the minimum to connect all the sites.
6.	The bridge should support room based video end points, users joining from browsers' supporting WebRTC and HTML5 and its own clients. In case additional components are required for this functionality, all additional components required to have this functionality has to be included in the solution.
7.	The bridge should have the capability to host meetings with internal and external participants in a secure way such that it should co-exist with the enterprise security policies.
8.	The bridge should have components such as the Web Server for Web RTC, Scheduler as part of the offering from day one.
9.	Should support H.263, H.263+, H.263++, H.264, H.265, WebRTC video algorithms.
10.	Should support video resolution from SD to Full HD to join into a conference.
11.	Along with the Support for basic algorithms like G.711 and G.722.1 the bridge should also support wideband Audio protocols like MPEG 4 AAC - LC or MPEG 4 AAC – LD.
12.	Must support the ability to allow Video conferencing devices, Clients on Mobile phones, Smart phones and Laptops to join into conference. These clients can be inside the WAN network or even on the Internet without a VPN.
13.	The bridge should support transcoding of different Audio/video Protocols.
14.	The bridge should have H.239/BFCP protocol for sending and receiving dual video streams (Presenter + Presentation).
15.	The bridge must also support advanced continuous presence such that the site that is "on-air" to be seen on a larger window and the other sites are seen in smaller quadrants.
16.	The bridge must be a secure Non-PC Hardware with a strong operating system. The Hardware and software must be from the same OEM.
17.	The bridge should support 128 Bit strong AES encryption for calls and H.235 for authentication.
18.	It should be possible for outside agencies (for State Government, central government, police department, etc.) to join the bridge for multi-party video conference call securely over internet.
19.	They should be able to join the bridge using standards based VC endpoints using internet (as long as these endpoints are exposed to internet) securely.
20.	It should be possible to connect 5 such external endpoints / locations concurrently at any given point of time.
21.	It should use secure firewall traversal technology.

22.	It should support any standards-compliant SIP or H.323 video conferencing endpoints.
23.	It should support for both H.323 and SIP Interworking Encryption and H.323 and SIP Interworking.
24.	It should use standards based firewall traversal methods - H.460.18/19.

5.1.15. Functional & Technical Requirements for Video Conferencing

It is essential requirement of city to connect virtually from various stakeholders and other cities:

a) The VC Room system must support H.323, and SIP standards for communications.
b) The VC Room System must Support High Definition room video up to 1080p60 format (1920x1080 pixels at 60fps progressive) and 720p60. It should also provide a PTZ (Pan, Tilt Zoom) High Definition autofocus camera with automatic exposure and automatic white balance supporting up to the 1080p60 format, a minimum horizontal field of view of 70°, at least a 10x optical zoom and a minimum range for PAN of +/-90° and for TILT of +/- 20°. Camera parameters must be configurable on the VC system user interface, and in particular white balance, back light compensation, exposure compensation, focus and sharpness.
c) The VC Room System must be able to support up to two cameras and two screens, and Support dual video capabilities both in H.323 (H.239) and SIP (BFCP based). Position of content and live video on available displays must be configurable. Optional support up to four cameras in switching mode must be available.
d) The VC Room System must Support the ITU-T standards H.263, H.264, H.264, H.265 High Profile, SVC for video and the ITU-T standards G.711, G.722, G.722.1 Annex C for narrowband, wideband and super wideband audio.
e) The VC Room System must provide full band (20 kHz) audio and support both the ITU standard (G.719) and ISO/MPEG low delay standard (MPEG AAC LD)
f) The VC Room System must Provide up to 2 cascadable 3 microphones digital PODs with each microphone independently echo cancelled
g) The VC Room System must be able to enable/disable the audio on connected displays.
h) The VC Room System must be capable of capturing high definition content from a laptop/PC/DVI source up to 1920x1080 at 60fps.
i) The VC Room System must provide the ability to send/receive simultaneously 1080p60 video on the main channel and 1080p60 video on the dual video channel and be able to display content at full resolution on the second monitor, when available. The user should be able to define the ratio between the bandwidth used for live video and presentation.
j) The VC Room System must Include HD multipoint conferencing capabilities (as option) supporting up to 9 sites in continuous presence. It must provide the capability of handling mixed mode multipoint with H.323 and SIP simultaneously participating terminals, and support for dual video

while in a multipoint session. IP VC DESKTOP and MOBILE multipoint videoconferencing support must be available, eventually with an external server PC.

k) The VC Room System must support embedded AES confidentiality for both room video channel and content video channel simultaneously
l) The VC Room System must Provide security tools for authentication and integrity (for SIP, HTTP Digest MD5 is required; for H.323, H.235 MD5 and HH.235 Annex D procedure I/IA are required).
m) The VC Room System must provide simultaneous support for IPv4 and IPv6, and tools for QoS
n) Double LAN network port for public and private network connection must be available.
o) The VC Room System must provide support for LDAP/H.350 directory services with an embedded LDAP server (local agenda) and LDAP client (in order to access remote LDAP/H.350 servers)
p) The VC Room System must have a WEB interface for management, able to provide snapshots (minimum requirement: local camera view when not in conference).
q) The VC Room System must provide the network administrator management tools to control and administer conferences.
r) The VC Room System must have an API command set. Control code samples for AMX and Crestron platform are desired.
s) The VC Room system must support H.460.18/.19 Firewall Traversal and STUN auto discovery
t) Audio I/O interface of the VC Room System must support both Digital and Analog.
u) Low level administrator tools (Remote Management of the GUI, TCP Dump) are desirable.
v) Monitor wake up features based on standard protocol (CEC) is required.
w) The VC Room System must be able to record the conference (up to 1080p resolution) on a USB Key or Disk. The file must be recorded in a standard format, compliant with common multimedia PC/Mac players.
x) LA control application with a multi-touch interface like the Apple iPad is desired. This interface should enable the user to:

    i. Dial an address with a list of the recent outgoing, incoming or missed calls or Access the company directory and place a call from the directory
    ii. Control the VC Room Camera (PTZ), mute microphone, change volume, set DND, start and stop presenting.
    iii. Inviting another participant by either dialling by address (IP, E.164 or SIP URI) or by accessing the company directory
    iv. Moderate the meeting when connected to a network MCU. When an external MCU is present, moderation includes:

y) Muting any remote participant's audio or video, disconnecting, changing the video layout, displaying information for any participant

z) Receive the H.239 presentation, and allow to browse previously presented slides without disrupting the presenter.

aa) Access the calendar of the VC Room. See what meetings are scheduled with the targeted VC Room, with an easy way to join a meeting from the calendar

5.1.16. Functional & Technical Requirements for Fixed Box /Bullet Cameras

S. No.	Parameter	Minimum Technical Requirements
1.	Video Compression	MJPEG, H.265,H.264 or better
2.	Video Resolution	1920 X 1080
3.	Frame rate	Min. 25 fps
4.	Image Sensor	1/3" Progressive Scan CMOS
5.	Lens Type	Varifocal, C/CS Mount, IR Correction
6.	Lens#	Auto IRIS 8 – 40 mm, F1.4
7.	Minimum Illumination	Color: 0.04 lux, B/W: 0.002 lux
8.	IR Cut Filter	Automatically Removable IR-cut filter
9.	Day/Night Mode	Color, Mono, Auto
10.	S/N Ratio	≥ 50 dB
11.	Auto adjustment + Remote Control of Image settings	Color, brightness, sharpness, contrast, white balance, exposure control, backlight compensation, Gain Control, Wide Dynamic Range should support True WDR-120dB
12.	Audio	Audio Capture Capability
13.	Local storage	Minimum 128 GB Memory card in a Memory card slot and support Automatic Network Replenishment (ANR) feature.
14.	Interoperability	ONVIF Profile S/G (with support for retrieving video stored in local memory card)
15.	Protocol	IPV4, IPV6, HTTP, HTTPS, FTP, RTSP, RTP, TCP, UDP, RTCP, DHCP, UPnP, QoS
16.	Security	Password Protection, IP Address filtering, User Access Log, HTTPS encryption
17.	Operating conditions	0 to 50°C (temperature), 50 to 90% (humidity)
18.	Casing	NEMA 4X / IP-66 rated
19.	Certification	UL, CE/EN,FCC
20.	IR Range	50m or better

5.1.17. Functional & Technical Requirements for Non-IT items

The selected bidder should adhere to the specifications given below for Non-IT components. It is essential that Fire Proof material be used as far as possible and Certification from Fire Department be taken for Command Centre and Office premises before Go-Live.

5.1.17.1. General Standards

The ICOMC interiors shall be state of the art adhering to the various best practices norms for integrated control centres, including:

a) Development of ergonomic reports for the ICOMC covering Human Factors Engineering (HFE), ISO9241 (Ergonomic requirements for office work with visual display terminals - VDTs) and ISO11064 (Ergonomic Design of Control Centres)
b) The proposed interior material should meet to basic control room norms, including but not limited to:
    i. ASTM E84 or equivalent fire norms,
    ii. High scratch resistant surfaces,
    iii. Seismic zone compliance and Green Guard passed Desk for ensuring safe environment for operators.

5.1.17.2. Non -Functional Requirments – Civil and Architectural Work.

The scope of civil works shall include but not limited to the following:

i. Interior design
ii. Pest Control
iii. Permanent walls and partitions (Fire rated)
iv. Temporary removable Partitions (Fire rated)
v. False Ceiling as per specifications
vi. False Flooring as per specifications.
vii. Thermal Insulation
viii. Painting (Fire rated)
ix. Doors (Fire rated)
x. Furniture
xi. Ramp
xii. Glass partitions (fire rated) if required
xiii. Any civil, masonry, trenching and fabrication works required for Electrical installation, Earthing, HVAC installation and other subsystems installations.
xiv. Any other civil works required at site

ICCC Interiors

1. Safety :- Seismic vibrations and Fire safety

2. Ergonomics :- Strict point by point compliance to ISO 11064

3. Sustainability :- Affectivity and longevity (warranty) of the proposed solution

4. Aesthetical appeal :- The entire control room must look aesthetically appealing so that whosoever is coming in the control room is impressed with the beauty.

To ensure that the solution meets the above norms MSI should submit a Certificate from OEM as mentioned below. General compliance / self-compliance shall be deemed unacceptable.

Following paramenters must be taken care for ICCC interiors:

1) Console Desk OEM must be FSC certified manufacturer. OEM should have had FSC Certification from last 2 years. Raw-material supplier certificate shall be deemed un-acceptable.
2) Control desk should be seismic zone 5 tested.
3) Copy of Test certification of ASTM E84 (from UL/Intertek) for control desk worksurface to ensure fire safety. Test must reference the actual assembled components for wood-core panels including core, laminates, edging. Raw-material supplier certificate shall be deemed un-acceptable.
4) The shutter (Front & Back shutters) tile shall be ASTM E-84 (UL/intertek certified only) for surface burning characteristics. Raw-material supplier certificate shall be deemed un-acceptable.
5) For Control room interiors Wood, laminates, Gypsum, POP and paint shall be deemed unacceptable to ensure 10 year's maintenance free working environment.
6) Wall Panelling and Ceiling tiles must be Class A fire rated certified for surface burning characteristics as per ASTM e84 (from UL/Intertek). This is mandatory to ensure that the materials used in the interiors do not provoke fire. Certificate to be attached with the bid.
7) Wall Panelling and Ceiling must be seismically tested & certified for Zone 5 Vibrations. Valid report from government approved test lab to be enclosed with the bid.
8) Control Room Interiors must be Greenguard certified (from UL/Intertek) to reduce health hazardous because of interior finishes.
9) To ensure the quality of the execution and integrity of the components it is mandatory for the main bidder that they get some qualified agency with experience of designing & execution of minimum 5 control command room interior projects with desk.
10) To ensure uniformity, consistency & quality in final product the desk manufacturer should have in-house powder coating plant, metal manufacturing & wood manufacturing plant.

For Control Room :-

i) Control Desk, Ceiling and Wall Paneling, must be tested and certified for Seismic Zone 5 vibrations. Valid test report from Government approved research institute must be submitted along with the technical Bid for project level approval.

ii) For operators' health :- Green-guard certified control room interiors from UL/Intertek to ensure healthy working environment for operators. A valid certificate/report need to be submitted along with the technical Bid.

iii) RoHS (Restriction of Hazardous Substances) certified ceiling, wall paneling & Control desk to ensure restriction of hazardous substance.

Control Desk design must take care of the following:-

i) ASTM E84 or BS2D0 certificate (From UL/intertek) to be submitted along with the technical Bid. Copy of Test certification for ASTM E84 (from UL/Intertek) for the surface burning characteristics of products and materials. Test must reference the actual assembled components for wood-core panels including core, laminates, edging. Raw-material supplier data alone is not acceptable.

ii) High scratch resistant laminate table top for surfaces with ANSI/NEMA LD3 certification.

iii) The Desk manufacture must be FSC certified. The manufacture must have had this certification from last two year as a concern towards environment.

Finishing and Work surface:-

i. The material of the working surface should be minimum 25 mm thick MDF with High Pressure scratch resistant NEMA LD3 certified Laminate finish.

ii. Edging Option :- Front ergonomic edge (MINIMUM 55mm DEPTH) shall be of injection molded Polyurethane(PU) on profiled wood core which gives cushion/comfort to wrist/palm during working hours. Sample of Injection Molded PU Edging on profiled wooden core to be produced for technical approval prior to opening of commercial bid.

Following should be the properties of the Control room False Ceiling:-

1. Fire Safety :- The proposed system has Class A fire rated tiles as per ASTM E84 to ensure safety against fire.

2. Seismic Safety :- The entire structure is seismically tested and qualified for Zone 5 vibrations. The design complements the overall control room design.

3. Acoustics :- The tiles are designed to provide acoustics and ensure that no echo is generated in the control room. Ceiling has acoustical properties as the perforated tiles have 0.6 NRC.

4. Durability:- Must not get damaged because of A/C condensation or unlikely event of water seepage.

5. Aesthetics: Metal ceiling have better acoustic properly as compared to gypsum.

6. Quality:-Quality in Manufacturing :- Proper laser cut outs shall be provided for proper installation of the ceiling lights.

7. Quality Workmanship :- All the panels are cut on laser so that desired clip in profile is obtained for quick and perfect installation at site. Human installation errors are almost reduced to zero with such manufacturing practices.

8. Aesthetics :- Unlike normal offices the False ceiling of the CCRs must be designed to suit the CCRs aesthetical/functional, safety and ergonomic requirements.

The Control Room must be aesthetically appealing hence following designer specifications are recommended for normal control room area with wide variety of colours.

Floor finish / False flooring system

1. Unlike normal conventional false floors, the floors have to be provided with calcium silicate floor tiles which shall have acoustic laminate on the top. Calcium silicate floors are resistant to fire.

2. The top finish material must be bio-degradable, acoustical in nature and must not emit any harmful VOCs, should be durable in nature and resistant to scratches.

3. Top finish of acoustic Laminate must reduce impact sound by 14dB (ISO 717-2)). It shall be twin layer linoleum built up from 2 mm acoustic laminate.

Unlike normal offices the False ceiling of the Command and Control Room must be designed to suit the Control Rooms' aesthetical/functional, safety and agronomical requirements.

Ceiling tiles should be designed to provide acoustics and ensure that no echo is generated within the control room.

Partitions & Panelling

The vertical wall cladding/finishes and room partitions must add value to the control room in terms of:-

- Functionality (Achieving Acoustings & reducing Echo),
- Sustainability (Maintenance Free Environment),
- Safety(against fire and seismic vibrations),

Easy Up-gradation (for accommodating future technologies without any civil work (like increasing the number of Large Video Screens, access the cable ducts for any new equipment introduced at a later stage) etc.

Aesthetics : The control room being the Core Activity area/heart of any controlling/monitoring activity, hence it is recommended that it is designed to have World Class feel.

All the Civil works are to be carried out as per the layout diagram as shown at Annexure 2.

a) Civil Interiors:

Providing and constructing 200 mm thick Light Weight Concrete Block Masonry (Spore or equivalent make) in proper line and level, at all levels in cement mortar 1:4 using standard size of blocks of thicknesses as given below, including all scaffolding, staging, curing, all lifts, raking of joints, all labour, hire and fuel charges for all tools and plants employed etc. complete and as directed. Provision of Concrete Binders in proportion 1:2:4, 75mm thick reinforced with 2 nos. of 8 mm dia Fe 415 bars, RCC binders to be at every 1 metre interval from floor level inclusive of reinforcement and formwork, cover blocks for reinforcement etc., closing the gap between the masonry and RCC beam and slab finished to required slope. The width of the joints not to exceed 10mm.

b) FALSE FLOORING:

Providing and fixing Access floor systems of Preferred/ standard make confirming to EN12825 or equivalent standards. The Access floor system to be installed shall be of finished floor height of 600 mm from the existing floor level comprising of 600mm x 600mm square panels. The system will provide for suitable pedestal and under-structure designed to withstand various static loads and rolling loads subjected to it in server / rack area. The entire Access floor

system will provide for adequate fire resistance, acoustic barrier and air leakage resistance. At least 4 nos. of lifting suction devices to be provided. The raised floor must be capable of withstanding a uniform distribution load of 1200Kg/Sq. M.

c) VITRIFIED FLOORING FOR AREA NOT COVERED WITH RAISED FLOOR:

Providing and laying approved make and quality vitrified polished tiles 600x600mm size flooring to match floor pattern using BAL adhesives and laid to corrected level of +/-6mm and joints pointed with approved quality jointing compound including curing.

d) FLOOR INSULATION:

i. Providing and fixing 16 mm or 13 mm thick Nitrile rubber floor insulation below the false flooring and joints should be finished properly as per manufacturer's specification. The rate shall be inclusive of jointing tap, cleaning the surface to make it free from dust.
ii. Ramp: 2.5 mtrs x 2.9 mtrs ramp with MS Supports, with 1.5 Ton Load bearing capacity, with Anti-skidding sheet.

e) MODULAR GRID CEILING:

iii. Providing and fixing of Armstrong or Equivalent Mineral Fibre board 16mm thick and 600mm x 600mm Dune RH 99 tile with Micro look edge in true horizontal level suspended on locking Armstrong Grid system made of Hot Dip Galvanized steel section powder coated as per manufacturers specification including making opening for electrical & air conditioning fitting complete as directed. The tiles are to be installed on Armstrong 15 mm grid system having fire rating of 60 minutes as per BS 476 / 23 of 1987 with following properties : Noise Reduction. Co-efficient (NRC) of 0.50, Sound Attenuation of 32 db., Light Reflectance of 83%, Thermal Conductivity K-0.052 -0.057 W/moK Weight of 4.0 kg/m2 and Humidity Resistance of RH - 99.
iv. Erection of false ceiling with lay in tile system with Aluminium Coil coated Grade 3003 of 600 x 600 x 9mm depth and 0.7mm thick tile to meet NRC 0.7 of USG Panz or approved equivalent; MICRO PERFORATED of 1.5 mm dia in a 3mm diagonal square pattern given 22% perforated area in correct line and levels and as per specification, approved drawings and design submitted. All tiles edges to be compatible with design of grid as per architects specifications.

f) GYPSUM BOARD CEILING:

Providing and fixing in position gypsum board false ceiling with approved G.I Frame work and hangers including painting, openings for lights, border design at no extra cost etc. as per specification and description etc. complete.

g) PUNNY FINISH:

Existing wall to be finished in POP / Gypsum Plaster, smooth finish to take on paint.The average thickness of punning to be considered 20mm thick.

h) PAINTING:

To prepare & finish 3 coats of acrylic emulsion paint of approved quality & shade by sand papering the surface, applying one coat of primer, prepare the surface with two coats of full putty, sand papering again, repeating a coat of primer, applying one coat of plastic emulsion paint, touching up with putty & applying two final roller coats of plastic emulsion paint, to internal wall/ceilings masonry concrete surfaces incl. preparing the surface by cleaning scrapping, smooth filling crevices, scaffolding etc.

i) FIRE RATED PAINT (WALLS):

i. To prepare & finish the wall with fire rated paint of approved quality & shade by sand papering the surface, applying one coat of primer, prepare the surface with two coats of full putty, sand papering again, repeating a coat of primer, applying one coat of paint, touching up with putty & applying two final roller coats of fire rated paint, to internal wall/roof slab masonry concrete surfaces incl. preparing the surface by cleaning scrapping, smooth filling crevices, scaffolding etc. (columns and gyp boxing over the windows of the data centre included).
ii. 75MM THK FULL HEIGHT GYP PARTITION -25MM X 32MM Al framework, at every 600mmx 600mm spacing, vertically/horizontally, extended to the nearest structural members (continuing up to slab level), partition to have 75mm high Al skirting screwed onto the partition. Solid partition on both sides covered with 8mm ply & 12mm Gypsum.
iii. Framework to be continued up to the slab level and clad with gyp on. Necessary cut-outs for services to be provided as per the markings and to be sealed properly, inclusive of painting. (Additional reinforcement/backing to be provided to partitions that need to support plasma TV etc.) Partition as described above to be finished in paint on one side and laminate on the other with 75mm ht laminate skirting at the bottom with 6mm groove above the skirting.

j) GLAZED PARTITIONS:

i. 10 mm thick, toughened glass partition fixed to the floor with aluminium C-channel and to the false ceiling with concealed beading/equivalent to cater for fire and seismic requirements.
ii. COLUMN CLADDING: 3mm (Aluminium Panel)
iii. Fire rated doors as per specifications: Single leaf fire rated doors as per specification, of Size 1000 mm x2400 mm with 200 mm x 300 mm vision panel made of 2 hr fire rated glass, high quality heavy duty door closer etc.
iv. Glass doors: Double leaf glass door of Size 2000 mm x2400 mm with necessary accessories.
v. Glass doors: Single leaf glass door of Size 1000 mm x2400 mm with necessary accessories.

k) Miscellaneous – MSI has to work out the exact requirement as per given building layouts at Annexures.

i. Furniture
ii. Reception Table

iii. Meeting Table
iv. Security table
v. Chairs
vi. Metal Detector
vii. Fire Vault
viii. Baggage Scanner
ix. Printer (A3,A4) Scan and copier

5.2. ICT Infrastructure Components

5.2.1. ICT Hardware Components for Data Centre

5.2.1.1. Functional & Technical Requirements for Core Router

S.No.	Minimum Technical Requirements
1	**Architecture**
1.1	Router shall have Modular and distributed architecture, chassis based
1.2	Router shall have redundant management module or switching fabric.
1.3	Router shall have minimum 4 additional open slots in chassis (without any additional adaptor/module) apart from the Management/supervisor module slot
1.4	Shall be based on multi-core, multi-threaded processor
1.5	Shall have distributed forwarding architecture
1.6	The router shall be 19" Rack Mountable
1.7	Router Shall have minimum 8 nos. of 1G SFP ports & 8 x10G SFP+ ports populated with appropriate transceivers as per solution/ design.
1.8	Router shall have 8 x 1G SFP Ports in addition to S. No. 1.5 with populated with appropriate transceivers as per solution/design.
1.9	Shall have up to 1Tbps backplane Bandwidth with redundant switching fabric
1.10	Shall have minimum 70 Million packets per second and scalable up to 120Million packets per second in future
1.11	Console port, Auxiliary port/USB port/Management Port and Compact flash slots
1.12	Shall support various types of interfaces like 1G Ethernet, high-density 10 GbE WAN interface options.
1.13	Router shall have the sufficient free open slot for future scalability of 4 nos. of 10G SFP+ interface module
2	**Reliability Features**
2.1	Shall have dual routing processor/Management modules with 1:1 redundancy
2.2	Shall have redundant power supply (internal)
2.3	The Router shall support to connects multiple routers through physical ports to achieve system virtualization. All routers appears as one node on the network to allow for simplified configuration, while achieving high resiliency and increased system expandability
2.4	Support hot-swapping of interface cards, routing processor modules, power module and fan tray
2.5	VRRP/VRRPv3
2.6	MPLS TE FRR
2.7	IGP fast routing convergence
2.8	BFD: supporting collaboration with Static route/ RIP/OSPF/ISIS/ BGP/ VRRP/TE FRR
2.9	Graceful Restart: OSFP/BGP/IS-IS/ LDP/RSVP
2.10	Unified Modular operating system provides an easy to enhance and extend feature which doesn't require whole scale changes
3	**Layer 2 protocols**
3.1	ARP: Dynamic/static ARP, proxy ARP, gratuitous ARP
3.2	Ethernet, sub-interface VLAN
3.3	QinQ terminating

S.No.	Minimum Technical Requirements
4	**IP services & IP Routing (any software/license required to enable these features shall be provided from Day 1)**
4.1	TCP, UDP, IP option, IP unnumbered
4.2	Policy-based routing
4.3	Static routing
4.4	Dynamic routing protocols: RIPv1/v2, OSPFv2, BGP, IS-IS
4.5	Route recursion
4.6	Routing policy
5	**IPv4 multicast (any software/license required to enable these features shall be provided from Day 1)**
5.1	IGMP (Internet Group Management Protocol) v1/v2/v3
5.2	PIM-DM, PIM-SM, PIM-SSM
5.3	MSDP (Multicast Source Discovery Protocol)
5.4	MBGP
5.5	Multicast routing
6	**Network protocols**
6.1	DHCP Server/Relay/Client
6.2	DNS Client
6.3	NTP Server/Client
6.4	Telnet Server/Client
6.5	TFTP Client
6.6	FTP Server/Client
6.7	UDP Helper
7	**IPv6 Features (any software/license required to enable these features shall be provided from Day 1)**
7.1	Basic functions: IPv6 ND, IPv6 PMTU, dual-stack forwarding, IPv6 ACL
7.2	Static routing
7.3	Dynamic routing protocols: RIPng, OSPFv3, IS-ISv6, BGP4+
7.4	IPv6 multicast:MLDv1/v2,PIM-DM,PIM-SM,PIM-SSM
8	**MPLS Features (any software/license required to enable these features shall be provided from Day 1)**
8.1	L3VPN: Inter-domain MPLS VPN (Option A/B/C), nested MPLS VPN, Hierarchy PE (HoPE), CE dual homing, MCE, multi-role host, GRE tunnel
8.2	L2VPN: Martini, Kompella, CCC, and SVC
8.3	MPLS TE, RSVP TE
8.4	Multicast VPN
9	**QoS**
9.1	Traffic classification: based on port, MAC address, IP address, IP priority, DSCP priority, TCP/UDP port number, and protocol type
9.2	Traffic policing: CAR rate limiting, granularity configurable
9.3	Rate limiting based on source/destination address (supporting subnet-based rate limiting)
9.4	Priority Mark/Remark
9.5	Queue scheduling mechanism: FIFO, PQ, CQ, WFQ, RTPQ, CBWFQ
9.6	Congestion avoidance algorithm: Tail-Drop, WRED
9.7	MPLS QoS and IPv6 QoS
9.8	HQoS/Nested QoS
10	**Security**

S.No.	Minimum Technical Requirements
10.1	ACL and ACL acceleration
10.2	Time-based access control
10.3	Packet filter firewall
10.4	TCP attack prevention on local host
10.5	Control panel rate limiting
10.6	Virtual fragment reassembly
10.7	URPF
10.8	Hierarchical user management and password protection
10.9	AAA
10.10	RADIUS &TACACS
10.11	PKI Certification
10.12	SSH v1.5/2.0
10.13	RSA
10.14	IPSec, IPSec multi-instance, IKE
11	**Management & maintenance**
11.1	Configuration through the CLI, console, Telnet
11.2	Dial up configuration and remote maintenance
11.3	SNMP (v1, v2c, v3), RMON (group 1, 2, 3 and 9 MIB)
11.4	System logs, Hierarchical alarms
11.5	Ping and Traceroute
11.6	Network Quality Analysis, supporting collaboration with VRRP, policy- based routing, and static routing
11.7	Fan detection, maintenance, and alarm
11.8	Power supply detection, maintenance, and alarm
11.9	CF card detection, maintenance, and alarm
11.10	Temperature detection, alarm
11.11	Dual images
11.11	Loading/upgrading through FTP, TFTP
12	**Other Services**
12.1	Shall support Connection limit
12.2	Shall support NetStream/Slow/Netflow/equivalent
13	**Regulatory Compliance**
13.1	Router shall conform to UL 60950 or IEC 60950 or CSA 60950 or EN 60950 Standards for Safety requirements of Information Technology Equipment.
13.2	Router shall conform to EN 55022 Class A/B or CISPR22 Class A/B or CE Class A/B or FCC Class A/B Standards for EMC (Electro Magnetic Compatibility) requirements.

5.2.1.2. Functional & Technical Requirements for Internet Router

S.No.	Minimum Technical Requirements
1	**Architecture**
1.1	Router shall have Modular architecture with two slots for WAN modules
1.2	Shall be based on multi-core processor
1.3	The router shall be 19" Rack Mountable
1.4	Router Shall have minimum four Dual personality Gigabit Ethernet ports (Copper or SFP) and 2 x 10G SFP+ Ports. All SFP/SFP+ ports populated with appropriate transceivers as per solution/design.
1.5	Shall support 1G SFP, 1000 Base-T interface
1.6	Shall have 80 Gbps full duplex Routing capacity
1.7	Shall have to support up to 15 Mpps packet forwarding rate
1.8	Console port, Auxiliary port, USB port and Compact flash slots
1.9	Router shall have Min. 1 no. free open interface slot for future scalability of WAN/LAN interface module
2	**Reliability Features**
2.2	Shall have dual hot swappable redundant power supply
2.3	Shall support hot-swapping of interface cards, power module and fan tray
2.4	VRRP/VRRPv3
2.5	MPLS TE FRR
2.6	IGP fast routing convergence
2.7	BFD: supporting collaboration with Static route/ RIP/OSPF/ISIS/ BGP/ VRRP/TE FRR
2.8	Graceful Restart: OSFP/BGP/IS-IS/ LDP/RSVP
2.9	Software hotfix
3	**Layer 2 protocols**
3.1	ARP: Dynamic/static ARP, proxy ARP, gratuitous ARP
3.2	Ethernet, sub-interface VLAN, VLAN/Voice VLAN/Super VLAN/VLAN Mapping
3.3	QinQ terminating
4	**IP services & IP Routing**
4.1	TCP, UDP, IP option, IP unnumbered
4.2	Policy-based routing
4.3	Static routing
4.4	Dynamic routing protocols: RIPv1/v2, OSPFv2, BGP, IS-IS
4.5	Route recursion
4.6	Routing policy
5	**IPv4 multicast**
5.1	IGMP (Internet Group Management Protocol) v1/v2/v3
5.2	PIM (Protocol Independent Multicast) DM/SM
5.3	MSDP (Multicast Source Discovery Protocol)
5.4	MBGP
5.5	Multicast static routing
6	**Network protocols**
6.1	DHCP Server/Relay/Client
6.2	DNS Client
6.3	NTP Server/Client
6.4	Telnet Server/Client

S.No.	Minimum Technical Requirements
6.5	TFTP Client
6.6	FTP Server/Client
6.7	UDP Helper
7	**IPv6 Features**
7.1	Basic functions: IPv6 ND, IPv6 PMTU, dual-stack forwarding, IPv6 ACL
7.2	IPv6 tunnel: manually configured IPv6 tunnel, configured IPv6 over IPv4 tunnel, automatic IPv6 over IPv4 tunnel, 6to4 tunnel, ISATAP tunnel
7.3	Static routing
7.4	Dynamic routing protocols: RIPng, OSPFv3, IS-ISv6, BGP4+
7.5	IPv6 multicast:MLDv1/v2,PIM-DM,PIM-SM,PIM-SSM
8	**MPLS Features**
8.1	L3VPN: Inter-domain MPLS VPN (Option A/B/C), nested MPLS VPN, Hierarchy PE (HoPE), CE dual homing, MCE, multi-role host, GRE tunnel
8.2	L2VPN: Martini, Kompella, CCC, and SVC
8.3	MPLS TE, RSVP TE
8.4	Multicast VPN
9	**QoS**
9.1	Traffic classification: based on port, MAC address, IP address, IP priority, DSCP priority, TCP/UDP port number, and protocol type
9.2	Traffic policing: CAR rate limiting, granularity configurable
9.3	Rate limiting based on source/destination address (supporting subnet-based rate limiting)
9.4	Priority Mark/Remark
9.5	Queue scheduling mechanism: FIFO, PQ, CQ, WFQ, RTPQ, CBWFQ
9.6	Congestion avoidance algorithm: Tail-Drop, WRED
9.7	MPLS QoS and IPv6 QoS
10	**Security**
10.1	ACL and ACL acceleration
10.2	Time-based access control
10.3	Packet filter firewall
10.4	TCP attack prevention on local host
10.5	Control panel rate limiting
10.6	Virtual fragment reassembly
10.7	URPF
10.8	Hierarchical user management and password protection
10.9	AAA
10.10	RADIUS &TACACS
10.11	PKI Certification
10.12	SSH v1.5/2.0
10.13	RSA
10.14	IPSec, IPSec multi-instance, IKE
11	**Management & maintenance**
11.1	Configuration through the CLI, console, Telnet
11.2	Dialling up for configuration and remote maintenance via Modem through AUX port
11.3	SNMP (v1, v2c, v3), RMON (group 1, 2, 3 and 9 MIB)
11.4	System logs, Hierarchical alarms
11.5	Ping and Traceroute

S.No.	Minimum Technical Requirements
11.6	Network Quality Analysis, supporting collaboration with VRRP, policy- based routing, and static routing
11.7	Fan detection, maintenance, and alarm
11.8	Power supply detection, maintenance, and alarm
11.9	CF card detection, maintenance, and alarm
11.10	Temperature detection, alarm
11.11	Dual images
11.11	Loading/upgrading through Xmodem, FTP, TFTP
12	**EMC & Safety Compliance**
12.1	FCC Part 15 (CFR 47) CLASS A, ICES-003 CLASS A , VCCI-3 CLASS A, VCCI-4 CLASS A, CISPR 22 CLASS A, EN 55022 CLASS A, AS/NZS CISPR22 CLASS A, CISPR 24, EN 55024, EN 61000-3-2, EN 61000-3-3, EN 61000-6-1, ETSI EN 300 386, EN 301 489-1, EN 301 489-17
12.2	UL 60950-1, CAN/CSA C22.2 No 60950-1, IEC 60950-1, EN 60950-1/A11, AS/NZS 60950, EN 60825-1, EN 60825-2, FDA 21 CFR Subchapter J, GB 4943

5.2.1.3. Functional & Technical Requirements for Data Centre Firewall

S.No.	Minimum Technical Requirements
1	The next Generation Firewall should be Appliance based and have inbuilt features Firewall, IPS, Load balancing, QOS, VPN, AV, DPI, Application control for 3000+ applications
2	Support of 60 Gbps Maximum Firewall throughput
3	Support of 12 Gbps NGFW throughput all modules enabled
4	Support of 3000000 or more concurrent connections.
5	Support of 10 Gbps or more IPsec VPN throughput and Support of 10000 or more IPSec VPN Tunnels
6	The firewall should support a minimum of 12x 1G Copper Ethernet interfaces and 6x10G interface and 2x40 G Interface for future
7	For future redeployment flexibility, the firewall shall be a dedicated appliance supporting multi product roles capable of switching between L2FW/IPS/NGFW roles without change of licenses and additional cost.
8	The Firewall should have option for URL Filtering 90+ categories and Cloud sandboxing for malware analysis if required with License upgrade.
9	The firewall shall achieve the following industry recognized security certification standards: Common Criteria EAL4+/NDPP, FIPS 140-2.
10	The firewall must include support for high availability feature - Active-Active Load Sharing or Active-Standby, Stateful failover including VPN connections.
11	The firewall must support high availability clustering within the same HA cluster.
12	The firewall must be a Next Generation firewall that includes features like Application ID, User ID and Intrusion Prevention System (IPS) as basic and not as an add-on license or subscription. The firewall must support Full QoS or DSCP/ToS Throttling with granular QoS configuration per interface and/or individual rule basis
13	The firewall shall support full stack, multilayer normalization and stream-based data inspection and detection processes to detect advanced evasion techniques. The firewall shall include anti-evasion capability.

14	The solution should have separate management console of security policies. The firewall management console should support HA and shall be capable of managing up to 2000 NGFW nodes in future and integration with advance security (Web, Email and DLP console) . The firewall shall offer centralized management with integrated log server, with options to upgrade to multi domain architecture.
15	The firewall shall offer centralized management with integrated log server, with options to upgrade to multi domain architecture. The logs displayed on the firewall management console shall minimally contain the following fields on the same page: Timestamp, Sender (which Firewall sends the log), Geo Location, Source and Destination IP, Source and destination port, Service / Application, User, NAT address / Interface, Client Executable/File/MD5 hash, Rule, Event description, hit counts, action
16	The NGFW should transparently redirect HTTP and HTTPS traffic to a proxy on premises.

5.2.1.4. Functional & Technical Requirements for WAF

S.No.	Minimum Technical Requirementsfor Web Application Firewall
1	The device should be a hardware based appliance with support for redundant power supply
2	The device should provide an overall throughput of min 5Gbps of application layer throughput with 21KB to 44KB packet size and 500,000 concurrent connections. The device should have minimum of 4X 10/100/1000 ports & 2x10G Ports and it should support 6 inline bypass interfaces inbuilt for fail safe operation. The throughput should be sustained to its capacity with WAF enabled and security rules in blocking mode
3	Support for all deployment modes mentioned below: Transparent inline bridge mode(within built fail-open interfaces Transparent reverse proxy mode, Reverse proxy and Passive/promiscuous mode
4	The device should have abuse detection, tracking, Profiling and should support Abuse response and real-time incident management
5	Device should be able inspect HTTP and HTTPS traffic on TCP port 80 &443
6	Should be able to detect attempts to abuse form inputs and establish vectors for injection and cross-site scripting attacks
7	Must protect web application against Cookie Poisoning, cookie injection command injection.
8	Must protect web application against buffer overflow and layer 7 DDOS attacks.
9	Must protect web application against parameter tampering and must have inbuilt controls to block invalid files, filtering of sensitive words in HTTP request and response.
10	Should be able to detect suspicious application errors that indicate abuse including illegal and unexpected response codes.
11	Should be able to detect when an attacker is attempting to request files with suspicious extensions, prefixes and tokens
12	Should support creation of the policies for HTTP/HTTPS headers to ensure critical infrastructure information is not exposed. Response and request headers can be stripped, mixed, or filtered.

13	Should be able to detect and prevent attackers from finding hidden directories, inbuilt security control to limit the action of crawling and scanning
14	Should be able to detect attempts to abuse non-standard HTTP/HTTPS methods such as TRACE.
15	Should be able to detect attempts to manipulate application behaviour through query parameter abuse. Solution must support behaviour analysis to detect and prevent day 0 attacks
16	Should maintain a profile of known application abusers and all of their malicious activity against the application
17	Should enable application administrators to re-identify abusive users and apply persistent responses across sessions
18	Should be able to process SSL traffic using passive decryption or using equivalent technology
19	Should enable administrators to respond to application abuse with session specific warnings, blocks abusive application and undertake additional checks for the same.
20	Block connection and return arbitrary error/custom message
21	Should support network based security controls including ACL's, IP blacklist/whitelist and URL blacklist/Whitelist
22	Sends alert emails when specific incidents or incident patterns Occur
23	Enable command line interface/GUI for custom reporting
24	Should capture, log and display traffic related data to analyse for security incidents.
25	Should enable SNMP system logging and able to send alerts to a centralized EMS solution
26	Should support auditing – Tracks changes to the system made by the administrators in the configuration interface, security monitor and report generation.
27	Should be able to send security incidents via syslog
28	Management: Should support simplified GUI and web-based configuration. Should support web-based monitoring and analysis interface. Should have real-time and historical system monitoring, Should support role based access control.
29	The solution should be leader in Gartner Magic Quadrant since last 3 years.
30	The solution must support custom security rules. Administrators should be able to define rules for the positive and negative security model and to create correlation rules with multiple criteria. This should be possible without need to write any script/code.

5.2.1.5. Functional & Technical Requirements for APT

S.No.	Minimum Technical Requirements
1	The APT appliance should be a purpose built on premise appliance based solution with integrated support for sandboxing. Cloudbased solution will not be accepted.
2	The hardware based solution should provide protection for all incoming and outgoing web and email traffic from/to Internet.
3	Network/Web (2.0Gbps), E m a i l (1000 mailboxes) with 5000 mails per day and End point(1000 Endpoints) APT solution shall perform analysis on-premise and no files shall be sent outside the datacenter network where the same is deployed. It should be based on the throughput supported. All necessary additional devices, licenses required for such configuration should be quoted as part of the solution. The Network / Web solution must be deployed in Inline blocking mode with Hardware bypass built-in. TCP reset is not acceptable form of inline blocking and preferred deployment mode.
4	The APT appliance should be able to process min 1,000,000 files/month (either web or mail or both)
5	Appliance should have minimum 2x1TB storage in RAID 1.
6	Proposed Network & Email APT solution must be running their own sandboxing engine respectively per gateway for each deployed Device .Files should not be submitted from one location to another location for sandboxing for performance reasons. Each sandbox respectively should cater to more than 20 concurrent VM executions. The solution must be able to detect multi-flow web-based attack by executing flows in sandbox environment.
7	Min 4 Copper and 2 x 10G Fiber ports should be provided in APT appliances for achieving functionalities mentioned
8	Minimum one number of 1G Copper ports for management.
9	The Hypervisor used by sandboxing solution must not be an OEM solution such as from VM Ware ,Hyper V, Virtual Box, RHEV etc. however it should be a custom Hypervisor purpose built for sandboxing requirement
10	The solution must be able to detect and report malware by using multiple images of Windows XP, 7, 8 and 10, Mac & Windows Server 2008/12.
11	The solution must support pre-populated LICENSED copies of Microsoft windows and office images through an agreement with Microsoft. There should be no requirement for the customer to buy additional Microsoft licences for sandboxing solution
12	Anti-APT solution should be able to work independently of signature updates from OEM website.
13	The solution must be able to support scanning links inside emails/documents for zero days & unknown malware and support sandboxing of file sizes between 2 Kb and 50 MB. Solution should have an ability to remove all the active content, harmful links in email message/documents and macros sending only a clean document to the end user
14	The solution should inspect the web sessions(HTTP and HTTPS both) to detect and notify the malicious web activity including malicious file downloads through the internet. In case the SSL traffic inspection does not happen through the network APT appliance and a separate device is being provided the same must be a product from recognized OEM . Estimated SSL traffic out of total web traffic should be factored minimum at 80% as per network throughput asked in sizing guidelines.

15	The solution to be provided with complete endpoint detection and response (EDR) solution for at least 1000 endpoints and should work seamlessly with the same.
16	Anti-Apt Solution should be a dedicated solution without any dependency on other solutions for its functioning. The Solution should not be a bolt-on modules (e.g. firewall, IDS/IPS, security gateway, etc.). The capability should not be bundled as a part of an existing UTM or integrated security solution and should be capable of working in standalone mode.
17	The solution must have high efficacy for preventing threats. Vendor must attach the details of Zero Day vulnerability exploits identified by proposed solution technology over last 5 years. This should include publicly disclosed vulnerabilities with reference to applications exploited.
18	The Email APT should be inline solution (MTA mode) and should hold email during analysis and should have ability to quarantine email with malicious attachments, URL's and zero day malwares. Also should have ability to quarantine email with malicious attachments, URL's and zero day malwares.
19	Endpoint APT solution should have zero day exploit detection engine on same agent and can take the action based on activity of payload/executable. Solution should be able to automatically prevent the execution of even unknown executable files even if the endpoint does not have the latest signatures and without heuristics or behavioral patterns.
20	The solution should consolidate (at centralized location) the administration, reporting, and intelligence data sharing intelligence between deployed APT Sensors
21	Perform Full Packet Capture of network traffic of internet links at DC & DR with 1 Gbps capacity each location. It should Index all the data in the packets to simplify navigation across data silos.
22	Packet Forensics solution should enable SOC teams with search-driven data discovery of packet metadata AND content for incident analysis.
23	Solution should have features to perform full reconstruction of assets transferred, accessed and transmitted.
24	Packet Forensics data Storage : 15 days online storage for Raw Packet data on SAN/SAS attached storage and 90 days Indexed Meta data for investigation and reporting purpose.

5.2.1.6. Functional & Technical Requirements for AAA

AAA (Authentication, Authorization and Accounting)

a) AAA network security services provide the primary framework through which a network administrator can set up access control on network points of entry or network access servers, which is usually the function of a router or access server. Authentication identifies a user; authorization determines what that user can do; and accounting monitors the network usage time for billing purposes.

b) AAA information is typically stored in an external database or remote server such as RADIUS or TACACS+. The information can also be stored locally on the access server or router. Remote security servers, such as RADIUS and TACACS+, assign users specific privileges by associating attribute-value (AV) pairs, which define the access rights with the appropriate user. All authorization methods must be defined through AAA.

c) The RADIUS Protocol : The RADIUS protocol carries authentication, authorization and configuration information between a NAS and a RADIUS authentication server. Requests and responses carried by the RADIUS protocol are called RADIUS attributes. These attributes can be username, Service-Type, and so on. These attributes provide the information needed by a RADIUS server to authenticate users and to establish authorized network service for them. The RADIUS protocol also carries accounting information between a NAS and a RADIUS accounting server.

S.No.	Minimum Technical Requirements Authentication, Authorization and Access (AAA)
1	The solution should support AAA, NAC and Guest Access
2	The solution should support 25000 endpoints for AAA from day 1
3	The solution should support 25000 device profiling from day one
4	The solution should be scalable and stable solution to support 2000000 endpoints for AAA in future using additional appliances
5	AAA server should have device profiling functionality for 25000 devices from day 1 to enforce context aware policies.
6	Solution must be Agnostic to existing wired, wireless and VPN network in place today.
7	Shell protected by CLI providing configuration for base appliance settings.
8	Appliance must provide disk or file encryption.
9	Ability to mix and match virtual and hardware appliances in one deployment.
10	Platform must be deployable in out-of-band model and support for clustering with N+1 active redundancy model.
11	Flexibility to operate all features/functions on any appliance in the cluster.
12	Server Cluster must be Upgradeable from the GUI. A single pane which upgrades all the nodes in a cluster
13	Web-based, interface that includes several productivity tools such as a configuration wizard and preconfigured policy templates.
14	Support any type of networking equipment (wired, wireless, VPN) and a variety of authentication methods (802.1X, MAC auth, Web auth).

15	Ability to take advantage of a phased implementation approach by starting with one element of access management (role based) and later incorporating added security measures (endpoint health).
16	Must incorporate a complete set of tools for reporting, analysis, and troubleshooting. Data from access transactions can be organized by customizable data elements and used to generate graphs, tables, and reports. Must correlate and organize user, authentication, and device information together.
17	Solution must have fully integrated support for Microsoft NAP allowing health and posture checks on Windows endpoints without the need to install an agent.
18	AAA server must support both functionality RADIUS server for client device authentication and TACACS+ for network device authentication and logging from day 1.Overlay component can be added to achieve both functionality.
19	The system should provide standard based external facing APIs to extend support and integration with external applications like Ticketing systems, Firewall, IDS/IPS solutions etc
20	The solution Must be an easy-to-deploy hardware platform that utilizes identity based policies to secure network access and includes an integrated set of capabilities bundled under one policy platform:
	• Built-in guest management and device/user on-boarding
	• Web based management interface with Dashboard
	• Reporting and analysis with custom data filters
	• Data repository for user, device, transaction information
	• Rich policies using identity, device, health, or conditional elements
	• Deployment and implementation tools.
21	The solution should support flexible licensing model based on required functionality (i.e. Profile, Posture, Guest Access).
22	The solution should Correlation of user, device, and authentication information for easier troubleshooting, tracking
23	The solution should must allow for the complete separation of Authentication and Authorization sources. For example, authentication against Active Directory but authorize against Local database
24	The solution should support authentication or authorization support for LDAP, AD etc
25	Should support multiple methods for device identification and profiling
26	The solution should support endpoint audit via NESSUS or NMAP scanning
27	The solution should have policy creation tools:
	• Pre-configured templates
	• Wizard based interface
	• LDAP browser for quick look-up of AD attributes
	• Policy simulation engine for testing policy integrity
28	The solution should support incorporation of several contextual elements including identity, endpoint health, device, authentication method & types, and conditions such as location, time, day, etc.
29	The solution should support the following enforcement methods:
	1- VLAN steering via RADIUS IETF attributes and VSAs
	2- VLAN steering and port bouncing via SNMP
	3- Access control lists – both statically defined filter-ID based enforcement, as well as dynamically downloaded ACLs.

	4- Roles Based Access or any other vendor-specific RADIUS attribute supported by the network device.
30	The solution should support Location Based Access
31	The solution should support Time Based Access
32	The solution should able to join multiple Active Directory domains to facilitate 802.1x PEAP authentication.
33	The solution should support complex PKI deployment where TLS authentication requires validating client certificate from multiple CA trust chain. Must also support AAA server certificate being signed by external CA whilst validating internal PKI signed client certificates.
34	Failure of master node should not impact the ability for backup appliances to continue servicing authentication traffic.
35	Must support several deployment modes including centralized, distributed, or mixed.
36	The Policy Management solution should integrate with developed security and operations features like firewalls, MDM/EMM, and SIEM with REST based APIs , Syslog messaging, and deliver end-to-end policy enforcement and visibility from day 1
37	The solution should have Integrated Certificate Authority (CA) provides a complete and secure BYOD support.
38	The solution should support for Single Sign On (SAML 2.0) and O-auth for social logins with Facebook, Twitter, Office365, GoogleApps, LinkedIn from day one
39	The solution should support captive portal customization, and even offers professional, in-house creation from day one
40	The solution should support a wide array of REST/SOAP/XML APIs and protocols that customers can use to integrate their own CRMs, helpdesks, SIEM vendors, admission systems and more from day one
41	The solution should support Cluster deployment provides High Availability (HA) solution with no touch automatic failover from day one
42	The solution should support multivendor solution for network access, supporting over 100 RADIUS vendor dictionaries for ultimate end-user flexibility from day one
43	The solution should consolidates all Policy Manager and license features into a single appliance or cluster
44	The solution should supports Profiling and MDM integration, in the base appliance, to gather endpoint attributes for policy enforcement from day one
45	The solution should support TACACS+ device administration from day one
46	The solution should support SQL as authentication source from day one
47	The solution should support HTTP enforcement (JSON, XML, HTTP payload) from day one
48	The solution should support Advanced Posture Health Classes for Windows and OSX like Disk Encryption, Virtual Machines, USB, P2P apps
49	The solution should support social Network SSO through O-Auth (Facebook, Twitter, Office365, Google Apps, etc.)
50	The solution should have Enhanced capabilities for endpoint compliance and control
51	The solution should supports Microsoft, Apple, and Linux operating systems
52	The solution should support sponsored base Guest Access
53	The solution should support Self Provisioned Guest Access

54	The solution should maintain a list of active visitor sessions
55	Guest solution support a number of options for MAC Authentication and the ability to authenticate devices
56	Guest solution has ability to make changes to a visitor account's session while it is in progress.
57	It should be certified by EAL/NDPP/NIAP or equivalent.

5.2.1.7. Functional & Technical Requirements for Single Sign-On Process

To enhance a secure system login environment, Active Directory Integration/Single Sign-On (SSO) can be enforced, to ensure that users are authenticated to the system with their Windows login credentials.

5.2.1.8. Functional & Technical Requirements for Web Security Appliance

S.No.	Minimum Technical Requirements
1	The solution should provide proxy, caching, on box malware inspection, content filtering, SSL inspection, protocol filtering and inline AV in block mode on the same Appliance. The Solution should be designed for user base in active-active mode managed through centralized management console on server platform. The Solution should provide HA and Load balancing functionality in Secure web gateway solution with or without any dependency on pac, external load-balancer or dns round-robin methods. The solution should have complete license for Antivirus ,SSL, web security and content inspection and control should be built in solution for user base from the first day in same appliance. The Solution should intercepts user requests for web destinations (HTTP, HTTPs and FTP) for web security and in-line AV scanning.
2	The proposed solution should be able to inspect malicious information leaks even over SSL by decrypting SSL natively . The solution should be capable of dynamically blocking a legitimate website which has become infected and unblock the site in real time when the threat has been removed for below mentioned security categories and vulnerabilities.
3	Solution should ensure to provide below mentioned security categories from day1 with automatic database updates for security categories- Advanced malware command and control, Advanced malware payloads, Bot networks, Compromised websites, key loggers, Phishing and other frauds, Spywares. The solution should inspect the sensitive content through pre-defined templates, textual content inside image, cumulative content control and inspection through web channel. The solution should have ability to protect the sensitive data ex-filtration based on geo-location. The solution should be able to scan files, folders, databases and prevent the content from being sent over outbound web channel. The solution should have ability to provide geo-location awareness for security incidents.
4	The solution should have at least 20+ million websites in its URL filtering database and' should have pre-defined URL categories and application protocols along with YouTube, Facebook and linked-in controls. Solution vendor should ensure that 100 predefined categories & 100+ pre-defined protocols should be available on product from day-1. Also in-addition solution should have ability to configure custom categories for organization.

S.No.	Minimum Technical Requirements
5	The solution should have partnerships or third party inputs for web threat ratings from Virus total or Facebook. The solution must detect and block outbound Botnet and Trojan malware communications. The solution must log and provide detailed information on the originating system sufficient to enable identification of infected units for mitigation. The solution should support same policy enforcement in real time policy sync for users even when they access Internet outside the corporate network, this should be enforced through an agent deployment on roaming endpoints ((MAC/Windows) . And this solution should be on premises or with the help of SAAS/OEM Cloud.
6	The agent on the roaming user machines should be tamperproof, for example, the agent cannot be uninstalled by the user even with admin rights to the system or the user cannot stop the services. The solution should have ability to block anonymizer sites or proxy avoidance tools. Below mentioned tools should be blocked from first day and should be provided in default protocol database Ghost surf, Google web accelerator, Hopster, Jap, Real tunnel, Socks online, Tongtongtong, Toonel, Tor, Your freedom.
7	Solution should provide separate Management server which can push policies for centralized management and reporting in case of multiple site solution deployment. Management console should provide automatic policy sync to all the remote boxes when the change is made to central console. Centralized management and centralized reporting console can be appliance based or software server hardware based but no VM should be used for the same.
8	MAC OS X 10.10 and MS Windows 10 support for mobile laptop users web filtering client. The solution should have cloud application usage and associated risk visibility.
9	The solution should apply security policy to more than 100 protocols in multiple categories more than 15. This includes the ability to allow, block, log, and assign quota time for IM, P2P, and streaming media and solution should provide at least below mentioned security categories as below RIGHT FROM FIRST DAY:1)Advanced Malware Command and Control category 2)Advanced Malware payload detection category 3)Malicious embedded links and frame detection category 4)Mobile malware category 5)Key logger and Spyware category 6)P2P software database from day 1 to control/block the below P2P protocols
10	The solution should filter out embedded objectionable or unproductive content, this includes examination of the source server, URL, page content, and active content. The solution should have functionality to control web 2.0 and real time content categorization.
11	The solution should have granular control over popular social web applications like Facebook, Linkedln, Twitter, YouTube, and others. The solution should have social control Video UPLOADS to Facebook and YouTube applications.
12	The solution must provide below mentioned categories or similar to functionally for Facebook control from day 1 Facebook Posting: Facebook function that enables a user to share a post, status or link, Facebook Commenting, Facebook Friends, Facebook Photo Upload, Facebook Mail, Facebook Events, Facebook Apps,Facebook Chat, Facebook Questions, Facebook Video Upload, Facebook Groups etc.
13	The solution should have built-in or custom policies for identifying and segregate You Tube traffic for Education only and Other irrelevant non-compliance video, It should simplify design and implementation of policy to ensure user compliance.

S.No.	Minimum Technical Requirements
14	The solution should provide geo-location awareness for security incidents. The solution should provide inbuilt capability malicious content of password and unknown encryption files.
15	The solution should be able to manage the complete solution through centralized management and reporting console which should be software or appliance based.
16	The solution should support to have capability to differentiate between YouTube educational and entertainment videos through default categories and should have separate default categories for the same.
17	The solution should have authentication options for administration, the specific permissions available depend on the type of administrator and Administrator activity is logged and available for auditing or troubleshooting.
18	The solution should have authentication options for users/groups, It should supports authentication of users via Integrated Windows Authentication (Kerberos), NTLM (NTLM v1 and v2 in Session Security), and LDAP.
19	The solution should have support of multiple domains, the administrators can specify the sequence (Domain controllers checked first, second, next, etc.) used to authenticate users who login from different locations.
20	The solution should supports credential caching (for transparent and explicit proxy) to reduce load on domain controllers.
21	The solution should have Multi-Domain authentication to allow the admin to create rules that authenticate against multiple domain controllers in a sequence
22	The solution should have centralized management for multiple web egress points The solution should support for two factor Authentication for Management Server.
23	The solution should support real time graphical and chart based dashboard for the summary of web filtering activities. The solution should pre-built report templates which the administrator can use for generating reports.
24	The solution should have capabilities to automatically deliver reports based on schedule to selected recipients. The solution should support custom report creation in Excel and PDF.
25	The solution should be able to consolidate reports from multiple boxes for centralized logging and reporting. The solution should provide detailed information on security incidents to comprehensively investigate individual threat events. The solution should be integrated to third-party SIEM applications like syslog/CEF (ArcSight), syslog key-value pairs (Splunk and others), syslog LEEF (QRadar), and Custom. The solution should provide a Web UI to manage Internet usage policies, it should also support delegated administration and reporting capabilities so different roles can be created to manage policies and view reports. The solution should provide native system health monitoring, alerting and troubleshooting capabilities. The solution should provide reports based on hits, and bandwidth.
26	The solution should support configuring scheduled automatic backup of system configuration. The solution should support automatic download of available patches or fixes. The Solution should have inbuilt reporting feature like real time monitoring, reporting templates and investigation drill down report. The solution should have reporting on the user agent strings of applications to provide details on application usage and version details including browser version reports. The solution should be able to block back channel communication of sensitive data through default 1500 templates. The solution should have visibility and control for cloud applications and shadow IT application usage. The OEM should have own TAC centre in India.

S.No.	Minimum Technical Requirements
27	The solution should support server message block (SMBv2) for better security for authentication.

5.2.1.9. Functional & Technical Requirements for DLP

S.No.	Minimum Technical Requirements
	Network Data & Cloud Monitoring and Prevention
1	The solution should detect and prevent content getting posted or uploaded to specific websites, blogs, and forums accessed over HTTP, HTTPS. The solution should be able to enforce policies by URL's, domains or URL categories either natively or by integrated Web Security solution. The solution should be able to monitor FTP traffic including fully correlating transferred control information and should be able to monitor IM traffic even if its tunnelled over HTTP protocol.
2	The DLP Solution must have capability to integrate with 3rd party Proxy solution for content inspection using ICAP channel or must have DLP engine on OEM provided Proxy itself.
3	The solution should be able to block outbound emails sent via SMTP if its violates the policy.
4	The proposed solution work as a MTA to receive mails from mail server and inspect content before delivering mails to next hop and should quarantine emails that are in violation of company policy.
5	The solution should be able to prevent content getting posted or uploaded to destinations (Web, Email domains etc.) and should monitor and control sensitive emails downloaded to mobile devices through ActiveSync.
6	The solution should support Email DLP deployment in Microsoft Azure for Office 365. All licenses required for the same should be included and management should be from the same centralized management platform.
7	The solution should be able to identify data leaked in the form unknown and kwon encrypted format like password protected word document. The solution should be able to identify malicious traffic pattern generated by Malware infected PC in order to prevent future data leakage by the malware. The solution should support quarantine as an action for email policy violations and should allow the sender's manager to review the mail and provide permissions for him to release the mail without logging into the UI.
8	The DLP Solution must natively integrate with Cloud solutions like One Drive as well as Box to monitor uploads as well as sharing of data from different assets connected outside the organization. This must be outside endpoint DLP solution.
	Endpoint Data Monitoring & Protection
9	The solution should have more than 50 pre-defined applications and multiple application groups and allow each application/application group to monitor operations like Cut/Copy, Paste, File Access and Screen Capture or Download. Also solution should have the capability to define the third party application. The solution should be able to define the policies for the inside and out of office endpoint machines. The endpoint solution should have capabilities to monitor applications and ensure unauthorized applications do not have access to sensitive files. The endpoint solution should be able to perform discovery only when the endpoint is connected to external power or Machine is Idle.

S.No.	Minimum Technical Requirements
10	The solution should be able to monitor data copied to network file shares and should enforce structured and unstructured fingerprint policies even when disconnected from corporate network. The endpoint would be able to store both structured and unstructured fingerprints on the endpoint itself and should perform all analysis locally and not contact and network components to reduce WAN overheads. The solution should be able to enforce different policies for desktops and laptops.
11	The solution should Provide "Cloud Storage Applications" group which monitor sensitive content accessed by these cloud storage application on the endpoint and prevent sensitive data from uploading to the cloud. For Example (Should support from day 1(Windows 10 and MAC OSX 10.11) -Amazon Cloud Drive, Box, Drop box, Google Drive, Sky Drive, iCloud.
12	The endpoint solution should Blocking of non-Windows CD/DVD burners, it should also Inspect and optionally block Explorer writes to WPD class devices. The endpoint solution should encrypt information copied to removable media. It Should support both Native and Portable Encryption and manage the Encryption and DLP policies from the same management Console.
13	Endpoint solution should support win 32 and 64 bit OS, Mac & Linux OS, Support wide variety of platforms(Below support from Day1):Windows 7, Windows 8.1, and 10, Windows server 2008 R2, Windows server 2012 R2, Windows server 2012, Mac OS X -10.11.X,10.12.x, Red Hat Linux/Cent OS , VDI (Citrix and VM Ware)
14	The solution should Support PrtSc blocking on endpoint when configurable list of specific application are running, no matter it is in the foreground or background. The actual PrtSc capture will also be submitted to the DLP system as forensic evidence.
15	The solution should have ability to detect cumulative malware information leaks. The solution should able to detect the data leaks over to competitors and the data sent and uploaded after the office hours predefined patterns. The solution should able to detect and Block the sensitive information uploads to Group of P2P software :- Bit Tornado, Bit torrent, e Mule and e Mule Frost Wire.
16	The Endpoint DLP Solution must be able to encrypt data when business classified data is sent to removable media drives. The encryption solution can be built in or 3rd party solution needs to be factored to meet the requirement.
17	The Proposed Endpoint DLP Solution must be able to apply DLP policies to Microsoft RMS encrypted files on Windows endpoints to have better understanding of how RMS is being used by employees to protect sensitive data.
18	The solution should support the multiple Endpoint Profile Creation for the Better Security between the different departments. Encryption Keys are also should be isolated between the different departments. The endpoint installed should have the capability to create the Bypass ID after validation by the administrator by generating the Pass-code.
	Data Identification & Policy Management
19	The solution should have a comprehensive list of pre-defined policies and templates with over 1700+ patterns to identify and classify information pertaining to different industry like Energy, Petroleum industry vertical etc and India IT Act.
20	The solution should provide capabilities to identify data based on keywords or dictionaries and the solution should be able to enforce policies based on file types, size of files and also the name of the file.

S.No.	Minimum Technical Requirements
21	The solution should be able to detect and block encrypted and password protected files without reading the encrypted content.
22	The solution should be able to do full binary fingerprint of files and also should be able to detect even if partial information gets leaks from fingerprinted files or folders.
23	The solution should be able to recursively inspect the content of compressed archives.
24	The solution should be able to fingerprint only specific fields or columns within a database and should be able to identify information from databases by correlating information residing in different columns in a database.
25	The solution should have printer agents for print servers to detect data leaks over print channel.
26	The Solution should have advanced Machine Learning – Ability to automatically learn sensitive information from copies of information that needs to be protected and also automatically learn false positives.
27	The solution should enforce policies to detect low and slow data leaks.
28	The solution should be able to enforce policies to detect data leaks even through image files through OCR technology.
29	The solution should be able to identify data leaked in the form unknown and known encrypted format like password protected word document.
30	The solution should be able to identify and block malicious activity like data thefts through files encrypted using non-standard algorithms.
31	The Proposed DLP Solution must be GDPR Compliant.
32	The proposed DLP Solution must be able to detect Data Classification Labels applied by Data Classification partners by reading metadata as well as custom header analysis.
33	The solution should support the templates for detecting the Deep Web URLs- .i2P and .Onion , Encrypted attachments to competitors , Password Dissemination , User Traffic over time , Unknown Encrypted File Formats Detection. The solution should support detection of PKCS #12 files (.p12, .pfx) that are commonly used to bundle a private key with its X.509 certificate.
	Automated Response & Incident Management
34	The solution should be able to alert and notify sender, sender's manager and the policy owner whenever there is a policy violation, Different notification templates for different audience should be possible.
35	The solution should support quarantine as an action for email policy violations and should allow the sender's manager to review the mail and provide permissions for him to release the mail without logging into the UI.
36	The incident should include a clear indication of how the transmission or file violated policy (not just which policy was violated), including clear identification of which content triggered the match and should allow opening of original attachment directly from the UI.
37	The incident should display the complete identity of the sender(Full name, Business unit, manager name etc.) and destination of transmission for all network and endpoint channels. The solution should also allow assigning of incidents to a specific incident manager.
38	The solution should provide automatic notification to incident managers when a new incident is assigned to them and the incident should not allowed for deletion even by the product administrator.

S.No.	Minimum Technical Requirements
39	The solution should allow a specific incident manager to manage incidents of specific policy violation, specific user groups etc.
40	The solution should have options for managing and remediating incidents through email by providing incident management options within the in the notification email itself.
	Role Based Access and Privacy Control
41	The system should control incident access based on role and policy violated. The system should also allow a role creation for not having rights to view the identity of the user and the forensics of the incident.
42	The system should create separate roles for technical administration of servers, user administration, policy creation and editing, incident remediation, and incident viewing for data at rest, in motion, or at the endpoint.
43	The system should allow a role only to view incidents but not manage or remediate them.
44	The system should have options to create a role to see summary reports, trend reports and high-level metrics without the ability to see individual incidents.
45	The system should allow incident managers and administrators to use their Active directory credentials to login into the console.
	Reporting and Analytics
46	The solution should have a dashboard view designed for use by executives that can combine information from data in motion (network), data at rest (storage), and data at the endpoint (endpoint) in a single view.
47	The system should allow reports to be mailed directly from the UI and should allow automatic schedule of reports to identified recipients.
48	The reports should be exported to at least CSV, PDF, HTML formats.
49	The system should provide options to save specific reports as favourites for reuse
50	The system should have lots of pre-defined reports which administrators can leverage.
51	The proposed solution should provide Incident Workflow capabilities where user/Business Manager can remediate the DLP policy violations actions from handsets/emails without logging into the Management Console.
52	The DLP Solution must provide visibility into Broken Business process. For ex, if unsecured sensitive content is sent daily from several users to a business partner, the users are probably not aware that they are doing something wrong.
53	The Proposed DLP engine must performs a post-processing incident grouping step to avoid displaying related incidents in different cases. All incidents from the same user that have the same classification are combined into a group and DLP case card.
54	The DLP dashboard must display the number of cases in the designated period that fall above the risk score threshold that you've selected. Risk score thresholds must be customizable and instantly produce a report to prioritize the cases from high-to-low risk levels by leveraging analytics or machine learning technologies.
	Storage (Data at rest)
55	The system should allow automatic movement or relocation of file, delete files during discovery.
56	The system should display the original file location and policy match details for files found to violate policy.
57	The system should leave the "last accessed" attribute of scanned files unchanged so as not to disrupt enterprise backup processes.

S.No.	Minimum Technical Requirements
58	The system should support incremental scanning during discovery to reduce volumes of data to be scanned.
	Management Monitoring
59	The solution should have centralized management and unified policy enforcement platform.
60	The solution should provide detailed reporting and if database is required for reporting then please provide hardware/software requirements for the same.
61	The DLP and Web should be managed by same console for the ease of operation and better integration.

5.2.1.10. Functional & Technical Requirements for DC Core Switch

S.No.	Minimum Technical Requirements
1	Architecture
1.1	The Core switch should have chassis based, min. 6 slots for interface modules
1.2	The switch shall have Min Dual Management Modules/CPU/Supervisory Module/Routing Engine with 1:1 redundancy
1.3	Shall provide distributed /Centralized /Fabric switching technology (any additional hardware required for the same shall be proposed) & should support virtualization between both switches
1.4	The switch shall be 19" Rack Mountable and shall have all mounting accessories
1.5	Shall have up to 6 Tbps switching capacity and the chassis should support to upgrade up to 9 Tbps switching capacity in feature
1.6	Shall have up to 2 Bpps switching throughput
1.7	Minimum 3 Tbps (Full Duplex) per-slot bandwidth
1.8	The chassis shall support 40G and 100G port without any hardware upgrade
1.9	The switch shall have Modular operating system provides an easy to enhance and extend feature which doesn't require whole scale changes
2	Min Interface Requirement
2.1	Switch shall be provided with min. 8 nos. of 40GbE QSFP+ ports. Min. 2 ports should be populated with multimode SR4 transceivers.
2.2	Should have 112 nos. of 1G/10G SFP+ Ports distributed in min. 2 slots. Min. 16 ports should be populated with multimode SR transceivers, 48 nos. populated with 1000 Base-T transceivers. All the tranceivers should be from the same OEM as the switch.
2.3	Should have 48 nos. of 1000 Base-T Ports Copper (RJ-45)
3	Reliability and Resiliency Features
3.1	Redundant/Load-sharing power supplies with N+N power redundancy
3.2	Redundant Fans / redundant fans within the fan tray for redundancy
3.3	Passive/Redundant backplane design with hot swappable modules
3.4	The Switch should have the capability to extend the control plane across multiple active switches making it a virtual switching fabric, enabling interconnected switches to perform as single Layer-2 switch and Layer-3 Switch through Equivalent SDN Technology. The Fabric should be managed by a single IP Address.
3.5	The connected servers or switches should be attached using standard LACP for automatic load balancing and high availability

3.6	The virtual switching fabric shall be established over standard 10G Ethernet links
3.7	Virtual Router Redundancy Protocol (VRRP) support
3.8	Bidirectional Forwarding Detection (BFD) for RIP, OSPF, BGP, IS-IS and VRRP
3.9	Graceful restart for OSPF, IS-IS, BGP
3.10	UDLD or equivalent feature to prevent loops on detecting unidirectional links
3.11	Shall support a ring protocol to provide standard sub- 200 ms recovery for ring Ethernet-based topology
3.12	Shall support Virtual Extensible LAN (VXLAN), Software Defined Networking (SDN) architecture with OpenFlow 1.3 protocol.
4	Layer 2 features
4.1	Spanning Tree (IEEE 802.1d STP, 802.1w RSTP, 802.1s MSTP)
4.2	Up to 4000 port-based or IEEE 802.1Q-based VLANs
4.3	IEEE 802.3ad Link Aggregation
4.4	IEEE 802.3ab LLDP
4.5	Jumbo Frames Support
4.6	IGMPv1/v2/v3, MLDv2/MLDv2 Snooping
4.7	QoS, Traffic prioritization and shaping
4.8	Access Control Lists
4.9	IEEE 802.1X, Port Security
4.10	STP BPDU protection and Root Guard
4.11	DHCP Snooping and IP Source Guard
4.12	ARP attack protection
4.13	IEEE 802.1AE MACsec/Equivalent
5	IPv4 & IPv6 Routing features (any software/license required to enable these features shall be provided from Day 1)
5.1	Static routing, RIPv1/v2
5.2	OSPFv2, IS-IS, BGPv4
5.3	Equal-Cost Multipath (ECMP)
5.4	Policy Based routing
5.5	RIPng/Equivalent OSPFv3, BGP4+, IS-ISv6
5.6	IPv6 tunnelling
5.7	PIM-SM/PIM-DM/PIM-SSM
5.8	(PIM-SMv6, PIM-DMv6 , PIMSSMv6)/ MLD V1, V2 and 1 K multicast routes.
5.9	Multicast Source Discovery Protocol (MSDP)
5.10	Unicast Reverse Path Forwarding (uRPF)
6	Management & maintenance
6.1	Configuration through the CLI, console, Telnet, SSHv2
6.2	Switch management logon security (RADIUS/TACACS+)
6.3	SNMP v1/v2/v3
6.4	Traffic statistics via sFlow or equivalent
6.5	Network Time Protocol
7	Software Defined Networking (SDN) Capability
7.1	OpenFlow protocol capability to enable software-defined networking
7.2	Allows the separation of data (packet forwarding) and control (routing decision) paths, to be controlled by an external SDN Controller, utilizing Openflow protocol
8	Environment
8.1	Shall be Support for RoHS / WEEE regulations
8.2	Safety: UL / CAN / CSA-C22.2 / EN / IEC 60950-1

10	OEM qualification Criteria
10.1	The Switch or Switch Operating System should be EAL-2/NDPP certified

5.2.1.11. Functional & Technical Requirements for DC Switches

S.No.	Minimum Technical Requirements
1	**Architecture**
1.1	The switch should have at least 48 fixed 1000/10000 SFP+ ports, 4 x QSFP+ 40GbE ports.
1.2	The Switch should support,1 RJ-45 out-of-band management port and 1 USB 2.0 port
1.3	The switch should support dual power supply and redundant fan modules
1.4	The switch Shall support 1000 Base-SX, LX, LH
1.5	The switch Shall Support 10Gbase-SR,LR,ER
1.6	The switch should have 512 MB flash, 2 GB SDRAM
1.7	The Switch should have 9 MB packet buffer size
1.8	All the ports in the Switch should be 1U 19" Rack-Mountable
1.9	At least 1280 Gbps switching capacity
1.10	The switch shall have switching throughput up to 950 million pps
1.11	MAC Address table size of 128,000 entries
1.12	Switch should at least support 16,000 routing entries IPv4, 8,000 entries (IPv6)
2	**Quality of Service (QoS)**
2.1	The Switch should support Strict Priority (SP), WRR/WDRR/WFQ, SP+WRR/ SP+WDRR/SP+WFQ, Configurable Buffer, Time range, Queue Shaping, CAR with 8kbps granularity. The Switch should support traffic shaping technology.
2.2	The Switch should support packet filtering at L2 (Layer 2) through L4 (Layer 4); flow classification based on source MAC address, destination MAC address, source IP (IPv4/IPv6) address, destination IP (IPv4/IPv6) address, port, protocol, and VLAN.
3	**Resiliency, High availability and Optimization features**
3.1	The Switch should have cut-through and no blocking architecture
3.2	The Switch should have the capability to extend the control plane across multiple active switches making it a virtual switching fabric, enabling interconnected switches to perform as single Layer-2 switch and Layer-3 Switch through equivalent SDN technology. The Fabric should be managed by a single IP Address.
3.3	The connected servers or switches should be attached using standard LACP for automatic load balancing and high availability.
3.4	The Switch should have Advanced modular operating system
3.5	The Switch should support Reversible airflow
3.6	The Switch should have Internal redundant and hot-pluggable power supplies and dual fan trays
3.7	The Switch should support Jumbo frames on Gigabit Ethernet and 10-Gigabit ports
3.8	The Switch should support VXLAN Layer 2 and Layer 3 gateway support for up to 1k tunnels
3.9	The Switch should support Dynamic VXLAN configuration
3.10	The Switch should support OVSDB for dynamic VXLAN configuration

S.No.	Minimum Technical Requirements
3.11	The Switch should support EVPN
3.12	The Switch should support IEEE 802.1w Rapid Convergence Spanning Tree Protocol
3.13	The Switch should support IEEE 802.1s Multiple Spanning Tree
3.14	The Switch should support Virtual Router Redundancy Protocol (VRRP)
3.15	The Switch should support Hitless patch upgrades
3.16	The Switch should support Bidirectional Forwarding Detection (BFD) to enables link connectivity monitoring and reduces network convergence time for RIP, OSPF, BGP, IS-IS, VRRP, and switch virtualization technology
3.17	The Switch should support Device Link Detection Protocol (DLDP) or Link Layer Discovery Protocol (LLDP)
3.18	The Switch should support Graceful restart for OSPF, BGP, and IS-IS
4	**Layer 2 switching**
4.1	The Switch should support MAC-based VLAN
4.2	The Switch should support Address Resolution Protocol (ARP) and supports static, dynamic, and reverse ARP and ARP proxy
4.3	The Switch should support IEEE 802.3x Flow Control
4.4	The Switch should support Ethernet Link Aggregation
4.5	The Switch should support IEEE 802.3ad Link Aggregation of up to 128 groups of 32 ports and support for LACP, LACP Local Forwarding First, and LACP Short-time provides a fast, resilient environment that is ideal for the data center
4.6	The Switch should support STP (IEEE 802.1D), Rapid STP (RSTP, IEEE 802.1w), and Multiple STP (MSTP, IEEE 802.1s)
4.7	The Switch should support for 4,096 VLANs based on port, MAC address, IPv4 subnet, protocol, and guest VLAN; supports VLAN mapping
4.8	The Switch should support for IGMP Snooping, Fast-Leave, and Group-Policy; IPv6 IGMP Snooping provides Layer 2 optimization of multicast traffic
4.9	The Switch should support DHCP support at Layer 2
5	**Layer 3 services from day-1 (any additional licenses required shall be included)**
5.1	The Switch should support Address Resolution Protocol (ARP)
5.2	The Switch should determines the MAC address of another IP host in the same subnet; supports static ARPs; gratuitous ARP allows detection of duplicate IP addresses; proxy ARP allows normal ARP operation between subnets or when subnets are separated by a Layer 2 network
5.3	The Switch should support simplifies the management of large IP networks and supports client and server; DHCP Relay enables DHCP operation across subnets
6	**Layer 3 routing from day-1(any additional licenses required shall be included)**
6.1	The Switch should support Virtual Router Redundancy Protocol (VRRP)
6.2	The Switch should support Policy-based routing
6.3	The Switch should support Equal-Cost Multipath (ECMP)
6.4	The Switch should support static routes, RIP and RIPv2, OSPF, BGP, and IS-IS
6.5	Intermediate system to intermediate system (IS-IS)
6.6	The Switch should support Static IPv6 routing
6.7	The Switch should support separate stacks for IPv4 and IPv6 to ease the transition from an IPv4-only network to an IPv6-only network design

S.No.	Minimum Technical Requirements
6.8	The Switch should allow IPv6 packets to traverse IPv4-only networks by encapsulating the IPv6 packet into a standard IPv4 packet; supports manually configured, 6to4, and Intra-Site Automatic Tunnel Addressing Protocol (ISATAP) tunnels; is an important element for the transition from IPv4 to IPv6
6.9	The Switch should allow custom filters for increased performance and security; supports ACLs, IP prefix, AS paths, community lists, and aggregate policies
6.10	The Switch should enables link connectivity monitoring and reduces network convergence time for RIP, OSPF, BGP, IS-IS, VRRP and switch virtualisation technology
6.11	The Switch should Multicast Routing PIM-DM/PIM-SM, PIM-SSM for IPv4 and IPv6
6.12	The Switch should static routing, RIPng/ equivalent OSPFv3, BGP4+ for IPv6, and IS-ISv6, Multiprotocol BGP (MBGP)
6.13	The Switch should able to shut off unused ports and utilizes variable-speed fans, reducing energy costs
6.14	The Switch should able to shut off unused ports and utilizes variable-speed fans, reducing energy costs
7	**Management**
7.1	The Switch should allow users to copy switch files to and from a USB flash drive
7.2	The Switch should support Multiple configuration files and stores easily to the flash image
7.3	The Switch should SNMPv1, v2c, and v3
7.4	The Switch should Out-of-band interface
7.5	The Switch should enable traffic on a port to be simultaneously sent to a network analyser for monitoring
7.6	The Switch should support Remote configuration and management
7.7	The Switch should support IEEE 802.1AB Link Layer Discovery Protocol (LLDP)
7.8	The Switch should support sFlow (RFC 3176)
7.9	The Switch should leverage RADIUS to link a custom list of CLI commands to an individual network administrator's login; an audit trail documents activity
7.10	The Switch should provide support management access through a modem port and terminal interface, as well as in-band and out-of-band Ethernet ports; provides access through terminal interface, Telnet, or secure shell (SSH)
7.11	The Switch should restrict access to critical configuration commands; offers multiple privilege levels with password protection; ACLs provide Telnet and SNMP access; local and remote syslog capabilities allow logging of all access
7.12	The Switch should support ingress and egress port monitoring and trace-route and ping
7.13	The Switch should support sFlow (RFC 3176)
7.14	The Switch should support ISSU/NSSU/hitless upgrade and hot patching/hitless patching
7.15	The Switch should support NTP, SNTP and PTP
10	**Security**
10.1	The Switch should provide IP Layer 3 filtering based on source/destination IP address/subnet and source/destination TCP/UDP port number
10.2	The Switch should support RADIUS/TACACS+

S.No.	Minimum Technical Requirements
10.3	The Switch should support Secure shell encrypt all transmitted data for secure remote CLI access over IP networks
10.4	The Switch should support IEEE 802.1X and RADIUS network logins
10.5	The Switch should support allow access only to specified MAC addresses, which can be learned or specified by the administrator
11	**Software Defined Networking (SDN) Capability**
11.1	The Switch should have Open Flow 1.3 protocol capability to enable software-defined networking from Day one
11.2	The Switch should Allow the separation of data (packet forwarding) and control (routing decision) paths, to be controlled by an external SDN Controller, utilizing Open flow protocol
12	**EMC & Safety Compliance**
12.1	The switch should have UL 60950-1; EN 60825-1 Safety of Laser Products-Part 1; CAN/CSA-C22.2 No. 60950-1; ROHS Compliance Emissions : VCCI Class A; EN 55022 Class A
13	**OEM qualification Criteria**
13.1	The Switch or Switch Operating System should be EAL-2/NDPP certified

5.2.1.12. Functional & Technical Requirements for Blade Servers

S.No.	Description	Minimum Technical Requirements
1	CPU	Latest Generation x86-64 Bit, Populated with dual Multi-tasking Processors having min 16 cores of minimum 2.8 GHz each. Cache as per offered processor. Processor should be from latest announced series.
2	Motherboard	Intel C621 Series Chipset or latest
3	Memory	RAM should be configured with 12 GB Per core. Memory should be scalable to double the capacity configured.
4	Memory Protection	Advanced ECC with multi-bit error protection, Online spare.
5	Hard disk drive with carrier	2 * 1.2 TB GB hot plug SFF SAS drives or higher
6	Storage Controller	12Gb/s SAS Raid Controller with RAID 0/1/1+0 and shall have at-least 1GB flash backed write cache.
7	Networking features	Converged Network Adaptor with 50Gbps bandwidth (100Gbps bi-directional) which supports carving FlexNICs/vNIC and FlexHBA/vHBA per downlink port (minimum up to 8 sub-ports)
8	Blade Server Connectivity to SAN	Should be capable of supporting 32 Gbps Dual port Fibre Channel HBA internal to the Server Blade or using convered Network Adapter having backward compatibility of 16Gb FC.
9	Bus Slots	Minimum of 3 Nos of x16 PCIe 3.0 based mezzanine slots supporting Converged Ethernet/Ethernet/ FC adapters/SAS adaptors

S.No.	Description	Minimum Technical Requirements
10	Embedded system management	1. Should support Gigabit out of band management port to monitor the servers for ongoing management, service alerting and reporting. 2. Should support UEFI to configure and boot the servers securely 3. System should support RESTful API integration 4. System management should support provisioning servers by discovering and deploying 1 to few servers with embedded Provisioning tool 5. System should support embedded remote support to transmit hardware events directly to OEM or an authorized partner for automated phone home support
11	OS Support	1. Microsoft Windows Server 2. Red Hat Enterprise Linux (RHEL) 3. SUSE Linux Enterprise Server (SLES) 4. VMware
12	System tuning for performance	1. System should support feature for improved workload throughput for applications sensitive to frequency fluctuations. This feature should allow processor operations in turbo mode without the frequency fluctuations associated with running in turbo mode 2. System should support workload Profiles for simple performance optimization
13	Embedded Remote Management and firmware security	1. System remote management should support browser based graphical remote console along with Virtual Power button, remote boot using USB/CD/DVD Drive. It should be capable of offering upgrade of software and patches from a remote client using Media/image/folder; It should support server power capping and historical reporting and should have support for multifactor authentication 2. Server should have dedicated remote management port 3. Remote management port should have storage space earmarked to be used as a repository for firmware, drivers and software components. The components can be organized in to install sets and can be used to rollback/patch faulty firmware

S.No.	Description	Minimum Technical Requirements
		4. Server should support agentless management using the out-of-band remote management port 5. The server should support monitoring and recording changes in the server hardware and system configuration. It assists in diagnosing problems and delivering rapid resolution when system failures occur 6. Applications to access the server remotely using popular handheld devices based on Android or Apple IOS should be available 7. Remote console should provide support for AES and 3DES on browser. Should provide remote firmware update functionality 8. Should support managing multiple servers as one via 9. Group Power Control 10. Group Power Capping 11. Group Firmware Update 12. Group Configuration 13. Group Virtual Media 14. Group License Activation 15. Should support RESTful API integration 16. System should support embedded remote support to transmit hardware events directly to OEM or an authorized partner for automated phone home support
14	Server Management	1. Software should support dashboard view to quickly scan the managed resources to assess the overall health of the data center. It should provide an at-a-glance visual health summary of the resources user is authorized to view. 2. The Dashboard minimum should display a health summary of the following: • Server Profiles • Server Hardware • Appliance alerts 3. The Systems Management software should provide Role-based access control 4. Management software should support integration with popular virtualization platform management software like vCenter, and SCVMM 5. Should help provide proactive notification of actual or impending component failure alerts on critical components like CPU, Memory and HDD.

S.No.	Description	Minimum Technical Requirements
		6. Should provide an online portal that can be accessible from anywhere. The portal should provide one stop, online access to the product, support information and provide information to track warranties, support contracts and status. The Portal should also provide a Personalised dashboard to monitor device heath, hardware events, and contract and warranty status. Should provide a visual status of individual devices and device groups. The Portal should be available on premise (at our location - console based) or off premise (in the cloud). 7. Should help to proactively identify out-of-date BIOS, drivers, and Server Management agents and enable the remote update of system software/firmware components. 8. The Server Management Software should be of the same brand as of the server supplier.

5.2.1.13. Functional & Technical Requirements for Blade Chassis

S.No.	Description	Minimum Technical Requirements
1	Solution Requirement	1. Each chassis should be left 25% vacant for future scalability. 2. Solution should support API to integrate into popular management tools such as Microsoft Systems Center and VM Ware v Center and into open source automation and Dev Ops tools such as Chef, Docker and Open Stack. 3. Solution should support software defined templates to quickly make changes to the infrastructure. Template should include server BIOS, firmware, boot order, RAID, storage configs and network config of the infrastructure required for workload
2	Blade Chassis	1. Solution to house the required number of blade servers in smallest number of enclosures. 2. Should support full height and half height blades in the same enclosure, occupying a min of 10U rack height 3. Enclosure should support Intel Xeon processors based 2 CPU and 4 CPU blades 4. Should support technology built-in to every chassis for Auto-Discovery of resources 5. Should support linking multiple enclosures together to form single management ring to reduce complexity and provide single console of management for connected enclosures

S.No.	Description	Minimum Technical Requirements
3	Interconnects support	1. Should support housing of FCoE/Ethernet/FC/SAS interconnect fabrics offering redundancy as a feature.
4	Converged Interconnect	1. Redundant Interconnect modules to should support aggregate 50 Gbps downlinks bandwidth (100 Gbps bi-directional) to the Blades in redundancy supporting carving Flex NICs/vNIC and Flex HBA/vHBA. Each Flex HBA/vHBA should support to transport either Fibre Channel over Ethernet/CEE or Accelerated iSCSI protocol. 2. Blade Solution should provide aggregate 400Gbps Ethernet and aggregate 128Gbps FC uplink bandwidth. Redundant I/O modules to be provided with the Blade solution to achieve the same. 3. Any other intermediate switch/modules if required should be included in solution with 1:1 non-blocking architecture.
5	Power Supply	1. The enclosure should be populated fully with power supplies of the highest capacity available with the vendor. Power supplies should be supplied with N+N redundancy. 2. Power supply should be N+N redundant even when the chassis is fully populated with highest watt processor available in the processor category from Intel in offered model. 3. Should offer a single phase power subsystem enabled with technologies for lower power consumption and offering Platinum energy efficiency.
6	Cooling	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
7	Warranty	3 years comprehensive warranty
8	System Software	Management/controlling softwares have to be from the hardware OEM.
9	Chassis management capabilities	1. Solution should support redundant physical management appliances within/ outside the enclosure with failover and high-availability 2. Should support auto-discovery of Compute, Memory and Fabrics within an enclosure or on multiple connected enclosures. 3. Should support activity, Health and Power LEDs/LCDs for immediate status 4. Should support software-defined intelligence for configuring profiles to provision compute,

S.No.	Description	Minimum Technical Requirements
		fabrics and images so that image of one server can be transferred to another. 5. Should offer collaborative user interface which support logical resources to physical resources mapping, Smart Search, Activity Log, HTML5 mobile access, and Customizable Dashboard 6. Should provide a dedicated GbE or higher management network for communications, separate from data plane 7. Should support reporting capabilities for asset and inventory information for the devices in the enclosures 8. Thermal and power information, including real-time actual power usage per server and per enclosure 9. Reports should be exportable to csv or Microsoft Excel format
10	Integration with virtualization and open source software	1. Should support integration with popular virtualization offerings VMware v Center and Microsoft system center 2. Should support integration with open source automation and Dev Ops tools such as Chef, Docker, and Open Stack

5.2.1.14. Functional & Technical Requirements for SAN Switch

S.No.	Minimum Technical Specifications
1	The fibre channel switch must be rack-mountable. Thereafter, all reference to the 'switch' shall pertain to the 'fibre channel switch'
2	The switch to be configured with minimum of 48 ports 16 Gbps FC configuration backward compatible to 4/8. This is minimum port requirement, however additional SAN Switch port if required may be procured to complete the solution.
3	The switch must have hot-swappable redundant power supply & fan module without resetting the switch, or affecting the operations of the switch.
4	The switch must be able to support non-disruptive software upgrade.
5	The switch must be able to support stateful process restart.
6	The switch must be capable of creating multiple hardware-based isolated Virtual Fabric (ANSI T11) instances. Each Virtual Fabric instance within the switch should be capable of being zoned like a typical SAN and maintains its own fabric services, zoning database, Name Servers and FSPF processes etc. for added scalability and resilience.
7	The switch must support minimum 4 Virtual Fabric Instances.
8	The switch must be capable of supporting hardware-based routing between Virtual Fabric instances.
9	The switch must support graceful process restart and shutdown of a Virtual Fabric instance without impacting the operations of other Virtual Fabric instances.
10	The switch shall support hot-swappable Small Form Factor Pluggable (SFP) LC typed transceivers.

11	The switch must support hardware ACL-based Port Security, Virtual SANs (VSANs), and Port Zoning.
12	The switch must support Smart Zoning such that the entries in the TCAM is significantly reduced and therefore increasing the overall scalability of the SAN Fabric.
13	The switch must support Power On Auto Provisioning (POAP) and Quick Configuration Wizard for simplified operations.
14	Inter-switch links must support the transport of multiple Virtual Fabrics between switches, whilst preserving the security between Virtual Fabrics.
15	The switch must support routing between Virtual Fabric instance in hardware.
16	The switch shall support FC-SP for host-to-switch and switch-to-switch authentication.
17	The switch must be able to load balance traffic through an aggregated link with Source ID and Destination ID. The support for load balancing utilizing the Exchange ID must also be supported.
18	The switch must be equipped with congestion control mechanisms such that it is able to throttle back traffic away from a congested link.
19	The switch must be capable of discovering neighbouring switches and identify the neighbouring Fibre Channel or Ethernet switches.
20	The switch should support IPv6. It should support native switch based RESTful APIs
21	Provision of atleast 2 switches
22	The interface requirement mentioned here is the minimum. If the solution requires more number of interfaces (considering 100% redundancy) then the same should be procured.

5.2.1.15. Functional & Technical Requirements for Storage

S.No.	Description	Minimum Technical Requirements
1	Controller	Dual active controller scalable to 4 or more with automated I/O path failover. Controllers must be offered which shall be true active-active so that a single logical unit can be shared across all offered controllers in symmetrical fashion, while supporting all the major functionalities like Thin Provisioning, Data Tiering etc.
2	Connecting ports(SAN)	Should have minimum of 4x10Gbe and 4x16Gb FC Host ports.
3	Management Software	Must include Storage Manager software, to centrally manage all Storage subsystems, Multi-path (Load Balancing & Failover), LUN masking and should Support RAID migration on to the vacant space available
4	O/S Support	Support for multiple Operating Systems connecting to it, including of Windows/Linux/AIX/HP UX etc.
5	Capacity	Offered Storage Solution shall be configured and populated with 4000 TB usable with 7.2K RPM NL-SAS or 10K RPM SAS/SSD hot swappable HDD . The solution should be designed such that the entire capacity may be equally split into maximum 2 storage arrays without compromising on any of the Storage Technical Specifications mentioned in this RFP.

6	Raid Controllers	Dual, both Active, minimum 64 GB cache across the two Controllers (32 GB per Controller).
7	Protocol Support	FCP, iSCSI
8	Drive Interface	The storage should have 12 Gb Drive interface. Minimum 8 Nos 12 Gb/s SAS Ports to be provided across controllers.
9	Supported Drives, Mixed Drives	Should support SSD, SAS, NL-SAS, 12 Gb Drives in same enclosure.
10	RAID levels	The storage should support 0,1, 5, 6 and 10 RAID levels. Offered Storage Array shall support distributed Global hot Spare for offered Disk drives and shall be configure as per industry practice.
11	Fans and power Supplies	Redundant, hot-swappable power supplies and fans
12	Rack Support	Suitable for industry-standard Racks and PDUs
13	Data Services	Should include data Snapshot, Thin provisioning, Volume Cloning or equivalent features for the offered capacity of the storage solution. The proposed system support storage based replication software.
14	Alerts	Automated alerts for Improving service response times.
15	Others	All required cable and connectors to be supplied
16	Container support	Offered Storage array shall be integrated with Docker, Red-hat OpenShift, Kubernetes and MESOS container technologies on persistent storage. Vendor shall support for both Fiber channel as well as ISCSI. Container platform with offered storage shall support and integrated to support Snapshot, Clone, Latency control for containerized applications and remote replication.

Note: The storage requirement is to be estimated and supplied as per the solution proposed, if the estimation is more than above specified. Above storage is calculated for storing streams of 2500 cameras at 4Mbps on Full HD @25FPS for 30 days + assuming 10% cameras feed has to be stored for 90 days as flagged data (this flagged data will be reviewed by competent authority every 30 days for further retention) + 400 TB storage for Enterprise database & GIS data.

5.2.1.16. Functional & Technical Requirements for Back up Application

S.No	Description
1	The Proposed backup solution should be available on various OS platforms such as Windows, Linux and Unix platforms and be capable of supporting SAN based backup/restore from various platforms including Unix, Linux and Windows. It should able to integrate with virtualization software and should be able to take back-up of virtual servers. The proposed solution should have integrated view of backup and replication.
2	Granular restoration along with BMR option for quick recovery of deleted files. For DB & Mail applications expected granular restoration at application aware manner
3	The proposed backup solution has in-built media management and supports cross-platform device and media sharing in SAN environment. It provides centralized scratch pool thus ensuring backup never fails for media
4	The proposed solution should provide variable length data deduplication at global level along with compression.
5	The proposed email archival solution should support multi tenancy. It should have encryption and Single Instance Storage capabilities. Email archiver should be available as soft appliance and should be capable of getting deployed at cloud such as AWS.
6	Proposed email archival solution should support Microsoft Exchange, MS Office 365, IBM Lotus, Google mail and others. Email archival solution should provide access to all message ever sent or received through a web interface or Outlook plugin.
7	Proposed solution should support universal recovery to restore from P2P, P2V, V2V, and V2P without having to wait to extract the full backup to production storage
8	The proposed Backup and archival should provide role based access control for security and audit purpose.
9	The software should be able to create Standby server on virtualized systems (VMWare/Hyper-V Server/EC2) and should monitor the heartbeat of the source to enable recovery during production server failure
10	The software must allows administrators to back up a server as frequently as every 15 minutes. The software must allow Administrator to backup of servers , desktop and laptop from a single console .
11	The software should be able to generate logs & report e.g. de-duplication report, Data growth analysis report, Compute utilization report during backup etc.
12	The proposed backup solution should have Global dashboard with Infrastructure Visualization capability to launch Dashboard Reports on a backup node
13	The proposed solution should be able to perform cross platform Instant VM Recovery. The solution should be capable of Instantly restoring VM running on ESX on Hyper V and vice versa. The solution should be capable of taking backup from hardware snapshot.
14	The proposed solution should provide assured recovery mechanism for testing backup integrity.Backup and restoration should contain indication to backup paths and diverse devices like Virtual platform, Raw SCSI, Block file system etc.
15	The proposed software should provide inbuilt capability to integrate with cloud from 3-2-1 perspective and should also allow to perform Instant VM Recovery/ Virtual Standby operation on EC2.

16	The proposed solution should provide D2D2T,D2T and D2D2C capabilities.
17	The proposed backup solution should have inbuilt asynchronous server based replication. The replication software should have data rewind capability and should be vendor agnostic.
18	The proposed solution should provide push button switchover/failover capability.
19	The replication software should provide capability of full system replication and migration of Windows-based servers quick and easy and should provide assured recovery mechanism for non-disruptive DR testing.

Tape Library:

OS Platform	The proposed backup solution should be available on various OS platforms such as Windows,Linux and UNIX platforms
	The proposed backup solution shall support industry leading cluster solution such as MSCS, MC Service Guard, Veritas Cluster. Vendor shall offer Backup software in clustering
Management	The proposed backup solution shall have same GUI across heterogeneous platform to ensure easy administration.
	The proposed backup solution should support tape mirroring of the same job running concurrently with primary backup.
	The proposed backup solution should allow creating tape clone facility after the backup process.
Licensing	The proposed backup solution shall be configured in such a fashion that no extra license for client and media servers is required while moving from LAN to SAN based backup.
	The proposed backup solution shall be configured with unlimited client and media licenses for both SAN based backup and LAN based backup.
	The proposed backup solution must not require separate licensing when upgrading from a lower end server (1-2 CPU-based server) to higher end server (4-and CPU-based server)
	The backup software should support either the Capacity based model or Application based model of licensing and shall be offered accordingly
Performance	The proposed backup solution supports the capability to write up to 32 data streams.
	The proposed backup solution support de-multiplexing of data cartridge to another set of cartridge for selective set of data for faster restores operation to client/servers.
Management	The proposed backup solution has in-built media management and supports cross platform device and media sharing in SAN environment. It provides a centralized scratched pool thus ensuring backups never fail for media.
Scheduling	The proposed backup solution has in-built frequency and calendar based scheduling system.
	The proposed backup solution has certified “hot-online” backup solution for different type of Enterprise databases and applications. Vendor shall configure the backup solution for backing up databases to tape Library and shall offer required licenses accordingly.

	The proposed backup solution shall also support granular recovery for virtualization platform.
Management	The proposed backup software should use the same API for software and hardware deduplication
	The backup software should support backup to disk /VTL / Deduplication Device via Fiber channel
	The backup software should support IP sec encryption for the VTL / Disk device
Efficiency	The proposed backup software should give the option to allow de duplication to be done either on the Application Server or on the Backup Server or at the Target Device.
	The proposed backup software should support contextual search based on meaning.
	The proposed backup software should support both on-premise and secure hosted backup solution
Security	The proposed backup solution shall be able to copy data across firewall.
Management	The proposed backup solution shall support automatic skipping of backup during holidays.
Security	The proposed backup solution must support at least AES 256-bit encryption capabilities.
Management	The proposed backup solution must support integration with Openstack and shall be able to backup Cinder volumes.
	The backup software should support the Recurrence type Every Minute which will support more frequent backup jobs
	The backup software should support priority based backup schedule
Efficiency	The backup software should support missed job execution
Management	The Backup software should support Advanced Scheduling options
	The Backup software should be able to recover only critical volumes and later restore other volumes that were backed up in separate sessions.
Efficiency	The backup software should be capable to supporting 99,999 backup sessions in day
	The backup software should be capable of supporting 1000 concurrent sessions
	The backup software should be able to support maximum of 40 Million files per directory

5.2.1.17. Functional & Technical Requirements for Aggregation Switches

S.No.	Minimum Requirements
1	**Architecture**
1.1	The switch should have at least 24 fixed 1G/10G SFP+ ports from day 1 and scalable up to 48nos 1G /10G SFP+ ports. Switch shall have mini 4 x QSFP+ ports
1.2	The Switch should have 1 x RJ-45 out-of-band management port, 1 x RJ-45 console port and 1 USB 2.0 port
1.4	The switch Shall support 1000 Base-SX, LX, LH
1.5	The switch Shall Support 10Gbase-SR,LR,ER

S.No.	Minimum Requirements
1.6	The switch should have 1 GB flash, 2 GB SDRAM
1.7	The Switch should have 12 MB packet buffer size
1.8	All the ports in the Switch should be 1U 19" Rack-Mountable
1.9	At least 1280 Gbps switching capacity
1.10	The switch shall have switching throughput up to 950 million pps
1.11	MAC Address table size of 128,000 entries
1.12	The Switch should support minimum 8,000 Multicast enteries
1.13	Switch should at least support 100,000 routing entries IPv4, 50,000 entries (IPv6)
2	**Quality of Service (QoS)**
2.1	The Switch should support Strict Priority (SP), WRR/WDRR/WFQ, SP+WRR/ SP+WDRR/SP+WFQ, Configurable Buffer, Time range, Queue Shaping, CAR with 8kbps granularity. The Switch should support traffic shaping technology.
2.2	The Switch should support packet filtering at L2 (Layer 2) through L4 (Layer 4); flow classification based on source MAC address, destination MAC address, source IP (IPv4/IPv6) address, destination IP (IPv4/IPv6) address, port, protocol, and VLAN.
3	**Resiliency, High availability and Optimization features**
3.1	The Switch should have cut-through and nonblocking architecture
3.2	The Switch should have the capability to extend the control plane across multiple active switches making it a virtual switching fabric, enabling interconnected switches to perform as single Layer-2 switch and Layer-3 Switch through equivalent SDN technology. The Fabric should be managed by a single IP Address.
3.3	The connected servers or switches should be attached using standard LACP for automatic load balancing and high availability.
3.4	The Switch should have Advanced modular operating system
3.5	The Switch should support Reversible airflow
3.6	The Switch should have Internal redundant and hot-pluggable power supplies and dual fan trays
3.7	The Switch should support 10K bytes Jumbo frames on Gigabit Ethernet and 10-Gigabit ports
3.8	The Switch should support VXLAN Layer 2 and Layer 3 gateway support for up to 1k tunnels
3.9	The Switch should support Dynamic VXLAN configuration
3.10	The Switch should support OVSDB for dynamic VXLAN configuration
3.11	The Switch should support EVPN
3.12	The Switch Should Support Ethernet Ring Protection
3.13	The Switch should support IEEE 802.1w Rapid Convergence Spanning Tree Protocol
3.14	The Switch should support IEEE 802.1s Multiple Spanning Tree
3.15	The Switch should support Virtual Router Redundancy Protocol (VRRP)
3.16	The Switch should support Hitless patch upgrades
3.17	The Switch should support Bidirectional Forwarding Detection (BFD) to enables link connectivity monitoring and reduces network convergence time for RIP, OSPF, BGP, IS-IS, VRRP, and switch virtulization technology
3.18	The Switch should support Device Link Detection Protocol (DLDP) or Link Layer Discovery Protocol (LLDP)
3.19	The Switch should support Graceful restart for OSPF, BGP, and IS-IS
4	**Layer 2 switching**

S.No.	Minimum Requirements
4.1	The Switch should support MAC-based VLAN
4.2	The Switch should support Address Resolution Protocol (ARP) and supports static, dynamic, and reverse ARP and ARP proxy
4.3	The Switch should support IEEE 802.3x Flow Control
4.4	The Switch should support Ethernet Link Aggregation
4.5	The Switch should support IEEE 802.3ad Link Aggregation of up to 128 groups of 32 ports and support for LACP, LACP Local Forwarding First, and LACP Short-time provides a fast, resilient environment that is ideal for the data center
4.6	The Switch should support STP (IEEE 802.1D), Rapid STP (RSTP, IEEE 802.1w), and Multiple STP (MSTP, IEEE 802.1s)
4.7	The Switch should support for 4,096 VLANs based on port, MAC address, IPv4 subnet, protocol, and guest VLAN; supports VLAN mapping
4.8	The Switch should support for IGMP Snooping, Fast-Leave, and Group-Policy; IPv6 IGMP Snooping provides Layer 2 optimization of multicast traffic
4.9	The Switch should support DHCP support at Layer 2
5	**Layer 3 services from day-1 (any additional licenses required shall be included)**
5.1	The Switch should support Address Resolution Protocol (ARP)
5.2	The Switch should determines the MAC address of another IP host in the same subnet; supports static ARPs; gratuitous ARP allows detection of duplicate IP addresses; proxy ARP allows normal ARP operation between subnets or when subnets are separated by a Layer 2 network
5.3	The Switch should support simplifies the management of large IP networks and supports client and server; DHCP Relay enables DHCP operation across subnets
6	**Layer 3 routing from day-1(any additional licenses required shall be included)**
6.1	The Switch should support Virtual Router Redundancy Protocol (VRRP)
6.2	The Switch should support Policy-based routing
6.3	The Switch should support Equal-Cost Multipath (ECMP)
6.4	The Switch should support static routes, RIP and RIPv2, OSPF, BGP, and IS-IS
6.5	Intermediate system to intermediate system (IS-IS)
6.6	The Switch should support Static IPv6 routing
6.7	The Switch should support separate stacks for IPv4 and IPv6 to ease the transition from an IPv4-only network to an IPv6-only network design
6.8	The Switch should allows IPv6 packets to traverse IPv4-only networks by encapsulating the IPv6 packet into a standard IPv4 packet; supports manually configured, 6to4, and Intra-Site Automatic Tunnel Addressing Protocol (ISATAP) tunnels; is an important element for the transition from IPv4 to IPv6
6.9	The Switch should allow custom filters for increased performance and security; supports ACLs, IP prefix, AS paths, community lists, and aggregate policies
6.10	The Switch should enables link connectivity monitoring and reduces network convergence time for RIP, OSPF, BGP, IS-IS, VRRP and switch virtualisation technology
6.11	The Switch should Multicast Routing PIM-DM/PIM-SM, PIM-SSM for IPv4 and IPv6
6.12	The Switch should static routing, RIPng/ equivalent OSPFv3, BGP4+ for IPv6, and IS-ISv6, Multiprotocol BGP (MBGP)
6.13	The Switch should able to shut off unused ports and utilizes variable-speed fans, reducing energy costs

S.No.	Minimum Requirements
6.14	The Switch should able to shut off unused ports and utilizes variable-speed fans, reducing energy costs
7	**Management**
7.1	The Switch should allow users to copy switch files to and from a USB flash drive
7.2	The Switch should support Multiple configuration files and stores easily to the flash image
7.3	The Switch should SNMPv1, v2c, and v3
7.4	The Switch should Out-of-band interface
7.5	The Switch should enable traffic on a port to be simultaneously sent to a network analyser for monitoring
7.6	The Switch should support Remote configuration and management
7.7	The Switch should support IEEE 802.1AB Link Layer Discovery Protocol (LLDP)
7.8	The Switch should support sFlow (RFC 3176) or equivalent
7.9	The Switch should leverage RADIUS to link a custom list of CLI commands to an individual network administrator's login; an audit trail documents activity
7.10	The Switch should provide support management access through a modem port and terminal interface, as well as in-band and out-of-band Ethernet ports. Switch shall support access through terminal interface, Telnet, or secure shell (SSH)
7.11	The Switch should support ingress and egress port monitoring and trace-route and ping
7.12	The Switch should support ISSU/NSSU/hitless upgrade and hot patching/ hitless patching
7.13	The Switch should support NTP/SNTP
8	**Security**
8.1	The Switch should provide IP Layer 3 filtering based on source/destination IP address/subnet and source/destination TCP/UDP port number
8.2	The Switch should support RADIUS/TACACS+
8.3	The Switch should support Secure shell encrypt all transmitted data for secure remote CLI access over IP networks
8.4	The Switch should support IEEE 802.1X and RADIUS network logins
8.5	The Switch should support allow access only to specified MAC addresses, which can be learned or specified by the administrator
9	**Software Defined Networking (SDN) Capability**
9.1	The Switch should have Open Flow 1.3 protocol capability to enable software-defined networking from Day one
9.2	The Switch should Allow the separation of data (packet forwarding) and control (routing decision) paths, to be controlled by an external SDN Controller, utilizing Open flow protocol
10	**Environmental Features**
10.1	Operating Temperature: 0°C to 45°C
10.2	Operating relative humidity: 10% to 90% noncondensing
11	**EMC & Safety Compliance**
11.1	Safety and Emission standards should be including UL 60950-1; IEC 60950-1; VCCI Class A; EN 55022 Class A. The Switch OS should be certified for EAL-2/NDPP.

5.2.1.18. Functional & Technical Requirements for 24 Port L3 Switch

S.No.	Minimum Technical Requirements
1	**Architecture**
1.1	Shall be 19" Rack Mountable Chassis or Stackable or Integrated solution
1.2	Shall be 1RU, 19" Rack Mountable
1.3	Switch Should be Industrial grade in nature and shall have 24 Nos. of 1G SFP ports and 4 x 1G/10G SFP+ Ports to support 1G/10G transceivers (1000 Base-T, LX/LH, SX, LR, SR) and switch shall have 1 open slot to support 2x10G SFP+ or 2x10G Base-T or 2x40G QSFP+ ports.
1.4	Shall have an RJ45 console port and one RJ45 management port.
1.5	Shall have 1 GB of Memory and 256MB of Flash memory
1.6	Shall have switching capacity of 168 Gbps
1.7	Shall have up to 125 million pps switching throughput
1.8	The switch shall have Modular operating system provides an easy to enhance and extend feature which doesn't require whole scale changes
2	**Resiliency**
2.1	The Switch should have the capability to extend the control plane across multiple active switches making it a virtual switching fabric, enabling interconnected switches to perform as single Layer-2 switch and Layer-3 Switch . The Fabric should be managed by a single IP Address.
2.2	The connected servers or switches should be attached using standard LACP for automatic load balancing and high availability.
2.3	Shall support virtual switching fabric creation across nine switches using 10G Ethernet Links
2.4	The switch shall be non-blocking in architecture
2.5	IEEE 802.1D Spanning Tree Protocol, IEEE 802.1w Rapid Spanning Tree Protocol and IEEE 802.1s Multiple Spanning Tree Protocol
2.6	IEEE 802.3ad Link Aggregation Control Protocol (LACP)
2.7	Shall support 128 Groups of up to 8 ports in a link aggregation
3	**Layer 2 Features**
3.1	Shall support 32K MAC address table
3.2	Shall support up to 4,000 port or IEEE 802.1Q-based VLANs
3.3	Shall support GVRP or equivalent feature to allow automatic learning and dynamic assignment of VLANs
3.4	Shall have the capability to monitor link connectivity and shut down ports at both ends if uni-directional traffic is detected, preventing loops
3.5	Shall support IEEE 802.1ad QinQ and Selective QinQ to increase the scalability of an Ethernet network by providing a hierarchical structure
3.6	Shall support Jumbo frames on GbE ports
3.7	Internet Group Management Protocol (IGMP)
3.8	Multicast Listener Discovery (MLD) snooping
3.9	IEEE 802.1AB Link Layer Discovery Protocol (LLDP)
3.10	The switch shall support 64 instances of MSTP
3.11	Shall support port isolation or equivalent
3.12	Shall support Voice VLAN feature to automatically assigns VLAN and priority to devices like IP phones
4	**Layer 3 Features (any additional licenses required shall be included)**
4.1	Static Routing for IPv4

S.No.	Minimum Technical Requirements
4.2	Static Routing for IPv6
4.3	Shall support RIPv1, RIPv2, OSPF, OSPF v3, BGP, BGP4+, PIM-DM, PIM-SM, PIM-SSM
4.4	User Datagram Protocol (UDP) helper function to allow UDP broadcasts to be directed across router interfaces
4.5	Dynamic Host Configuration Protocol (DHCP) client and Relay
4.6	Proxy ARP to allow normal ARP operation between subnets
4.7	Switch shall support 512 entries (IPv4), 256 entries (IPv6) routing table size.
5	**QoS and Security Features**
5.1	Access Control Lists for Layer 2 to Layer 4 traffic filtering
5.2	Shall support global ACL, VLAN ACL, port ACL, and IPv6 ACL
5.3	Traffic classification using multiple match criteria based on Layer 2, 3, and 4 information
5.4	Powerful QoS feature supporting strict priority (SP) queuing/ weighted round robin (WRR) / SP+WRR
5.5	Shall support applying QoS policies on a port, VLAN, or whole switch, to set priority level or rate limit selected traffic
5.6	IEEE 802.1x to provide port-based user authentication with multiple 802.1x authentication sessions per port
5.7	Media access control (MAC) authentication to provide simple authentication based on a user's MAC address
5.8	Dynamic Host Configuration Protocol (DHCP) snooping to prevent unauthorized DHCP servers
5.9	Port security and port isolation
5.10	STP BPDU port protection to prevent forged BPDU attacks
5.11	STP Root Guard to protect the root bridge from malicious attacks or configuration mistakes IP Source guard to prevent IP spoofing attacks
5.12	IP Source guard to prevent IP spoofing attacks
5.13	Dynamic ARP protection blocking ARP broadcasts from unauthorized hosts
6	**Management Features**
6.1	Configuration through the CLI, SSL, console, Telnet, SSH, SNMPv3 and Web Management
6.2	SNMPv1, v2, and v3 and Remote monitoring (RMON) support
6.3	sFlow (RFC 3176) or equivalent for traffic analysis
6.4	Management security through multiple privilege levels
6.5	FTP, TFTP, and Secure FTP support
6.6	Port mirroring to mirror ingress/egress ACL-selected traffic from a switch port or VLAN to a local or remote switch port
6.7	RADIUS/HWTACACS for switch security access administration
6.8	Network Time Protocol (NTP) or equivalent support
6.9	Shall have Ethernet OAM (IEEE 802.3ah) management capability
7	**Software Defined Networking (SDN) Capability**
7.1	The Switch shall support Open Flow without any hardware change from Day 1 to enable the switch to work in SDN environment.
7.2	shall be able to operate in Hybrid mode. This will allow the switch to function in SDN as well non SDN environment.
8	**Environmental Features**

S.No.	Minimum Technical Requirements
8.1	Shall provide support for RoHS and WEEE regulations
8.2	Shall have features to improve energy efficiency like variable-speed fans, shutoff unused ports etc.
8.3	Operating temperature of 0°C to 45°C .
8.4	Safety and Emission standards including UL 60950-1; IEC 60950-1; VCCI Class A; EN 55022 Class A
9	**OEM qualification Criteria**
9.1	The Switch or Switch Operating System should be EAL-2/NDPP certified

5.2.1.19. Functional & Technical Requirements for PoE Ruggedized Switches

S. No.	Minimum Specifications
1	The Switch Should be Industrial grade in nature and should have eight 10/100/1000 Base-T PoE+ ports out of which three ports can support 60W HPoE.
2	Switch Should have additional Four 100/1000 Base-X SFP ports and to be supplied with one number of 1000Base-LX industrial Gigabit Ethernet optical transceiver.
3	The switch should have minimum switching capacity of 24Gbps.
4	Switch Should support 16K MAC addresses and 4000 VLAN
5	Switch should support MAC Sec/FIPS 180-1 and IEEE 1588v2 PTP
6	Switch should support surge protection of 6KV on copper ports (external)
7	Switch should support maximum PoE Budget of 240 watt
8	Operating Temperature of switch should be 0°C to 70°C
9	The switch should have internal/external (DIN rail mountable) AC power supply.
10	Protection Class should be minimum IP 30 and NEMA TS-2
11	Switch should support Jumbo frame , Bridge Protocol Data Unit (BPDU) blocking , STP Root Guard ,DHCP Option 82 , IEEE 802.1ad .
12	Switch should support DHCP Snooping, DHCP IP and Address Resolution Protocol (ARP) spoof protection, ARP poisoning detection, IP Source Filtering.
13	Switch should support IGMP v1/v2/v3 snooping , MLD v1/v2 snooping and should have should have Digital Diagnostic monitoring
14	Switch should be EN 55022 (Emission Standard) , EN 55024 (Immunity Standard) or equivalent.
15	Warranty 5 years hardware replacement including 24x7 Remote Tel Support, Diagnosis, SW Upgrades.

5.2.1.20. Functional & Technical Requirements for Online UPS – 300 KVA

S.N.	Parameter	Minimum Specifications
1	Capacity	300 KVA or higher. Higher capacity to cover all above IT Components at DC site has to be evaluated
2	Output Waveform	Pure Sine wave
3	Input Power Factor At Full Load	>0.90
4	Input Phases	Three Phases + Neutral
5	Input Voltage Range	150-280VACatFullLoad
6	Input Frequency	50Hz+/-3 Hz
7	Output Voltage	220V AC, Three phase

8	Output Frequency	50 Hz+/-0.5%(Free running);+/-3%(Sync. Mode)
9	Inverter efficiency	>90%
10	Overall AC-AC Efficiency	>85%
11	UPS shutdown	UPS should shut down with an alarm and indication on following conditions 1) Output over voltage 2) Output under voltage 3) Low Battery 4) Inverter over load 5) Over temperature 6) Output short
12	Battery Back up	Min 2 Hours and as per design consideration
13	Battery	SMF(Sealed MaintenanceFree)Battery or Lithium Ion battery technologies with advanced charge control management.
14	Indicators &Metering	Indicators for AC Mains, Load on Battery, Fault, Load Level, Low Battery Warning, Inverter On, UPS on By-pass, Overload, etc. Metering for Input Voltage, Output Voltage and frequency, battery voltage, output current etc.
15	Cabinet	Rack/Tower type

5.2.1.21. Functional & Technical Requirements for Online UPS – 1/2/3/5 KVA

S. No.	Parameter	Minimum Specifications
1.	Technology	Fully Microprocessor Based; True Online(double conversion)
2.	Input	170V to 280V AC @ 45Hz to 55Hz
3.	Output	230VAC +-1%
4.	Wave Form	Pure Sinewave
5.	Overloaded Capacity	125% for 1 Minute; 150% for 10 Secs
6.	Battery	SMF Batteries complete with self-standing Cabinet / Battery Rack for 4 hours backup
7.	Operating Temperature	0 to 50 Degrees
8.	Operating Humidity	95% Non-condensing
9.	Protection	Built in overload / Short Circuit protection; battery deep discharge protection; Earth Leakage Protection; Static Trip protection
10.	Monitoring	Output monitoring for Voltage, Current and Wave form with Closed Loop feedback
11.	By-Pass	Static and manual by-pass switch
12.	Indicators	ON/OFF/Faulty/Trip

5.2.1.22. Functional & Technical Requirements for Line Interactive UPS – 500 VA

S.N.	Parameter	Minimum Specifications
1	Capacity	Adequate capacity to cover all above IT Components at respective location has to be evaluated.
2	Input Power Factor At Full Load	>0.80
3	Input	Single Phase 2 Wire upto 5 KVA
4	Input Voltage Range	90-300 VA Cat Full Load
5	Input Frequency	50Hz+/-3 Hz
6	Output Voltage	220V AC, Single Phase
7	Output Frequency	50 Hz+/-0.5%(Free running);+/-3%(Sync. Mode)
8	Inverter efficiency	>90%
9	Overall AC-AC Efficiency	>85%
10	UPS shutdown	UPS should shut down with an alarm and indication on following conditions 1) Output over voltage 2) Output under voltage 3) Low Battery 4) Inverter over load 5) Over temperature 6) Output short
11	Battery Back up	Min 40 Mins on Full Load
12	Battery	SMF(Sealed MaintenanceFree)Battery or Lithium Ion battery technologies with advanced charge control management.
13	Indicators &Metering	Indicators for AC Mains, Load on Battery, Fault, Load Level, Low Battery Warning, Inverter On, UPS on By-pass, Overload, etc. Metering for Input Voltage, Output Voltage and frequency, battery voltage, output current etc.
14	Cabinet	Rack/Tower type

5.2.1.23. Functional & Technical Requirement for NIPS & HIPS

S.No	Minimum Technical Requirement
1	Intrusion Prevention System (IPS) should be based on purpose-built platform that has Field Programmable Gate Arrays (FPGAs). NIPS should be independent standalone and dedicated appliance based solution, NIPS should not the part of firewall and UTM.
2	The NIPS appliance must have at least 40 Gbps inspection throughput, which includes SSL inspection. NIPS should have 2 * 40 GE QSFP+ and 8 * 10G SFP+ ports.
3	The NIPS must support 115,000,000 concurrent sessions and 6,50,000 new connections per second with latency should be <40 Micro.
4	The proposed IPS solution must support Adaptive Filter Configuration (AFC) and proposed IPS should support the ability to mitigate Denial of Service (DoS/DDoS) attacks such as SYN floods and proposed IPS solution must be able to provide zero-day filters that must be included in weekly signature update.
5	The IPS filter must support network action set such as Block (drop packet), Block (TCP Reset), Permit, Trust, Notify, Trace (Packet Capture), Rate Limit and Quarantine & proposed IPS solution must support signatures, protocol anomaly, vulnerabilities and traffic anomaly filtering methods to detect attacks and malicious traffic
6	The IPS filters must be categories into the following categories for easy management: - Exploits, Identity Theft/Phishing, Reconnaissance, Security Policy, Spyware, Virus, Vulnerabilities, Network Equipment, Traffic Normalization, Peer to Peer, Internet Messaging, Streaming Media
7	The proposed IPS must be able to support granular security policy enforcement based on the following methods: Per IPS device (all segments), Per physical segment uni-direction and bi-directional.
8	The proposed IPS must be able to control the known bad host such as spyware, botnet C2 server, spam and so on based on country of origin, exploit type and the reputation score & NIPS should be different from Network and firewall OEM.
9	The centralized management server for NIPS must be an appliance based on a hardened OS shipped by-default from factory and system shall allow the latest update to be manually, automatically or based on schedule with central management and reporting.
10	The proposed IPS solution must support Layer 2 Fall back option to bypass traffic even with the power on, in event of un-recoverable internal software error such as firmware corruption, memory errors. NIPS should able submit file to sandboxing for real time execution and sandboxing should be customized and able to support win 7, win 8, win 2008, win2012 at least.
11	The HIPS and server security solution should support stateful Inspection Firewall, Anti-Malware, Deep Packet Inspection with HIPS, Integrity Monitoring and Recommended scan in single module with agent-less and agent capabilities for physical and virtual servers and Firewall should have the capability to define different rules to different network interfaces with stateful inspection.
12	The server Security solution should provide automatic recommendations against existing vulnerabilities with CVE number, Dynamically tuning IDS/IPS sensors (eg. Selecting rules, configuring policies, updating policies, etc.) and provide automatic recommendation of removing assigned policies if vulnerability no longer

	exists - For Example - If a patch is deployed unwanted signatures should be un-assigned automatically.
13	The offered HIPS product series must have achieved EAL (Evaluation Assurance Level) Certification of EAL4 or higher in the Common Criteria for Information Technology Security Evaluation (ISO/IEC 15408) for computer security certification.
14	HIPS solution should support server class OS - Windows Server 2K3, 2K8 and 2K12, 2k16, Linux, Centos, SUSE Linux, Debian.

5.2.1.24. Functional & Technical Requirement for Anti-DDoS

S.No	Minimum Technical Requirement
1	**Hardware and Performance**
1.1	DDoS solution should be a dedicated hardware appliance and must not use common hardware platform of Firewall, load-balancer and IPS
1.2	Device should have at least 5 x 1G copper Interfaces
1.3	Should have at least 4x 10 G fibre interface
1.4	System should have inspection throughput of 5 Gbps
1.5	System must have on device black/white list capacity of 8 million
1.6	Should support minimum rate enforcement rate of 100 millisecond
1.7	System must support L2 and L3 mode of deployment
1.8	The device should support high availability using VRRP standards
1.9	System must support 8 million IP sessions from day 1
2	**Generic Features**
2.1	System should support, In-Line, Out-of-Path deployments modes from day 1
2.2	System should support following environments:
a	Symmetric
b	Asymmetric
c	Out of path
2.3	Solution should be transparent to control protocol including MPLS, VLAN, IP in IP and GRE
2.4	The system should be transparent to ‘logical link bundle’ protocols like LACP
2.5	Solution Should detect IPv6 Attacks
2.6	Solution should mitigate IPv6 Attacks
2.7	The DDoS detection capability of the solution must not be impacted by asymmetric traffic routing.
2.8	Should detect and Mitigate attacks at Layer 3 to Layer 7
2.9	Must support static and dynamic routing protocol's including OSFP and BGP
2.10	The system must allow protection parameters to be changed while a protection is running. Such change must not cause traffic interruption
3	**Security / DDoS Feature**
3.1	System should Protect from multiple attack vectors on different layers at the same time with combination of Network, Application, and Server-side attacks
3.2	Solution should provide protection for volumetric/Protocol and Application layer-based DDoS attacks
3.3	Inspection and prevention is to be done in same solution
3.4	The system must have an updated threat feed that describes new malicious traffic (botnets, phishing, etc...).

S.No	Minimum Technical Requirement
3.5	The system should be capable to mitigate and detect both inbound and outbound traffic.
3.6	Solution should provide real time Detection and protection from unknown Network DDOS attacks.
3.7	System should have mitigation mechanism to protecting against zero-day DoS and DDoS attacks without manual intervention with traffic indicators
3.8	System supports behavioural-based application-layer HTTP DDoS protection
3.9	System supports DNS application behavioural analysis DDoS protection
a	System must be able to detect and block SYN Flood attacks and should support different mechanism
b	SYN Protection - Transparent Proxy/out of sequence
c	SYN Protection - Safe Reset
3.10	SYN Protection /TCP Reset.
3.11	System must be able to detect, and block HTTP GET Flood and should support mechanisms to avoid False Positives
a	Should support following HTTP flood Mechanism:
b	High Connection Rate
c	High rate GET to page
3.12	High rate POST to page
a	System should detect and Mitigate different categories of Network Attacks:
b	High rate SYN request overall
c	High rate ACK
d	High rate SYN-ACK
e	Push Ack Flood
f	Ping Flood
3.13	Response/Reply/Unreachable Flood
3.14	System must be able to detect and block ICMP, DNS Floods
3.15	Should support IP defragmentation, TCP stream reassembly.
3.16	The system must be able to block invalid packets including checks for: Malformed IP Header, Incomplete Fragment, Bad IP Checksum, Duplicate Fragment, Fragment Too Long, Short Packet, Short TCP Packet, Short UDP Packet, Short ICMP Packet, Bad TCP / UDP Checksum, Invalid TCP Flags, Invalid ACK Number) and provide statistics for the packets dropped
3.17	Should detect and Mitigate from Low/Slow scanning attacks
3.18	should detect and mitigate from Proxy & volumetric Scanning
3.19	System Should support dedicated DNS protection from DDoS
3.20	System should support suspension of traffic/ blacklisting from offending source based on a signature/attack detection
3.21	System should support user customizable and definable filter
3.22	System should have capability to allow custom signature creation
3.23	System protects from DDoS attacks behind a CDN by surgically blocking the real source IP address
3.24	System must support up to 5 level of auto escalation of any DDOS event
4	**High detection and mitigation accuracy**
4.1	System supports Challenge-response (Layers 4 to 7) mechanisms without Scripts
4.2	System supports HTTP Challenge Response authentication without Scripts
4.3	System supports DNS Challenge Response authentication
5	**Integration Capabilities**

S.No	Minimum Technical Requirement
5.1	System should have capability to integrate with SIEM solution
5.2	Should have ready API for SDN environment integration/ Anti-DDoS system for attack mitigation in custom portal
6	**Monitoring & Management**
6.1	The system must support configuration via standard up to date web browsers. System user interface must be based on HTML
6.2	System must support CLI access over console port, SSH.
6.3	The system must have a dedicated management port for Out-of-Band management
6.4	Management interfaces must be separated from traffic interfaces. System management must not be possible on traffic interfaces, management interfaces must not switch traffic
6.5	System must have role-based access control
6.6	Management certificate must be possible to change
6.7	Proposed solution should have centralized management system (Either appliance or VM based) and helps to manage, monitor, and maintain all DDoS Appliances from a centralized location.
6.8	Role/User Based Access Control
6.9	The system must support the generation of PDF and e-mail reports
6.10	Integration with RADIUS and TACACS+
6.11	System must support NetFlow based integration with Network elements to detect DDOS offline

5.2.1.25. Functional & Technical Requirement for DAM

S.No	Minimum Technical Requirement
1	The solution must be able to perform database & data discovery and classification. Must be able to detect sensitive data types, such as credit card numbers, email address, passwords etc., in database objects.
2	The solution must be able to run database vulnerability assessment and configuration review scans on database servers. Out of box policies for these scans as per standards like NIST, CIS, PCI should be present
3	The solution must be able to monitor all types of database activities including, privilege user activities, SQL queries from web applications, queries from clients like sqlplus, toad etc.
4	The solution should out of box come with security and db audit policies as per standards like PCI, SOX etc.
5	The agent must be able to monitor the local, network traffic and same agent could be used for blocking the traffic.
6	Database audit data must be tamper-proof and must be stored in encrypted flat files.
7	The solution must support the ability to configure a cap on the memory and CPU utilization of the agent on the database server.
8	The solution must support the following range of heterogeneous databases: -
a	DB2
b	MS-SQL
c	MySQL
d	Oracle
e	Teradata
f	Postgres
9	The solution should not require and rely on the use of native database audit functionality.
10	The solution should not rely on database triggers to block the traffic.
11	The solution must be able to capture DML, DDL and DCL database statements by user/role.
12	The solution must identify database user activity/behaviour deviation from the built baseline user behaviour and alert on these deviations.
13	The solution should be able to detect OS user chaining where full chain of OS user login should be identified in audit logs
14	The solution does not require any changes to monitored database and/or application

15	The solution must have a centralized management hardware/ virtual appliance to manage WAF and DAM.
16	The solution management appliance must be able to manage up to 8 WAF/ DAM appliances for future growth

5.2.1.26. Functional & Technical Requirement for Database Encryption

S.No	Minimum Technical Requirement
1.	Encryption solution must be a platform to support Embedded Format preserving encryption to enable transparent key rotation and should seamlessly support custom built applications and commercially off the shelf software.
2	Solution must be stateless supporting data masking, file level encryption, Data De-identification, Data Tokenization.
3	Solution must be capable of format preserving encryption of data at source (application) level and must be independent of any database which customer is using.
4	It should work without schema changes in the databases where private data may reside and must integrate with proposed SIEM seamlessly.
5	It must comply to NIST-Standard FF1 AES Format-Preserving Encryption (SP800-38G) should be provided & necessary security proofs should be provided.
6	The encryption keys should be regenerated on the fly for future e-discovery and the data protected by the system may be shared without exchanging keys with an external party

5.2.1.27. Functional & Technical Requirement for HSM

S.No	Minimum Technical Requirement
1	The HSM should be able to store unlimited number of keys and the HSM should offer scalability on the same device and offer multi-factor authentication.
2	File based encryption solution to be considered instead that is agnostic to any data base and should be able to manage keys in a secured FIPS appliance for managing keys - Separate from the HSM used for e-sign/document signing or PKI Infrastructure.
3	The HSM should be able to store unlimited number of keys and the HSM should offer scalability on the same device and offer multi-factor authentication.
4	The HSM should be able to store unlimited number of keys and the HSM should offer scalability on the same device and offer multi-factor authentication.
5	"Key Management in the enterprise architecture for improved security. Key Management Solution should support both on-premise and on cloud.
6	Key Management solution to be provided on a common/same platform."
7	Data Encryption solution that support both on premise and on cloud. This should be supported on a common/same platform.
8	Encryption solution should be able to offer multiple services like Cloud Gateway Encryption, Management of Keys, Transparent Encryption (File Based) from a common extensible Platform. Also, multi-tenancy to provide more granular level role-based admin control.

5.2.1.28. Functional & Technical Requirements for SSLi

Sr.No.	SSLi Specifications
1	Physical Specification
1.1	System must of be 19-inch rack mountable 1 U form factor
1.2	System must have dedicated management port
1.3	System must have RJ-45 console port
1.4	System must have 5 x 1 G cu Interface , 4 x 10 G fibre ports
1.5	System must be a purpose built appliance and must not be the part of IPS, Proxy, DLP and Load-balancer
2	Performance
2.1	System must support 20 Gbps of L7 throughput
2.2	System must support 125 K Connection SSLi traffic
2.3	System must support 4 K SSLi CPS on RSA 2 K Key and 3 K SSLi CPS on ECDHE cipher
2.4	System must support 7 Gbps of bulk SSL throughput
2.5	System must support 1.5 Gbps outbound SSL interception
3	Application delivery partition/Virtual Context
3.1	System must support 30 Application delivery partition/Virtual Context
3.2	System must support dedicated configuration file for each Virtual context
3.3	System must support resource allocation to each context including throughput, CPS, Concurrent connection, SSL throughput
3.4	System must be able to modify the resource allocation on the fly without restarting/rebooting any context
3.5	All the virtual context must be available from day-1
4	DDOS
4.1	System must support protection from Fragmented packets
4.2	System must support protection from IP Option
4.3	System must support protection from Land Attack
4.4	System must support protection from Packet Deformity Layer 3
4.5	System must support protection from Packet Deformity Layer 4
4.6	System must support protection from Ping of Death
4.7	System must support protection from TCP No Flag
4.8	System must support protection from TCP Syn Fin
4.9	System must support protection from TCP Syn Frag
4.1	System must support connection limit based on source IP
4.11	System must support connection rate limit based on source IP
4.12	System must support request rate limit based on source IP
5	Traffic redirection features
5.1	System must support load-balancing of multiple security devices
5.2	System must support Explicit proxy functionality with proxy chaining
5.3	System must support traffic redirection based any L2-L7 parameters
6	SSL Insight features
6.1	System must Outbound SSL interception
6.2	System must support L2 and L3 mode of deployment
6.3	System must support ICAP integration with DLP and AV
6.4	System must support modification of headers
6.5	System must support before proxy interception (between Client and Proxy)

6.6	System must support SSL interception bypass based on source and/or destination IP
6.7	System must support SSL interception bypass based SNI values
6.8	System must support SSL interception bypass based URL category
6.9	System must support bump in a wire deployment mode
6.10	System must support interception of SSH traffic
6.11	System must support sending decrypted feed to upto 4 off path devices
6.12	System must support dynamic SSL interception for SSL traffic on any tcp port
6.13	System must support URL blacklisting and whitelisting
6.14	System must support TCL based scripts for custom rules
7	Redundancy
7.1	System must support VRRP based redundancy
7.2	System must support active-active and active-backup configuration
7.3	System must support automatic and manual configuration sync
7.4	System must support dynamic VRRP priority by traffic interface, server, nexthop and routes
7.5	System must support scale-out configuration upto 8 devices to support higher throughput
7.6	System must support dedicated VRRP setting per virtual context
8	Management
8.1	System must have Web-based Graphical User Interface (GUI)
8.2	System must have Industry-standard Command Line Interface (CLI)
8.3	System must support Granular Role-based\Object-based Access Control
8.4	System must support SNMP, Syslog, email alerts, NetFlow v9 and v10 (IPFIX), sFlow
8.5	System must support REST-style XML API (aXAPI) for all functions
8.6	System must support external authentication including LDAP, TACACS+, RADIUS

Intelligent Integrated Infrastructure

a) Intelligent integrated/inbuilt infrastructure, standalone system design, engineering, manufacture, assembly, testing at manufacturer's works, supply, delivery at site, unloading, handling, proper storage at site, erection, testing and commissioning at site of complete infrastructure for the proposed Data Centre to be installed.
b) The detail specifications of the intelligent integrated/inbuilt infrastructure, standalone system shall be in adherence to TIA 942 guidelines thus shall be composed of multiple active power and cooling distribution paths, but only one path active. Shall have redundant components.
c) The Intelligent Integrated Infrastructure essentially includes internal redundant or backup power supplies, environmental controls (e.g., precision air conditioning, fire suppression, smoke detection, Water leak detection, humidity sensor etc.), security devices etc. Critical systems like UPS and Precision Air-conditioning system will have N+N and N topology respectively.
d) The Intelligent integrated infrastructure would provide many functionality and some of the key functionalities are Cold Contained Front Aisle & Rear Contained Hot Aisle, insulation, remote management and single point of service.
e) The Intelligent integrated Infrastructure shall have following components:-

i. Precision Air conditioner with variable capacity cooling, heater and humidifier to cater IT load approximately 2X300 KVA in N+N redundancy for a total of 15racks(including 5 network racks).
ii. 2 x 300 KVA UPS with P.F. up to 0.9 & efficiency 92% ~94%. There should be approximately 120 minutes battery back-up.
iii. Novec 1230 Gas based fire suppression system as per NFPA guidelines
iv. Smoke detectors, water leaks detection system, temperature & humidity sensor, door sensor, and alarm beacon.
v. 42 U racks of dimension 800 mm x 1000 mm.
vi. Monitoring system – capable for Email alerts
vii. Standalone rodent repellent system
viii. Biometric access control system, which should be control by access control panel.
ix. Exhaust Fan with Gravity Damper
x. 32A Vertical Rack mount PDU of type IEC C13 & IEC C19 combination, each rack shall have two such PDU's.
xi. Electrical system with essential MCB/MCCB.

Intelligent integrated infrastructure would have provision to add extra racks in future. It should be flexible, adaptable, controllable infrastructure.

5.2.2.1. 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.

S.No.	Item	Minimum Specifications
1.	Capacity	2MX1MX3M
2.	Temperature to Withstand	1000° C for at least 1 hour
3.	Internal Temperature	30° C after exposure to high temperature For 1 hour
4.	Locking	2 IO-lever high security cylindrical / Electronic lock

5.2.2.2. Structured Cabling

To supply and installation, testing and commissioning of the following equipment but not limited to

i. OFC Cabling (MTO Cabling) As per rack layout
ii. Copper Cabling As per rack layout using Patch Panels and CAT 6 I/O
iii. Fibre Runner As per rack layout
iv. Wire basket for Copper As per rack layout
v. The fibre Runner and wire basket shall connect all the rooms

S.No.	Parameter	Minimum Specifications
1.	Standards	ANSI TIA 568 C for all structured cabling components
2.	OEM Warranty	OEM Certification and Warranty of 15-20 years as per OEM standards
3.	Certification	UL Listed and Verified

5.2.2.3. Electrical System & Cabling

To supply and installation, testing and commissioning of the following equipment but notlimited to

i. LT panels ,SUB Distribution Panel, UPS Input and Output Panel with Switch gear as per
ii. specification
iii. Power Cable tray as per requirement
iv. Conduiting and wiring as per requirement
v. Floor PDU as per requirement based on Layout Drawing
vi. LED lighting and Motion detector as per site requirement

All electrical components shall be design manufactured and tested in accordance withrelevant Indian Standard IECSs

5.2.2.4. Cooling System

To supply and installation, testing and commissioning of the following equipment but not limited to

i. DX based Precision Air Conditioning(Perimeter Cooling)
ii. DX based Row Based Cooling (Row Cooling)and Containment for Server room 3

iii. Both Hot and cold Aisle Containment for Server room as per layout in Annexure-2&3 of RFP Vol-II for better PUE, Cooling, Power, DCIM from same OEM for better Integration

5.2.2.5. Safety and Security System

To supply and installation, testing and commissioning of the following equipment but not limited to

i. Addressable Fire Detection and Alarm System
ii. Rodent Repellent System
iii. Gas Based fire Suppression System
iv. Portable Fire Extinguishers

5.2.2.6. Monitoring System

To supply and installation, testing and commissioning of the following equipment but not limited to

i. Building Management System
ii. Temperature and Humidity Sensor
iii. Flow meter for Diesel unloading
iv. Float Sensor for Diesel Monitoring at day tank level
v. Integration with All energy meter, MCCB, ACB, Safety and Security Equipment's, Diesel monitoring, Data centre Temperature and Humidity Monitoring, UPS, PAC, Panel ON/Off/Trip status etc.

5.2.2.7. 42U Racks and PDU

To supply and installation, testing and commissioning of the following equipment but not limited to

i. 19" 42 U Rack with necessary Accessories
ii. Cable entry brush (rack bottom)
iii. 32A IP PDU with Ethernet based Environment Monitoring System with one Temperature Sensor as per Rack layout
iv. 16A IP PDU with Ethernet based Environment Monitoring System with one Temperature Sensor
v. All racks must be lockable on all sides with unique key for each rack
vi. Racks should have Rear Cable Management channels, Roof and base cable access
vii. Two vertical and four horizontal Wire Managers
viii. Blanking Panels
ix. The racks must have steel (solid / grill / mesh) front / rear doors and side panels. Racks should NOT have glass doors / panels
x. Detachable side panels (set of 2 per Rack)
xi. Fan Tray with 4 Nos. per Rack
xii. Manufacturer should have ISO 9001-2015 Certifications, and UL/EN and RoHS certified. Certificate needed to be submitted.

5.2.2.8. 9U Rack

S.No.	Minimum Specifications
1	Racks manufactured out of steel sheet punched, formed, welded and Powder coated
2	Standard for Racks configuration will be welded frame and vented top cover or better
3	Rack should have Front Toughened Glass Door with lock & Key
4	Rack should be 9U in Height, 550MM Width, 1000MM Depth
5	Provision for easy wall mounting should be there with appropriate anchor fasteners
6	Rack must be provided with 2 fan directly mounted on the roof top as an exhaust from the cabinet. Fan should be of AC 230V
7	Rack should be provided with cable management accessories.1U Cable manager, PDU with 6 Nos. Sockets of 5 Amp
8	Manufacturer should have ISO 9001-2015 Certifications, and UL/EN and RoHS certified. Certificate needed to be submitted.

5.2.2.9. KVM Switch

S.No.	Item	Minimum Specifications
1	KVM Requirement	Keyboard, Video Display Unit and Mouse Unit (KVM) for the IT Infrastructure Management at Data Center
2	Form Factor	19” rack mountable
3	Ports	minimum 8 ports
4	Server Connections	It should support both USB and PS/2 connections.
5	Auto-Scan	It should be capable to auto scan servers
6	Rack Access	It should support local user port for rack access
7	SNMP	The KVM switch should be SNMP enabled. It should be operable from remote locations
8	OS Support	It should support multiple operating system
9	Power Supply	It should have dual power with failover and built-in surge protection
10	Multi-User support	It should support multi-user access and collaboration

5.2.2.10. Anti-Climb & Cantilever Poles for Mounting Camera, etc.

S.N.	Parameter	Minimum Specifications
1.	Pole type	Hot Dip Galvanized after Fabrication with Silver coating of 86 micron as per IS:2629; Fabrication in accordance with IS-2713 (1980)
2.	Height	5-10 Meters, as-per-requirements for different types of cameras & Site conditions
3.	Pole Diameter	Min. 10 cm diameter pole (larger diameter for higher height should be chosen)

4.	Cantilevers	Based on the location requirement suitable size cantilevers to be considered with the pole
5.	Bottom base plate	Minimum base plate of size 300mmx300mmx15mm (or) 30cmx30cmx1.5cm
6.	Mounting facilities	To mount CCTV cameras, Switch, etc.
7.	Pipes, Tubes	All wiring must be hidden, through tubes/pipes. No wires shall be visible from outside.
8.	Foundation	Casting of Civil Foundation with foundation bolts, to ensure vibration free erection (basic aim is to ensure that video feed quality is not impacted due to winds in different climatic conditions). Expected foundation depth of min. 100cms. Please refer to earthing standards.
9.	Protection	Lightning arrester at select sites as per the requirements
10.	Sign-Board	A sign board describing words such as "This area under surveillance" (in English and Hindi)

5.2.2.11. DG Set

S.No.	Parameter	Minimum Specifications
1.	General	Auto Starting DG Set Mounted on a common based frame with AVM (Anti-Vibration) pads, residential silencer with exhaust piping, complete conforming to ISO 8528 specifications and CPCB certified for emissions. KVA rating as per the requirement.
2.	Capacity	650 KVA
3.	Fuel	High Speed Diesel (HSD) With 100Ltr. Tank Capacity or better. It should be sufficient and suitable for containing fuel for 12 hours continuous operation, Complete with level indicator, fuel inlet and outlet, air vent, drain plug, inlet arrangement for direct filling and set of fuel hoses for inlet and return.
4.	Power Factor	0.8
5.	Engine	Engine should support electric auto start, water cooled, multi cylinder, maximum 1500 rpm with electronic/manual governor and electrical starting arrangement complete with battery, 4 stroke multiple cylinders/single and diesel operated conforming to BS 5514/ ISO 3046/ IS 10002
6.	Alternator	Self-exciting, self-regulating type alternator rated at 0.8 PF or better, 415 Volts, 3 Phase, 4 wires, 50 cycles/sec, 1500 RPM, conforming to IS 4722/ BS 5000, Windings of 100% Copper, class H insulation, Protection as per IP 23.
7.	AMF (Auto Main Failure) Panel	AMF Panel fitted inside the enclosure, with the following meters/indicators: ▪ Incoming and outgoing voltage ▪ Current in all phases ▪ Frequency ▪ KVA and power factor ▪ Time indication for hours/ minutes of operation ▪ Fuel Level in field tank, low fuel indication ▪ Emergency Stop button

S.No.	Parameter	Minimum Specifications
		▪ Auto/Manual/Test selector switch ▪ MCCB/Circuit breaker for short-circuit and overload protection ▪ Control Fuses ▪ Earth Terminal ▪ Any other switch, instrument, relay etc. essential for Automatic functioning of DG set with AMF panel
8.	Acoustic Enclosure	The DG set shall be provided with acoustic enclosure / canopy to reduce the sound level and to house the entire DG set (Engine & Alternator set) assembly outside (open-air). The enclosure shall be weather resistant powder coated, with insulation designed to meet latest MOEF/CPCB norms for DG sets, capable to withstand local climate. The enclosure shall have ventilation system, doors for easy access for maintenance, secure locking arrangement.
9.	Output Frequency	50 HZ
10.	Tolerance	+/- 5% as defined in BSS-649-1958
11.	Indicators	Over speed /under speed/High water temperature/low lube oil etc.
12.	Intake system	Naturally Aspirated
13.	Certifications	ISO 9001/9002, relevant BS and IS standard

5.2.2.12. NOVEC 1230 Gas based Fire Suppression System

a) Gas Based Fire Suppression System (GBFSS)
   i. The bidder shall supply, install, test and put in operation NOVEC1230 based fire suppression system.
   ii. The fire suppression system shall include and not be limited to gas release control panel, CCE approved seamless cylinders, discharge valve (with solenoid or pneumatic actuator) as the case may be, discharge pipe, non-return valve and all other accessories required to provide a complete operation system meeting applicable requirements of NFPA 2001 or ISO standards and installed in compliance with all applicable requirements of the local codes and standards.
   iii. The system design should be based on the specifications contained herein, NFPA 2001 & in accordance with the requirements specified in the design manual of the agent.
   iv. The bidder shall confirm compliance to the above along with their bid.
   v. The system shall be properly filled and supplied by an approved OEM (Original Equipment Manufacturer)

b) Generally the key components* of the system shall be VdS or LPCB or FM/UL listed. The NOVEC 1230 gas shall:
   i. comply with NFPA 2001 or ISO 14520 standard
   ii. have the approval from US EPA (Environmental Protection Agency) for use as a total flooding fire extinguishing for the protection of occupied space:
   iii. Be given Underwriters' Laboratories Inc. (ULI, USA) component listing for the NOVEC 1230 gaseous agent.
   iv. must have zero ozone depletion potential (ODP);

v. have a short life span in the atmosphere, with atmospheric life time of less than 5 days
vi. be efficient, effective and does not require excessive space and high pressure for storage
vii. commercially available
viii. *Key components are valves and its accessories, actuators, flexible discharge and connection hoses, check valves, pressure switch, and nozzles

c) Design Condition
i. The hazard space volumes shall be protected from a common central or individual supply, the cylinder bank or individual cylinder system, with corresponding pipes and nozzle system.
ii. The individual zone/ system shall be dimensioned to give a complete discharge of the agent in less than 10 seconds into the affected zone.
iii. The software calculation shall be approved VdS or FM / UL. The discharge time shall not exceed 10 seconds. After end of discharge (10s) a homogeneous NOVEC 1230 concentration shall be built-up in the room.
iv. The design concentration shall follow ISO 14520 or at minimum NFPA 2001 for under floor, room and ceiling space. Unless otherwise approved, room temperature for air-conditioned space shall be taken around 20□C. For non-air conditioned space, the temperature shall be taken around ambient temperature. The system shall be designed with minimum design concentration of 4.7 % as applicable to Class-A & C fire.
v. All voids within each hazard shall be discharged simultaneously. Each hazard shall have an independent system, unless otherwise specifically stated.
vi. The system engineering company should carry out the piping Isometric design and validate the same with a hydraulic flow calculation generated by using the agent's design software. Appropriate fill density to be arrived at based on the same.
vii. The system shall be so designed that a fire condition in any one protected area shall actuate automatically the total flooding of clean agent in that area independently.
viii. The entire system shall incorporate inter-alia detection, audible and visual alarms, actuation and extinguishing.

d) Clean Agent Supply System
i. The extinguishing agent shall be NOVEC 1230 with physical properties conforming to NFPA Standard 2001 or ISO 14520 standard.
ii. Each zone to be protected by the Total Flooding System shall be capable of being flooded independently of the other.

e) Re-Filling and Maintenance
i. In case of any leakage or accidental discharge of the agent, it should be possible to re-fill the cylinders in India itself.
ii. The bidder should indicate the source of re-filling and the time that will be taken for re-filling and replacement.188

f) Storage of Extinguishing Agent

i. The agent shall be stored in liquid form at ambient temperature in high-pressure seamless cylinder containers designed for the purpose. The cylinder shall be high pressure, seamless, flat type and concave bottom.
ii. As per the regulations of the Chief Controller of Explosive (CCE) Nagpur, any system which has a working pressure above 19 bar will require the use of seamless cylinders that have been duly approved by the CCE, Nagpur.
iii. Each cylinder shall have its own built-in pressure safety relief valves and shall also be equipped with pressure gauge to indicate the pressure of its content.
iv. The cylinders shall be super-pressurized with dry Nitrogen to 42 Bar. The cylinder shall be capable of withstanding any temperature between -30 Deg C and 70 Deg C.
v. All cylinders shall be distinctly and permanently marked with the quantity of agent contained, the empty cylinder weight, the pressurization pressure and the zones they are protecting.
vi. All cylinders shall be adequately mounted and supported in a manner to facilitate individual servicing or content weighing.
vii. Cylinders installed shall be of the same size where possible and the manifold shall be provided with non-return or check valves to prevent back flow when any cylinder is being removed for maintenance.

g) Piping and Fittings
i. All piping shall be Schedule 40 seamless pipes complying with grade B and all fitting shall be of ASTM A-105.

h) Discharge Nozzles
i. Discharge nozzles shall be manufactured in corrosion resistant material and shall be positioned in a manner to effect a uniform concentration at the shortest time after discharge. Each nozzle shall be able to cover a height of 5m effectively.

i) Detection
i. The detection part shall consist of the installation of an adequate number of smoke detectors strategically positioned for the early detection of smoke, and/or products of combustion. All detectors shall be ULI, FMRC and/or LPC or Vds approved.
ii. The detection of smoke by such detectors shall immediately set of an audible alarm at the control unit and visual indication of the zone where smoke has been detected.
iii. The detectors in each zone protected by Total Flooding System shall be wired on a DUAL RISK CIRCUIT basis. The actuation of one detector in a zone shall not be sufficient to cause the discharge of the agent. The agent shall only be actuated to discharge on activation of another adjacent detector in that zone.
iv. The signal from the second activated detector within the particular zone protected by the Total Flooding System shall after a time delay activate the agent release device of the Total Flooding System. The time-delay circuit shall have a delay period adjustable from zero second to 180 seconds.

j) Documentation:
i. The system engineering company should prepare & submit along with the bid documents, the piping Isometric drawing and support the same with a hydraulic

flow calculation generated by using the agent's design software. The calculations shall validate the fill density assumed by the bidder.

ii. The bidder shall submit copies of the datasheets of the hardware used in the system.

iii. The bidder shall also submit copy of CCE approval letter for the cylinder proposed to be used.

iv. The bidder shall also submit calculations to evidence the quantity of agent considered for the system.

v. The successful vendor must submit, along with the supply invoice, a certificate of authenticity, for the agent from the system engineering company duly checked and verified by distributor.

vi. The system engineering company should provide, as part of the handing over, the As built drawings and operation & maintenance manual.

5.2.2.13. Rodent Repellent System

a) It would consist of :-

i. Controllers –Be capable of generating variable high frequency electronic signals that are ultrasonic in nature (20 KHz to 50 KHz) and these signals shall be transmitted to the transducers for emission all around.

ii. Transducers – To cover an open area of 300 Sq.ft. minimum with an average ceiling height of 10ft.

1	Operating Frequency	Above 20Khz
2	Power Consumption	15W max
3	Sound Output:	80db to 110db (at 1m)
4	Power output	800mW per transducers

5.2.2.14. Water Leak Detection System

It consists of:-

a) Water Leak Detection Panel

The water Leak detection panel consists of multiple zones. These controllers shall have MODBUS/BAC net output to be integrated with BMS system. The features are as under:-

i. Alphanumeric LCD Display with the minimum of 3Lines

ii. Soft Touch Membrane Keypad

iii. LED Indication of the events like power, Alarm & Fault

iv. Password protected event log facility

v. Remote monitoring via MODBUS/BAC net protocol

vi. Configurable sensitivity adjustment

vii. Dedicated Hooter output for local alarm

b) Water Leak Sensing Cable

i. Water leak sensing cable shall be mechanically strong, resistant to corrosion and abrasion.

ii. It shall be constructed with two sensing wires, an alarm signalling wire and a continuity wire constructed by fluoropolymer carrier.

iii. It shall have end circuit to detect open circuit fault.

c) Hooter

5.2.2.15. High Sensitivity Smoke Detection System

a) High Sensitivity Smoke Detection aspiration General Description:

i. A high performance aspirating smoke detection system shall be supplied, installed and commissioned by the specialist contractor in accordance with the requirements detailed in the NFPA – 72, Aspirating Detection Systems.
ii. The system has been designed to sense incipient smoke at a very early stage in all critical rooms, namely:
   - Data Centre.
   - UPS & Battery Room
   - Technical Area
iii. The panels shall be mounted inside the risk protected and there shall be a network of air sampling pipe work.
iv. The High Sensitivity Smoke detection consist of highly sensitive Laser-based Smoke Detectors with aspirators connected to networks of sampling pipes. The alarms are generated once the laser sensor receives smoke at a pre-determined obscuration level to activate and alert, Fire 1, Fire 2 and alert signal.
v. The signal is extended to the Fire Alarm monitor Modules / BMS through Volt free contacts for further investigation.
vi. When required, it shall be possible to connect an interface card for open Protocol output to BMS system for online Monitoring with Software level integration.
vii. When required, an optional remote Display unit shall be provided to monitor each detector, and a Programmer shall be supplied to configure the system.

b) Scope of Work

i. This specification covers the requirements of design, supply of materials, installation, testing and commissioning of Aspirating Smoke Detection System. The system shall include all equipment's, appliances and labour necessary to install the system, complete with high sensitive LASER-based Smoke Detectors with aspirators connected to network of sampling pipes.
ii. The Bidder shall also make provision in the Aspirating Smoke Detectors to trip AHU and to shut fire dampers in the event of fire through the relay contacts**.**

c) Codes and standards
The entire installation shall be installed to comply one or more of the following codes and standards:

i. NFPA Standards,
ii. British Standards, BS 5839 part :1

d) Approvals
All the equipment's shall be tested, approved, and/or listed by :

i. LPCB (Loss Prevention Certification Board), UK
ii. FM Approved for hazardous locations Class 1,Div 2
iii. UL (Underwriters Laboratories Inc.), US

iv. ULC (Underwriters Laboratories Canada), Canada
v. Vds (Verband der Sachversicherer e.V), Germany

e) Design Requirements

i. The System shall consist of a high sensitive LASER-based smoke detector, aspirator, and filter.
ii. It shall have a display featuring LEDs and Reset/Isolate button. The system shall be configured by a programmer that is either integral to the system, portable or PC based.
iii. The system shall allow programming of:

- Multiple Smoke Threshold Alarm Levels
- Time Delays.
- Faults including airflow, detector, power, filter block and network as well as an indication of the urgency of the fault.
- Configurable relay outputs for remote indication of alarm and fault Conditions.
- It shall consist of an air sampling pipe network to transport air to the detection system, supported by calculations from a computer-based design modelling tool.
- Optional equipment may include intelligent remote displays and/or a high level interface with the building fire alarm system, or a dedicated System Management graphics package.

iv. Performance Requirements

- Shall provide very early smoke detection and provide multiple output levels corresponding to Alert, Action, and Fire 1 & 2. These levels shall be programmable and shall be able to set sensitivities ranging from 0.025 – 20% obscuration / meter.
- Shall report any fault on the unit by using configurable fault output relays or via the graphics Software.
- Shall monitor for filter contamination.
- Shall incorporate a flow sensor in each pipe and provide staged airflow faults.

f) Materials and Equipment's

i. The Laser detection Chamber shall be of the mass Light Scattering type and capable of detecting a wide range of smoke particle types of varying size.
ii. A particle counting method shall be employed for the purposes of preventing large particles from affecting the true smoke reading.
iii. Monitoring contamination of the filter (dust & dirt etc.) to notify automatically when maintenance is required.
iv. The Laser Detection Chamber shall incorporate a separate secondary clean air feed from the filter; providing clean air barriers across critical detector optics to eliminate internal detector contamination.

v. The detector shall not use adaptive algorithms to adjust the sensitivity from the set during commissioning. A learning tool shall be provided to ensure the best selection of appropriate alarm thresholds during the commissioning process.

g) Detector Assembly

i. The Detector, Filter, Aspirator and Relay Outputs shall be housed in a mounting box and shall be arranged in such a way that air is drawn continuously from the fire risk area by the Aspirator and a sample passed through the Dual Stage Filter and then to the detector.
ii. The detector shall be LASER-based and shall have an obscuration sensitivity range of 0.025 – 20% obs/m.
iii. The detector shall have four programmable smoke alarm thresholds across its sensitivity range with adjustable time delays for each threshold between 0 - 60 seconds.
iv. The detector shall also incorporate the facility to transmit a fault through a relay.
v. The detector shall have a single pipe inlet that must contain an ultrasonic flow sensor. High flow fault (urgent and non-urgent) and low flow fault (urgent and non-urgent) can be reported.
vi. The filter must be a two-stage disposable filter cartridge. The first stage shall be capable of filtering particles in excess of 20 microns from the air sample. The second stage shall be ultra-fine, removing more than 99% of contaminant particles of 0.3 microns or larger, to provide a clean air barrier around the detector's optics to prevent contamination and increase service life.
vii. The aspirator shall be a purpose-designed rotary vane air pump. It shall be capable of allowing/ supporting for a single pipe run / multiple sampling pipe runs with a transport time of less than 90 seconds.
viii. Detectors shall be capable of supporting a single pipe run of 25m with a maximum transport time of 120 seconds or as appropriate standards dictate.
ix. The Assembly must contain relays for fire 1, Action and fault conditions. The relays shall be software programmable (latching or non-latching). The relays must be rated at 2 A at 30V DC. Remote relays shall be offered as an option and either configured to replicate those on the detector or programmed differently.
x. The Assembly shall have built-in event and smoke logging. It shall store smoke levels, alarm conditions, operator actions and faults. The date and time of each event shall be recorded. Each detector (Zone) shall be capable of storing up to 18000 events.

h) Displays on the Detector Assembly

i. The detector will be provided with LED indicators.
ii. Each Detector shall provide the following features at a minimum.
iii. Alert, Alarm, Fire 1 and Fire 2 corresponding to the alarm thresholds of the detector.
iv. Smoke Dial display represents the level of smoke present.
v. Fault Indicator.
vi. Disabled indicator.

vii. Buttons supporting the following features shall be accessible to authorized personnel.
viii. Reset – Unlatches all latched alarm and faults.
ix. Disable – Disables the fire relay outputs from actuating and indicates a fault.

i) Sampling Pipe

i. The sampling pipe shall be smooth bore with an outside diameter of 25mm and internal diameter of 21mm should be used.
ii. The pipe material should be suitable for the environment in which it is installed or should be the material as required by the specifying body.
iii. All joints in the sampling pipe must be air tight and made by using solvent cement except at entry to the detector
iv. The pipe shall be identified as Aspirating Smoke Detector Pipe along its entire length at regular intervals not exceeding the manufacturer's recommendation or that of local codes and standards.
v. All pipes should be supported at not less than 1.5m centres, or that of the local codes or standards.
vi. The far end of each trunk or branch pipe shall be fitted an end cap and drilled with a hole appropriately sized to achieve the performance as specified and as calculated by the system design.

j) Sampling Holes

i. Sampling Holes of 2mm, or otherwise appropriately sized holes, shall not be separated by more than the maximum distance allowable for conventional detectors as specified in the local codes & standards. Intervals may vary according to calculations.
ii. Each sampling point shall be identified in accordance with Codes or Standards.
iii. Consideration shall be given to the manufacturer's recommendations and standards in relation to the number of Sampling Points and the distance of the Sampling Points from the ceiling and roof structure and forced ventilation systems.

k) Installation

i. The Contractor shall install the system in accordance with the manufacturers recommendation.
ii. Where false ceilings are available, the sampling pipe shall be installed above the ceiling and Capillary Sampling Points shall be installed on the ceiling and connected by means of a capillary tube.
iii. The minimum internal diameter of the Capillary tube shall be 5mm, the maximum length of the capillary tube shall be 2m unless the manufacturer in consultation with the engineer have specified otherwise.
iv. The Capillary tube shall terminate at a ceiling Sampling Point specifically approved by the Client. The performance characteristics of the sampling points shall be taken into account during the system design.

v. Air Sampling Piping network shall be laid as per the approved pipe layout. Pipe work calculations shall be submitted with the proposed pipe layout design for approval.

l) Testing

i. Commissioning Test

- Commissioning of the entire installation shall be done in the presence of the owner and/or its representative.
- All necessary instrumentation, equipment, materials and labour shall be provided by the Contractor.
- The Contractor shall record all tests and system calibrations and a copy of these results shall be retained on site in the system Log Book.

ii. Functional Test

- Introduce Smoke into the Detector Assembly to provide a basic functional test
- Introduce smoke to the least favourable Sampling Point in each Sampling Pipe. Transport time is not to exceed 120 Seconds.

m) Documentation

i. The bidder shall be authorized and trained by the manufacturer to design, install, test and maintain the Aspiration Smoke Detection system and shall be able to produce a certificate issued by the manufacturer along with the offer.
ii. The bidder shall submit computer generated software calculations for design of aspirating pipe network, on award of the contract.
iii. Product data and performance criteria shall be submitted by the bidder.
iv. The bidder should provide, as part of handing over, the as-built drawing, operation manual and maintenance manual. The as-built drawing shall exactly match the Sampling pipe layout with the pipe software calculation.

5.2.2.16. Raised Floor

Providing and fixing Access floor systems as per EN 12825 or equivalent standards.

a) System:

i. Access floor system to be installed at finished floor height of maximum 600 mm from the existing floor level.
ii. The system will provide for suitable pedestal and under-structure designed to withstand various static loads and rolling loads subjected to it in an office / server / DCS / panel / rack area.
iii. The entire Access floor system will provide for adequate fire resistance, acoustic barrier and air leakage resistance.

b) Panels:

i. Panels will be made up of inert material Calcium sulphate. The bottom of the panel shall be of Aluminium foil to create a fire and humidity barrier and this

should provide floor's electrical continuity. Panels will remain flat through and stable unaffected by humidity or fluctuation in temperature throughout its normal working life. The Panels will be UL listed/FM/DM approved.

ii. Panels will provide for impact resistance top surfaces minimal deflection, corrosion resistance properties and shall not be combustible or aid surface spread of flame.
iii. Panels will be insulated against heat and noise transfer.
iv. Panels will be 600 x 600mm x 30 mm height fully interchangeable with each other within the range of a specified layout.
v. Panels shall rest on the grid formed by the stringers which are bolted on to the pedestals.
vi. Panels shall be finished with anti-static 0.9 mm Laminate and 0.45 mm thick plastic edge material that is self-extinguishing and will be PVC free

c) Panel Loading

i. Concentrated point load: 450Kgas per European standard EN 12825*.
ii. Uniformly Distributed Load (UDL): 1200 Kg/M2.

d) Fire Rating:

i. The Panels will confirm to class O and Class 1 Fire Ratings tested as per CIRC 91/61 or BS 476 Part 6 & 7 (60 min).

e) Pedestals:

i. Pedestal installed to support the panel will be suitable to achieve a finished floor height of 600mm. Pedestal design will confirm speedy assembly and removal for relocation and maintenance. Pedestal base to be permanently secured to position on the sub-floor.
ii. Pedestal assembly will provide for easy adjustment of levelling and accurately align panels to ensure lateral restrain. Pedestals will support an axial load of 1500 Kgs, without permanent deflection and an ultimate load of 3000 Kgs. Pedestal head will be designed to avoid any rattle or squeaks.

f) Pedestal Assembly

i. The structure is made entirely of galvanized steel consisting of hexagonal shaped, 89 mm diameter, and 1.5 mm thick base plate, with 6 shaped stiffening ribs with niches that improve adhesion and with 5 holes mechanical fastening to the ground.
ii. The assembly will provide a range of height adjustment up to 25mm, with the help of check nuts.

g) Under structure:

i. Under structure system consists of stringers of size 525 x 30x 25 x 0.8 mm thick to form a grid of 600 x 600mm. These stringers are locked into the pedestal head and run both ways.
ii. The US system will provide adequate solid, rigid and quiet support for access floor panels.

iii. The US system will provide a minimum clear, uninterrupted height of 600 mm between the bottom of the floor and bottom of the access floor for electrical conducting and wiring.

h) Stringers:

i. Stringer system is composed of a special frame, made of pressed galvanized steel plate and with a section 25mm wide, 30 mm high and 0.8 mm thick. The longitudinal ribs and flaps in the lower part should be designed to increase flexion resistance.
ii. The grid formed by the pedestal and stringer assembly will receive the floor panel.

i) Floor Insulation:

i. The floor and ceiling slabs should be heat-insulated, or coated with a heat insulating material to avoid condensation on floors below and above and to reduce the heat transfer in the server/network room area.
ii. The insulation shall be done with either 16 or 13 mm thick self-adhesive aluminium foil face nitrile rubber. The floor and ceiling shall be coated with epoxy paint.
iii. The floor insulation should cover for true floor and true ceiling, this will not allow the thermal conductivity.
iv. The server & other required area should be equipped with raised floor with 600 mm (24 inch) height. Cavity floor shall have false flooring panels of 18 gauges steel 600 x 600 coated with APDCL Page: TSA – 2 50 micron epoxy conductive paint.
v. Floor shall be finished with 2mm thick antistatic high pressure laminate with 2mm thick PVC trim edge all-round.
vi. The interior of the panels shall be filled with non-combustible Cementous compound.
vii. The raised floor distributed load should not be less than 1200 Kg/Sqm.

5.2.2.17. False Ceiling

False Ceiling at appropriate height should be installed concealing any cabling tray and electrical lighting wiring in all areas.

a) Server room

i. False ceiling shall be provided with Armstrong Lay in (Hot dipped galvanized steel) metal ceiling system 600 x 600 x 5mm with
standard perforation of 2.5 mm die (16% open space) and fleece with NRC of 70 & CAC 36 to be laid on Armstrong grid system.
ii. Armstrong Orcal Lay in metal ceiling System consisting of 600x600mm lay in tiles of pre coated galvanised steel in 0.5 mm thickness in white colour with standard perforation of 2.5mm die & open area of 16%.
iii. The back of the tile should have black acoustical fleece with NRC of 0.70 & CAC 36 to be laid on Armstrong grid systems with 15mm wide T - section

flanges Colour white having rotary stitching on the Main Runner, 1200 mm & 600 mm Cross Tees, fixed to the structural soffit by Butterfly clip hangers, suspension wires & anchor fasteners as per the manufacturer's specification.

iv. Suspension wires to be provided at every 600mm c/c with two no's of ties on each anchor fastener, Perimeter trim of Trulok wall angle in white colour secured to wall at 450mm maximum centres.

b) Other Areas

i. Acoustical false ceiling of mineral fibre Board (600 x 600 x 15mm) of Armstrong (ELIT RH99) of Equipment. Laid on Grid system (Micro lock edge) with 15mm thick T section(White) having main runner 1200mm x 600mm, cross Tee at 295 HT.

ii. Mineral Fibre Board modular False Ceiling in Armstrong in Board edge Fissured ANF tiles of size 600mX600mmX15mm having Noise reduction Co-efficient 0.5, light reflection over 75%, Relative Humidity 99%, fire performance class0/class1 (BS 476) 24XL - Hot Dipped Galvanized Steel Suspension System having rotary stitching on main runner, 1200 mm & 600 mm cross tees with 15mm wide flanges of white colour with standard perforation of 2.5mm dia. (16% open space) fleece with NRC of 0.70 & CAC 36, fixed to the structural soffit by Butterfly clip hangers, suspension wires & anchor fasteners as per the manufacturer's specification, Suspension wires to be provided at every 600mm c/c with two no's of ties on each anchor fastener, Perimeter trim of Trulok wall angle in white colour secured to wall at 450mm maximum centres.

iii. The False Ceiling tile should be Dust free type and of Non-combustible material. Each False Ceiling tile (preferably 600mm x 600mm) should be individually removable for access to area above False Ceiling.

iv. The false ceiling area should cover with as per layout. The contractor should propose the right quantity. `

5.2.2.18. IIM Specification

The Intelligent Infrastructure Management/ Data Center Infrastructure Management solution offered must be ready to meet the following critical requirements:

S.No.	Minimum Technical Requirements
1	The solution should be capable of tracking device history for networked end devices including the following forensics details: • When device was first connected to the network • If and when it was removed from the network • If and when it was moved from one physical location to another • How long it has been active or inactive. • Asset, configuration and change management
2	The solution should be fully comply with ANSI/TIA 606-B (including B-1) and ISO/IEC 18598 standards.
3	The solution should be based on a designated IIM Hardware which deliver physical connectivity information to the management software

4	The Physical Layer Management solution should be strictly based on the physical detection of patch cord connectivity.
5	The solution should provide the capability of electronically tagging any network equipment such as network printer, servers, IP Camera, desktop, switches, modems, etc.
6	The system should be robust and should report the patching connectivity information as complete ONLYwhen the two ends of the same patch cords are connected and should not get confused by any subsequent insertion of any other patch cord.
7	Patch cord removal from Panel / Switch side should be monitored and alerts like email/SMS should be sent even if one end of the patch cords removed.
8	No need for manual acknowledge at the patch panel port if a cord has been inserted on the switch side. (Manual acknowledge means: push button adjacent to a specific port).
9	The solution should provide the technician an easy method of patching with- out imposing any specific sequence rules/order for the patching, thus allowing the technician to carry patching work orders as in the case of a non-intelligent solution including physical location.
10	The solution should provide the capability to automatically monitor 24/7 of remote sites network links and verify network availability all the time. In case of a link brake, the solution should send a real time event & alarm.
11	The solution should provide the capability to automatically connecting to a remote DB sites as well as to a local DB
12	The solution should provide the capability to automatically monitor 24/7 of a major network link verifying network availability all the time. In case of secure link brake, the solution should send a real time event & alarm.
13	The solution shall be able to maintain a record of the rack capacity and utilization including: • Total rack space and occupied rack space • Total number of available IIM panel ports • Total number of non-IIM panel ports • Total number of switch ports and “switch utilization” • Total number of PDU power outlets (if applicable) • Total number of env. Sensors (if applicable)
14	The solution should be able to monitor on-line of patch cord removal from either side : • Between intelligent panels • Between intelligent panel to active device like Switch.
15	The solution should have the following visual indications: • LED above each port - indicating patching rough, parching work order pending and correcting bilking mode in case of patching mistake. • LED per each patching frame – indicating panel status. • Sound – in case of patching or removal of a cord between either intelligent panels or between intelligent panels to a switch. • Rack indicator – the solution should support rack indicator (beacon) in order to guide the work order executer to the specific work order cabinets/racks.
16	All Changes of the telecommunications infrastructure facilities and networked devices should be maintained within the IIM systems to keep track of current activities and completed activities including: • Real time tracking of authorized and unauthorized patching activities

	• Generation of move, add, change work orders • Providing means for retrieval of work orders at racks with IIM equipment using port LEDs, tablet • Automated tracking of work order completion • Scheduled work order and work order history • Monitoring and alerting on connected information
17	The solution should provide the capability of monitoring port availability status on network equipment including switches, patch panels and telecommunication outlets should be monitored in real time for the purpose of detecting unexpected or unauthorized activities.
18	The solution should be able to communicate and exchange data with other system using of standard protocols and database formats (e.g. SNMP, SQL).
19	The solution should provide the capability of monitoring any Physical link port type including copper and fiber
20	The solution should be ready to integrate to IP power strips to get information of the power being consumed in the racks in real time and use this information for provisioning of servers inside any communication room.
21	The solution should be ready to connect to devices which control various parameters in the Data center / Hub room environment (temperature sensors, humidity sensors, door access sensors,etc.) and provide this information to the software in real time.
22	The solution should provide the capability to automatically check the possible movement of any device to a new location by verifying the network availability with any proposed setting, providing the patching information with options and creating a work order for the same. All this is to be achieved by a mere drag and drop operation.
23	Based on the information of network provisioning, space available in the racks and the real time power being consumed, the solution should be able to automatically provision any new device in a data center and provide the required work order. All this is to be achieved by a mere drag and drop operation.
24	The solution should be capable to handle multiple provisioning operations to reduce the time of such operations drastically.
25	The solution should offer as a built in feature the possibility to report any unauthorized MAC outside the white list of MACs allowed on the site.
26	The solution should be capable to block switch ports automatically on intrusion detection. This capability however should be selectable by the user depending on the critical nature of the location.
27	The solution should provide visual representation of the datacenter environment specially to view the power consumption status in the racks at one go.
28	The solution should be capable to detect IP Phones connected along with Computers.
29	The software should provide a location based security to manage authorized /un authorized connectivity. The security should be per port /desk/room/floor basis.
30	The solution should have inbuilt dashboard which should show switch/panel port utilization.
31	The solution should be capable to detect and report about device connection and identify the associated location. This information can be used to establish whether this is an authorized connection in order to respond appropriately.
32	The solution should provide a comprehensive open-ended solution e.g. an SDK (software development Kit) and not just the capability to send SNMP traps to integrate the solution with any 3rd party software or in-house software.

33	Integration can be done via: SNMP traps, XML, database sharing and web services.
34	The solution should be provided with an unlimited user/viewer licenses. This is important to enable use by multiple users/viewers.
35	The IIM solution should include out of the box support on environment sensors like temperature, humidity and others.
36	The info of these sensors must be shown in the client application screen and saved in the system database.
37	The scanning devices should automatically detect the panel type; the scanning devices are connected to, and should also automatically detect the connectivity between the scanning devices. This is necessary for automatic & error free real time detection & installation of hardware components in the software.
38	The solution should offer flexibility to extend the panel scanning capability to distances more than 7 feet (one rack) in order to cover more than a single rack.
39	The solution connectivity, between the different scanning appliances, should be based on RJ-45 cords.
40	Since all the upper & center units of the rack (critical real estate space in rack) will be required to mount panels or switches to provide a hassle free environment for their control and installation, the scanning devices would be mounted either at the top or bottom of the rack. Hence it is important that the scanning devices should carry a design such that they require minimum interaction during any work order execution and do not force any change in the rack design to enable their functioning.
41	The solution should be efficient and should not require use of multiple media for providing or verifying of the same information or carrying out a work order. Any work order execution should be achieved by means of lights without requiring any other interface. This is essential to ensure easy usage of the system.
42	It should have the ability to connect and provide data center environment reports like power consumption in racks in real time, temperatures within racks, rack door closures, water level sensing etc.
43	All Components Passive and active Components should be RoHS (Restriction of Certain Hazardous Substances) complied.
44	Declaration –RoHS Compliant should clearly be mentioned on datasheets of each Passive Components (Copper &Fiber).
45	There should be 20 year cabling performance warranty and Application Assurance
46	The solution must offer RJ-45, LC and MPO/MTP intelligent panels and cords
47	Fiber cable should be Zero Water peak
48	SM Fiber cable should compatible to banded insensitive compliant according to the ITU-T G.657 A Standard
49	MM Fiber cable should compatible to banded insensitive compliant according to the ANSI/TIA 568C.3 Standard
50	The solution should support tablet/smart phone in order to present the work orders.
51	Intelligent Modular Copper Frames
51.1	The Copper Frame should be a high-performance, cost-effective panel.
51.2	The Copper Frame should supports RJ-45 modular jacks for simple and modular architecture.
51.3	The Copper Frame should support mixed cross-connect and interconnect network topologies.
51.4	The Copper Frame should be a managed frame that supports up to 24 RJ-45 modular jacks.
51.5	The Copper Frame should have a single LED above each port

51.6	The Copper Frame should include a multi-mode LED and push button to assist technicians in monitoring, configuring, and troubleshooting
51.7	By incorporating a unique ID device within the frame and working together with autosense topology, the location of each frame within the network as well as its position within a rack should be available at all times, even after a frame has been relocated.
51.8	The Copper Frame back panel should support a socket for the Scanning Card that commands the port LEDs and patch cords, and also enables reading of the intelligent ID devices.
52	Copper Patch Cord
52.1	Should be High performance CAT6A copper Patch Cords support Intelligent cross-connect and interconnect topologies.
52.2	Based high-end CAT6A STP cord, the cord supports two additional stranded wires to produce an eight-wire cord. The cord is terminated with patented RJ-45 plugs that include two conductive, external contacts.
52.3	The cross-connect topology should include two intelligent ID devices, one on each end of the patch cord, while the interconnect topology includes one intelligent ID device at the switch side
52.4	The plugs on the interconnect patch cord are fitted with a dummy latched cover that enables easy plug insertion and removal from the frame or switch.
52.5	Cords must be under testing verification program by 3rd party lab certification like: ETL/SEMKO/ Delta or 3P.
53	Copper Interconnect Patch Cord
53.1	Should Comprise of 8 data-wires Category6A S/FTP flexible patch cable + 2 control wires, terminated with two fully shielded RJ-45 plugs at each end with two external ID contacts
53.2	Should be Non-molded flexible boot for enhanced life and reliability
53.3	Should Conform to ANSI/TIA-568-C.2, ISO/IEC 11801 2.1 edition and CENELEC EN50173 (2007) standards for Category 6A/CLASS EA
53.4	Should be Backward compatible with Category 5e and 6 – UTP and STP
53.5	Should be 100% tested at the factory
53.6	Cords must be under testing verification program by 3rd party lab certification like: ETL/SEMKO/ Delta or 3P.
54	Copper Cross Connect Patch Cord
54.1	Should Comprise of 8-wires Category6A S/FTP flexible patch cable, terminated with two fully shielded RJ-45 plugs at each end with two external ID contacts
54.2	Should be Non-moulded flexible boot for enhanced life and reliability
54.3	Should Conform to ANSI/TIA/EIA-568-C.2, ISO/IEC 11801 2.1 edition and CENELEC EN50173 (2007) standards for Category 6A/CLASS EA
54.4	Should be 100% tested at the factory
54.5	Cords must be under testing verification program by 3rd party lab certification like: ETL/SEMKO/ Delta or 3P.
55	Copper keystones:
55.1	Should have 8 internal contacts only.
55.2	The solution will support C5e, C6 and C6A shielded and un-shielded keystones types.
56	Intelligent Fiber Trays (Intelligent Tray without Cassette)
56.1	The Fiber Tray supports mixed cross-connect and interconnect network topologies.

56.2	The Fiber Tray should supports three types of fiber patching options: LC-LC, LC-MPO, and MPO-MPO.
56.3	The Fiber Tray should supports both Single-Mode (SM) and Multi-Mode (MM) OM4 fiber types.
56.4	By incorporating a unique ID within the tray and two external contacts in each port in the tray, it should be possible to achieve system-wide ID polling and message routing. This allows unique monitoring, control, and maintenance of the system.
56.5	The Fiber Tray should be a high-end fiber optics-managed tray that supports up to 96 LC-LC fiber strands (LC-LC and LC-MPO) along with a full management system.
56.6	To assist in monitoring, configuring, and troubleshooting, the Fiber Tray should include a bi-color LED on the tray and a single LED above each port in the cassette.
56.7	The Fiber Tray should contain a push button that enables you to initiate manual port scanning for viewing system connectivity.
56.8	The Intelligent LC-LC Fiber Tray supports two Scanning cards and two RJ-45 ports with keystones for connections to the Scanning Device /Analyzer ports.
56.9	Supports a simple, modular architecture with up to four cassettes; each cassette with 24 ports
56.10	Should support 96 fibers (48 duplex LC ports) in 1U format for LC, MPO, splitter/pigtail cassette installation and in mixed interconnect and cross-connect topologies
56.11	Should provide an individual LED on each port, which assists in visual monitoring and maintenance
56.12	Should provide a unique Intelligent ID to each of the four cassettes and internal PCB for system- wide identification and determination of cassette position within the chassis
56.13	The tray can support 1, 2, 3 or 4 cassettes in different location.
56.14	At any case, the fiber adapters (either LC or MPO) should not include any internal metal connectivity contacts (as part of the patching sensing). Any patching contacts must be external to these fiber adapters.
57	Intelligent Fiber LC Cassettes
57.1	Front connection (patch cord side) should have 12 x LC duplex adapters
57.2	Back connection (cabling side) should have 12 x LC duplex adapters
57.3	Should have one pair of LEDs for each port on the front panel (that is, one LED for each fiber).
57.4	LEDs should show the status of ports.
57.5	Should comply to EN 55022, Class B (Europe) compliant & FCC Part 15, subpart J, Class A (USA) compliant
58	Intelligent Fiber LC MPO Cassettes
58.1	Front connection (patch cord side) should have 12 x LC duplex adapters (MM or SM)
58.2	Back connection (cabling side) should have 2 x MPO adapters
58.3	Should have One pair of LEDs for each port on the front panel (that is, one LED for each fiber).
58.4	LEDs should show the status of ports.
58.5	The port LEDs can be activated by command from the network management station.
58.6	Attenuation should not greater than 0.5 dB
58.7	Should comply to EN 55022, Class B (Europe) compliant & FCC Part 15, subpart J, Class A (USA) compliant

59	Fiber Cords
59.1	All Intelligent Patch Cords should support both interconnect and cross-connect topologies.
59.2	Patch cords are designed for Single-Mode and Multi-Mode applications at 10G/40G/100Gbps.
59.3	Cross-connect topology should include two Intelligent ID devices, one on each end of the patch cord. The cord should include fiber plug interface with unique ID on both ends.
59.4	Interconnect topology should include one intelligent ID device at the switch side. The cord includes fiber plug interface with two external pins on both ends
60	Fiber Cords LC Interconnect Intelligent Patch chord
60.1	Should be Designed for Intelligent application and as stand-alone cord
60.2	Should be Available with two fiber types – Single-Mode and Multi-Mode 50/125 OM4
60.3	Should Comply to IEC 60332-3C IEC 61034 IEC 60754
60.4	The Jumper should meets the requirements of ANSI/TIA/EIA-568-C.3
61	Fiber Cords LC Cross Connect Intelligent Patch chord
61.1	Should be Designed for Intelligent application and as stand-alone cord
61.2	Should be Available with two fiber types – Single-Mode and Multi-Mode 50/125 OM4
61.3	Should Comply to IEC 60332-3C IEC 61034 IEC 60754
61.4	The Jumper should meets the requirements of ANSI/TIA/EIA-568-C.3
62	Fiber Cords MPO -MPO Cross Connect Intelligent Patch chords
62.1	Should be Designed for Intelligent applications
62.2	Connectors should be compliant with FOCIS-5D standard
62.3	Should be Fully compatible with 40G and 100G* IEEE 802.3 applications
62.4	Should be Available in several lengths
62.5	Should comply to IEC 60332, IEC 61034, IEC 60754
62.6	The Jumper should meet the ANSI/TIA-568-C.3 requirements.
63	Intelligent Scanning Card
63.1	The Card should be a pluggable device that supports physical network identification on interconnect and cross-connect topologies.
63.2	The Card should automatically detect and reads up to 24 Intelligent ID devices present on each Copper Frame or Fiber Tray and on patch cords.
63.3	The Card should routes commands to the port LEDs located above each panel port.
63.4	Every Card should contain unique ID information, enabling proper identification and communication on the Intelligent Infrastructure Management (IIM) network.
63.5	The Card should be connected via a socket on the back of the frame using dual mounting latches, locking it securely in place for enhanced reliability.
63.6	The Card should communicate with higher-level system components through a standard RJ-45 connector.
63.7	The Card can be added in later stages of the installation.
68	Scanning Hardware /Scanner / Analyzer
68.1	Should support mixed cross-connect and interconnect network topologies
68.2	Should allow ease of expansion, control, and management of an unlimited number of ports in real time.
68.3	Should support copper and fiber solutions, both individually and in a mixed configuration in the same system, with 10 Gbps and 40/100 Gbps.

68.4	Solution does not interfere with the actual network data. Therefore its communication over the network does not cause any load on the network.
68.5	Should give LED signalling of make/break status
68.6	Should support Tablet application for work orders
68.7	Should Support Environmental Controller
68.8	Should support SDK for easy interfacing to other application
68.9	Each scanning hardware should supports up to 24 Cards, with each Card capable of supporting 24 ports, resulting in a single device capable of supporting up to 576 ports.
68.10	The scanning hardware should supports up to four TCP/IP ports through an internal L2 switch, saving on ports in the main switch and enabling cascading of scanning hardware to provide unlimited network expansion.
68.11	Should also support connectivity to other network IP devices such as PDUs.
68.12	The Scanning hardware should support installation in zero-U configuration for rack space optimization. in case its needed the device can be installed also in 1U configuration.
68.13	The Scanning hardware should support connections to external devices such as a tablet PC (via mini-AB USB connector) and any USB device such as a flash drive (via a host type A USB socket).
68.14	The Scanning hardware should be powered through the mains supply via a power socket on the rear, and supplies power to the Cards over the RJ-45 connector.
68.15	Scanning hardware Power Input Voltage: 100–240 VAC, 47–63 Hz and Input Current: 1–2 A
68.16	Scanning hardware Power average Consumption: 11 W
68.17	Should not include any fan.
69	Tablet
69.1	The tablet supports performing work orders (MACs) in an easy and user-friendly manner.
69.2	The tablet should support multi-tasking MAC at the same time and have the ability to monitor whole infrastructure network.
70	ID Key Reader
70.1	Should be used for Learning Mode only
70.2	Builds the ID database of the Switch modules & ports
70.3	Should support LC duplex or RJ-45 male connectors
70.4	Should have Mini USB for tablet connection
71	Intelligent Copper ID Key
71.1	Intelligent ID Key that stores useful link information such as switch, rack, cable type, and revision level
71.2	Standard should be IEC 60603-7 compliant
72	Intelligent Fiber ID Key
72.1	The Return Loss should be $\geq$ 55 dB (UPC)
72.2	Attenuation Tolerance should be: 0.2 dB ± 0.05
72.3	Should Comply with ANSI/TIA-568-C.3
72.4	Should comply with Flammability – UL94V0

5.2.2.19. SIEM Specification (SOC component)

S.No	Minimum Technical Requirement
1	SIEM solution should provide capabilities of filtering unwanted logs at Logger layer and forward only meaningful security logs to Correlation layer for better performance and reduction of false positive.
2	The solution should be a hardware/software system with following components: a. Management & Reporting b. Normalization and Indexing c. Correlation Engine d. Data Management
3	There should be no limitation on number of devices to be supported. Any addition in no. of devices should have no cost impact on department.
4	The SIEM & Log Monitoring solution should be from a different OEM than the Prevention Security solutions like F/W, IPS, HIPS, AV, DLP,.
5	The solution should provide an integrated SOC dashboard and Incident analysis system that could provide a single view into all the analysis performed across all the different data sources and should have capabilities to ingest all different data sources but not limited to log, threat intelligence, vulnerability feed, IP Flow etc. The Tool should have role based access control mechanism and handle the entire security incident lifecycle .
6	Real time contextual information should be used at collection/normalization layer and also be available at correlation layer where any events are matched during correlation rule processing. In addition solution must provide contextual Hub at investigation layer for all relevant contextual awareness data regarding alerts/incidents available for any information asset like IP/Device etc.
7	All logs that are collected should be studied for completeness of information required, reporting, analysis and requisite data enhancement, normalization should be performed to meet the reporting and analysis needs.
8	Solution should be consolidated in a purpose build hardware to provide sustained 20,000 EPS and must be capable to handle burst/ spikes in traffic up to 40,000 peak EPS.
9	The solution should be storing both raw logs as well as normalized logs. The same should be made available for analysis and reporting. Solution should be sized to provide online storage till O&M period at central site. Both raw logs and normalized logs should be made available immediately, as and when required.
10	The solution should incorporate and correlate information that enables the Information Security Team to quickly prioritize it's response to help ensure effective incident handling.
11	The monitoring should be cross device and cross vendor and be both out of the box and scalable to cover additional devices and applications as required
12	Should be managed and monitored from SIEM unified console for Correlation, Alerting and Administration
13	Packet inspection solution and SIEM must integrate with each other, however they should be from different OEM. Packet inspection is preferred from specialised product vendor in this field and not just an integrated solution of SIEM vendor
14	SIEM solution must have capability to integrate with applications through an agent on web applications to monitor any attack like SQL injection, cross script etc. on application and should report to SIEM dashboard. Both solution must tightly integrate for a common dashboard.

5.2.3. ICT Software Components for Data Canter

Commencement of the date of all licenses of supplied software will start from the proposed date of Acceptance Test for the Go – Live of the component in which that software is used.

5.2.3.1. Enterprise Management System (EMS)

To ensure that ICT systems are delivered at the performance level envisaged, it is important that an effective monitoring and management system be put in place. It is thus proposed that a proven Enterprise Management System (EMS) is proposed by the bidder for efficient management of the system, reporting, SLA monitoring and resolution of issues. Various key components of the EMS to be implemented as part of this engagement are –

a) SLA & Contract management System
b) Network Monitoring System
c) Server Monitoring System
d) Helpdesk System
e) DC & DR should be in High Availability Mode for all critical services & applications.

The Monitoring system should be able to provide automated consolidated SLA reports for all the SLAs as mentioned in this RFP including real time status of various service levels achieved. The report to be available through a centralised web access / dash board the access for this to be given to at least 5 users of BSCL.
MSI will implement dedicated & integrated EMS and NMS solution to meet the SLA monitoring and other requirements as mentioned in the RFP. The implemented EMS solution to help BSCL in data driven decision making. The entire EMS implementation shall be certified by MSI also for its correctness, adequacy to meet RFP requirements and measurement of SLAs & KPIs etc.

EMS should take care of below Security parametres for API management:

i) The proposed solution should Protects against threats, OWASP vulnerabilities and controls access with Single Sign-On and identity management, providing end-to-end security for apps, mobile, and IoT.
ii) The proposed solution should support for idustry standard cryptographic algorithms (Triple DES, AES, SHA, RSA etc.)
iii) The proposed solution should Passed rigorous vulnerability tests, and integrates with any popular IAM system with support for OAuth, SAML and RADIUS.
iv) The proposed solution should be PCI-DSS compliant, and includes a built-in PKI engine, FIPS 140-2 level encryption, a robust RBAC system, and SAML support.
v) The proposed solution should be able to support OAuth, OpenID Connect, SAML, X.509 certificates, LDAP , HTTP basic, digest, SSL client-side certificate authorization etc.
vi) The proposed solution should be able to Integrate with enterprise identity, access, SSO and federation systems, LDAP, Microsoft Active Directory®/Federated Services, Oracle® Access Manager, IBM Tivoli® (TAM and TFIM), RSA ClearTrust, Sun Java™ Access Manager and Novell Access Manager etc.

vii) The proposed solution should be STIG tested ,PCI DSS certified , FIPS compliance and Common Criteria certification and other industry level certification and compliancy standards.

viii) The proposed solution should be albe to do threat detection and message content filtering.

ix) The proposed solution should be able to protect against cross-site scripting (XSS), injection attacks (Xpath SQL , XQuery etc.) and DoS attacks.

x) The proposed solution should, be able detect and filter for sensitive/confidential content with subsequent scrubbing, rejection or redaction of messages.

xi) The proposed solution should support protection against viruses.

xii) The proposed solution should support features to track failed authentications and/or violations to identify and report patterns and potential threats.

5.2.3.2. SLA & Contract Management System

The SLA & Contract Management solution should enable BSCL to capture all the System based SLAs defined in this Tender and then calculate quarterly (or for any duration) penalty automatically. BSCL desire to have a Contract Management System where the various types of contracts can be created using different templates and once drafted, those contracts will be evaluated, modified & approved through various authorities and the entire system can be configured/designed in a BPM based Workflow Solution. Measuring service performance requires incorporation of a wide variety of data sources of the project. The SLA solution should support the collection data from various sources in order to calculate Uptime / Performance / Security SLAs. Various features required in this component to EMS are :

S.No.	Description
1.	It must be a centralized monitoring solution for all IT assets (including servers, network equipment etc.)
2.	The solution must have integrated dashboard providing view of non performing components / issues with related to service on any active components.
3.	The solution must follow governance, compliance and content validations to improve standardization of service level contracts.
4.	The solution should be pre-configured so as to allow the users to generate timely reports on the SLAs on various parameters.
5.	The solution must support Service Level Agreements & Lifecycle Management including Version Control, Status Control, Effectively and audit Trail to ensure accountability for the project.
6.	The solution must have the ability to define and calculate key performance indicators from an End to End Business Service delivery perspective related to Project.
7.	The solution should support requirements of the auditors requiring technical audit of the whole system.
8.	The solution most have an integrated dashboard, view of Contract Parties & current SLA delivery levels and view of Services & current SLA performance.
9.	The solution should support SLA alerts escalation process.
10.	The solution should accept Data from a variety of formats; provide pre-configured connectors and adapters.
11.	Support for defining and calculating service credit and penalty based on clauses in SLAs.
12.	Reports (Indicative but not limited to) ▪ Ability to generate reports on penalty and credit due, to check on non-compliance of SLAs for the surveillance project ▪ Monetary penalties to be levied for non-compliance of SLA, thus the system must provide Service Level Performance Report over time, contract, service and more. ▪ Historical and concurrent service level reports for the surveillance project in order to ensure accountability of the service provider's performance ▪ Automatic Report creation, execution and Scheduling, must support variety of export formats including Spreadsheet, Word/Docs, Adobe PDF etc. ▪ Templates for report generation, Report Filtering and Consolidation and Context sensitive Drill-down on specific report data to drive standardization and governance of the surveillance project ▪ Drill-down capabilities in dashboard reports ensuring visibility for only relevant personnel of the surveillance project ▪ Real-time reports (like at-a-glance status) as well as historical analysis reports (like Trend, TopN, Capacity planning reports etc.) — Resource utilization exceeding or below customer-defined limits — Resource utilization exceeding or below predefined threshold limits
13.	The monitoring solution should have out-of-the-box integration with the proposed CMDB to relate event data to the service models in the CMDB to provide visibility into the business impact of downtime
14.	The Service impact view, Service-CI relationship, the capability to drill down from services to components in case of multiple events etc. should be built using application dependency map, discovered automatically by the Discovery Solution.

15.	The solution should have out-of-the-box bi-directional integration with the proposed service desk tool and should be able to view the ticket number in the events data and clear when ticket get resolved.
16.	The solution should have out-of-the-box integration with the proposed service desk to view the root cause of the issue, the business service affected and the CI that caused the downtime from within the Service desk
17.	The solution should have capability to enrich the events data with category, locations, owner etc from service desk system.
18.	The solution should have capability to view changes related to a CI in events console from the proposed service desk system.
19.	The solution offered by the OEM should be multitenant by nature, with a single platform for Reporting and Monitoring
20.	The OEM should have R&D and Technical Support Center based out in India

5.2.3.3. Functional & Technical Requirements for Server Load Balancer

Sr.No	Specifications
1	Physical Specification
1.1	System must of be 19-inch rack mountable 1 U form factor
1.2	System must have dedicated management port, RJ-45 console port, 6 x 1 G Interface , 1 x 2 G fibre and 4 x 10 G fibre ports
1.3	System must have dual Power supply
2	Performance
2.1	System must support 30 Gbps of L7 throughput, 64 million concurrent connection, 750 K Layer4 connection per second, 250 K 1:1 Layer7 connection per second for HTTP, 11 Gbps of SSL offloading throughput.
3	Application delivery partition/Virtual Context
3.1	System must support 60 Application delivery partition/Virtual Context
3.2	System must support dedicated configuration file for each Virtual context
3.3	System must support resource allocation to each context including throughput, CPS, Concurrent connection, SSL throughput
3.4	System must be able to modify the resource allocation on the fly without restarting/rebooting any context
3.5	All the virtual context must be available from day-1
4	DDOS
4.1	System must support protection from Fragmented packets, IP Option, Land Attack, Packet Deformity Layer 3 & 4, Ping of Death, TCP No Flag, TCP Syn Fin, TCP Syn Frag
4.2	System must support connection limit based on source IP
4.3	System must support connection rate limit based on source IP
4.4	System must support request rate limit based on source IP
5	Server Load-balancing /Proxy features
5.1	System must support Layer4-Layer7 load-balancing
5.2	System must support load-balancing algorithms including round-robin, least connection, service least connection, fastest response, hash etc.
5.3	System must support active-active and active-backup server configuration for load-balancing

5.4	System must support reverse proxy functionality of hosting multiple http/https service behind single IP
5.5	System must support Source-NAT for SLB traffic
5.6	System must have flexibility to config VIP as Source NAT IP
5.7	System must support X-forwarder option. The appliance should have option to enable x-forwarder option per service to log actual client IP in web server log.
5.8	System must support forward proxy with proxy chaining
5.9	System must support HTTP Compression
5.10	System must support Global Server load-balancing
5.11	System must support Authentication offloading from back-end servers using SAML, Kerberos, NTLM, TDS SQL Logon, LDAP, RADIUS, Basic, OCSP stapling, HTML Form- based
5.12	System must support graceful activation and disabling of the backend server
5.13	System must support application level load-balancing of Radius, Diameter, DNS, SPDY, SIP, FIX protocol
5.14	System must support application level IMAP,POP3, SMTP and database load-balancing
5.15	System must support DNS Caching and Single sign-on (SSO) authentication relay
5.16	System must support Anycast based Global server load-balancing
5.17	System must support connection limit per server/link
5.18	System must support connection rate limit per server/link
5.19	System must support request rate limit per server/link
5.20	System must support Authentication for Microsoft SharePoint, Outlook Web Access, and other packaged and custom applications
5.21	System must support Perfect Forward Secrecy (PFS) with Elliptic Curve Diffie Hellman Exchange (ECDHE) and other Elliptic Curve Cryptography(ECC) ciphers
5.22	System must support Scriptable health check support using TCL, Python, Perl, and Bash
5.23	System must support Next Hop Load Distribution (NHLD) for load balancing multiple links
5.24	System must support Internet Content Adaptation Protocol (ICAP)
5.25	System must support IPv4 to IPv6 and IPv6 to IPv4 SLB-PT
6	Web application Firewall
6.1	System must support cookie encryption, protection from SQL injection, protection from cross-site scripting, protection from BOT generated requests, HTTP protocol compliance check, Cloaking to hide server responses/error status codes, Credit Card numbers/US SSN masking, PCRE based masking, CSRF check & XSS check, filtering of http methods, protection from buffer overflow, URL blacklisting & whitelisting, TCL based scripts for custom rules, learning, passive and active mode of WAF deployment
7	Redundancy
7.1	System must support VRRP based redundancy, active-active and active-backup configuration, automatic and manual configuration sync.
7.2	System must support dynamic VRRP priority by traffic interface, server, nexthop and routes
7.3	System must support scale-out configuration upto 8 devices to support higher throughput
7.4	System must support dedicated VRRP setting per virtual context
8	Management

8.1	System must have Web-based Graphical User Interface (GUI) & Industry-standard Command Line Interface (CLI)
8.2	System must support Granular Role-based\Object-based Access Control
8.3	System must support SNMP, Syslog, email alerts, NetFlow v9 and v10 (IPFIX), sFlow
8.4	System must support REST-style XML API (aXAPI) for all functions
8.5	System must support external authentication including LDAP, TACACS+, RADIUS

5.2.3.4. Functional & Technical Requirements for Network Management System

Solution should provide fault & performance management and monitor IP/SNMP enabled devices like Routers, Switches. Proposed Network Management shall also help monitor key KPI metrics like availability, in order to measure SLA's. Bidder is supposed to proposed IP based NMS only. NMS features for RF & Wireless are not required.

Following are key functionalities that are required which will assist administrators to monitor network faults & performance degradations in order to reduce downtimes, increase availability and take proactive actions to remediate & restore network services as per specification or better.

S.No.	Minimum Technical Requirements
1	Network Management System(NMS) should be capable of monitoring both LAN and WLAN.
2	Solution must provide Wireless LAN Planning and Design, Network Monitoring and Troubleshooting, Indoor location monitoring capability, Wireless IPS management. Centralized Software updates, Network mapping with floor plans for easier automated site survey, Rogue detection and containment.
3	NMS should provide real-time monitoring, pro-active alerts, historical reporting, efficient troubleshooting through centralized intuitive user interface
4	NMS should have option to customize report on parameters like client health, RF health, device inventory, auditing, compliance and option to scheduling report time.
5	CWMS should provide tools to help better manage RF coverage, address security issues, location tracking to provide a clear picture of who is on the network, their location and how the network is performing.
6	Solution must provide client troubleshooting tools, including showing client Signal to Noise Ratio (SNR), Received Signal Strength Indicator (RSSI) and session throughput.
7	Policy creation and enforcement - to easily create virtual LAN (VLAN), RF, quality of service policies, security policies, network topology maps, Customized reports
8	System should automatically discover WLAN infrastructure devices and create visibility into wired infrastructure that connects controllers and APs
9	Should collect and display client device details like Manufacturer, model, device type, OS & more
10	Central configuration for controller and APs and there should be an option to cancel out of a new configuration or reverts back to the last saved configuration.
11	Allows quick location of users and wireless devices for troubleshooting, planning and asset tracking.
12	Playback location history of individual users over the past day to aid in troubleshooting and recovery of lost devices.
13	Last known location of each tracked device is stored indefinitely to help find lost or stolen devices

14	Display the location of each rogue device on a building floor plan and disable wired switch ports if attached rogue APs are detected.
15	Aggregates, correlates, alerts and logs wireless attacks that have been detected and reported on the network, providing a comprehensive picture of infrastructure.
16	System should facilitate various administrative roles to match each individual users responsibility e.g. HelpDesk user may be given read-only access to monitoring data without being permitted to make configuration changes.
17	System must be able to provide detailed performance statistics for WLAN equipment (statistics related with bandwidth, coverage etc.) and must not be tied to specific WLAN vendors, also provide graphical details of WLAN utilization, average data rate, WLAN traffic etc. on a per AP basis
18	System should provide current list of clients connected to each AP, graphical details of wireless traffic & data rates on a per client basis, recent history of association with APs & ad-hoc networks for clients, alerts when wireless clients use interface bridging or Internet
19	System should provide DHCP response times for every user. Aggregated DHCP response times for servers.
20	System should provide Authentication response times for every user. Aggregate Auth server response times per server.
21	System should provide DNS response times for every user. Aggregated DNS response information per server.
22	System should provide client troubleshooting information including Association time, Authentication success/failure and time, DHCP time and DNDS time.
23	Connection Sharing, trends for WLAN performance parameters, alert when wireless bandwidth is being wasted due to excessive auxiliary traffic, trends for WLAN performance parameters
24	System must be able to maintain recent history of connected clients for each AP for up to 60 days
25	The operations solution should provide a network “dashboard” on all screens, providing up-to-date network-wide information on key usage and performance metrics. The operations solution should monitor edge switches to which wireless devices are connected. The operations must be able to monitor IDS events, since they have a potential impact on network performance as well as security.
26	NMS should support VLAN Management to view current VLAN configuration, VLAN topology, VLAN deployment, ACL Management to simplify definition and deployment of ACLs and perform ACL rule optimisation
27	The operations must provide mechanisms for remediating and/or containing rogue devices it has detected.

5.2.3.5. Functional & Technical Requirements for Server Performance Monitoring

S.No.	**Description**
1.	The proposed tool should integrate with network performance management system and support operating system monitoring for various platforms supplied as part of this Project.
2.	Proposed solution shall integrate with SLA & Contract Management system in order to supply KPI metrics like availability, utilization, and performance in order to measure central SLA's and calculate penalties.
3.	The proposed tool must provide information about availability and performance for target server nodes.
4.	The proposed tool should be able to monitor various operating system parameters such as processors, memory, files, processes, file systems, etc. where applicable.
5.	If the offered server/computing solution includes virtualization, then the server performance monitoring solution must include virtualization monitoring capabilities.

5.2.3.6. Functional & Technical Requirements for Centralized Helpdesk

S.No.	Description
1.	Help desk system should provide incident management, problem management templates along with help desk SLA system for tracking SLA's pertaining to incident resolution time for priority / non-priority incidents.
2.	System should also automatically create tickets based on alarm type.
3.	The proposed helpdesk solution must provide flexibility of logging, viewing, updating and closing incident via web interface for issues related to the project.
4.	The proposed helpdesk solution must have a built-in workflow engine to define escalations or tasks to be carried out after issues or change order are logged pertaining to surveillance project.
5.	Centralized Helpdesk System should have integration with Network and Server Monitoring Systems so that the Helpdesk Operators can to associate alarms with Service Desk tickets to help operators that for what particular alarms corresponding helpdesk tickets got logged.
6.	IT Asset database should be built and managed in order to carry out the scope of work items.
7.	Surveillance Network admin should be able to manually create tickets through Fault Management GUI.
8.	System should provide a link to directly launch a Service Desk view of a particular ticket created by alarm.

5.2.3.7. Functional & Technical Requirements for Centralized AV & Anti-Spam

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

S.No.	Minimum Technical Specification
1.	AV Solution: Should have critical components for total security on the endpoint. (Antivirus, Antimalware, Vulnerability protection, iDLP, HIPS, Firewall, Device control & Virtual Patching.)
2.	Personal Firewall: Firewall should block unwanted traffic, prevents malware from infecting endpoint systems, and makes them invisible to hackers.
3.	Program Control with Program Advisor: Program Control ensures that only legitimate and approved programs are allowed to run on the endpoint. Program Advisor is a real-time Vendor knowledge base of over a million trustworthy applications and suspected malware used to automatically set the Program Control configuration.
4.	Heuristic virus scan: Should Scan files and identifies infections based on behavioral characteristic of viruses
5.	On-access virus scan :Should Scan files as they are opened, executed, or closed, allowing immediate detection and treatment of viruses
6.	Deep scan: Should Scan Runs a detailed scan of every file on selected scan targets
7.	Scan target drives: Should Specifies directories and file types to scan
8.	Scan exclusions: Should Specify directories and file extensions not to be scanned
9.	Treatment options: Should Enables choice of action agent should take upon detection of virus: Repair, rename, quarantine, delete
10.	Intelligent quick scan: Should Check the most common areas of the file system and registry for traces of spyware
11.	Full-system scan: Should Scans local file folders and specific file types
12.	Deep-inspection scan: Should Scan every byte of data on the computer
13.	Scan target drives: Should Specify which directories and file types to scan
14.	Scan exclusions: should Specify directories and file extensions not to be scanned
15.	Treatment options: Should Enable choice of action agents should take upon detection of virus: Automatic, notify, or confirm
16.	Browser Security
a.	Should Support latest versions leading web browsers i.e. IE, Mozilla, Chrome, Safari etc.
b.	Endpoint security solution should provide vulnerability protection, which should scan the machine and provide CVE number visibility and accordingly recommend rule for virtual patch against vulnerability.
c.	Should Allow users the freedom to surf with full protection against malicious software that is automatically downloaded and phishing attempts
d.	Endpoint Host based IPS should support virtual patching both known and unknown vulnerabilities until the next scheduled maintenance window. Endpoint security solution should submit unknown files to on-premise sandbox appliance for simulation. It should also support creation of IOC's on real time basis. These IOC's should be distributed to rest of the servers for block, remediate and clean up threats and sandboxing should have at least 55 virtual instances, which should have OS (win7, win8, win 10, Win 2003, win 2008, win 2012) instances in sandboxing- along with customized sandboxing feature.

e.	Should support prevention against script-based attacks used to deliver malware such as ransomware. Endpoint solution should able to consume IOC's and output from sandboxing from Zero day threat solution to protect and clean zero day threat at endpoint level.
f.	Should Support Signature & Heuristic Phishing Protection
g.	Should Support Site Status Check
h.	Should Support Centralized Browser Security Policy Management
i.	Should Support Centralized Browser Security Event Logging & Reporting
17.	Management Platform Support
a.	Operating systems: Should Support Windows Server 2008, 2012, 2016
b.	Browsers: Should Support Internet latest version of leading web browsers
c.	Client Platform Support
d.	Should support Windows 8, 10 (32 & 64 bit), Mac
18.	Spam Filtering
a.	The proposed solution should Stop spam, denial-of-service attacks, and other inbound email threats using industry-leading technologies and response capabilities, leverage adaptive reputation management techniques that combine global and local sender reputation analysis to reduce email infrastructure costs by dropping up to 90% of spam at the connection level, Filter email to remove unwanted content, demonstrate regulatory compliance, and protect against intellectual property and data loss over email, Secure and protect other protocols, such as public IM communications, using the same management console as email, Obtain visibility into messaging trends and events with minimal administrative burden.
b.	The proposed solution should automatically back up all configuration and quarantine databases on the appliance at specified intervals. Administrators should be given an option to store data on the local machine or a remote server.
c.	should be able to detect spam mails in SMTP, POP3 as well as IMAP protocols
d.	The proposed solution should have inspection facility on the header and body of the mail to check for spam URI content and identify whether the mail is a spam mail or not.
e.	The proposed solution should support real time statistics of scan performance, message processed and security violations and proposed solution should support message tracking for quarantined, archived and postpone messages in message tracking logs
f.	should have options to configure white list as well black list based on IP address and validate against the same to detect whether a mail is spam mail or not
g.	Should have configurable parameter to enable HELO DNS lookup to check whether a mail is a spam or not.
h.	Should have configurable parameter to enable return email DNS lookup to check whether a mail is a spam or not.
i.	Should have provision to define banned key words and check against that key words to identify spam mails.
j.	Should have options to define mime headers and check against the same to identify spam mail.
k.	The solution should have Global sender reputation and local sender reputation analysis to reduce email infrastructure costs by restricting unwanted connections.
l.	Solution must be scalable to incorporate the following with no installation of component on clients should need be in future:
m.	Email Security solution should able submit files to customize sandboxing for zero day protection

n.	Should have integrated data loss prevention technologies to check loss of data through mails at gateway
o.	The proposed solution should have an option to restore an solution to its original image configuration.
p.	Should have configurable spam actions for detected spam mails (e.g. tag the mail, delete the spam mail etc.).

5.2.3.8. Functional & Technical Requirements for Mailing & Messaging Solution

S.No.	Minimum Technical Specification
1.	General
a.	Network/Server edition should run on Linux /Windows.
b.	Desktop client should run on Mac, Linux and Windows.
c.	Solution should be based on open standards for minimum 1000 users.
d.	Should support advanced search and file indexing for large inboxes
e.	Ability to use custom logos in the web interface
f.	Should support e-mail, Address Book, Calendar, Task & File Server
g.	Should support real-time backup and restore
h.	Should support clustering/High-Availability
i.	Ability to access the Mail server via IMAP clients, with the option to connect over SSL/TLS
j.	Ability to access the Mail server via POP clients, with the option to connect via SSL/TLS
k.	Comprehensive suite of standards-based web services APIs enabling seamless integration with other applications
l.	Ability to utilize Active Directory for user authentication and/or Global Address List
m.	Admin can configure an initial password in the migration wizard and import wizard for newly provisioned accounts
n.	Should support multi-tenancy
o.	Should support e-mail Archiving & Discovery
p.	Should have rich, interactive, web-based interface for end user functions (access via HTTP or HTTPS)
q.	Ability to customize the colors and appearance of the web interface
r.	Option to check and correct spelling in a mail message, calendar appointment, or web Document
s.	Ability to share Address Books, Calendars, and Notebooks (Documents) with internal users and groups (read or write access)
t.	Ability to share Address Books, Calendars, and Notebooks (Documents) with external users via a custom password (read access)
u.	Ability to quickly categorize messages, contacts, and/or documents by attaching "Tags" with user-defined names and colors
v.	Option to quickly view attachments in HTML format
w.	Should support conversations span folders
x.	Ability to create personal folders and folder hierarchies
y.	Ability to print a message and see a print preview
z.	Ability to sort messages based on subject, date, or sender

aa.	Ability to flag/unflag messages/conversations for follow up
bb.	Ability to define filter rules and priorities for incoming messages
cc.	Ability to enable/disable a custom away message
dd.	Ability to add a custom signature to a message
ee.	Option to popup a separate window when composing a message
ff.	Ability to save in-progress messages to a Drafts folder
gg.	Ability for a user to set an automatic forwarding address and choose whether to leave a copy in the primary mailbox
hh.	Option to Reply or Reply-All while retaining the attachments from the original message
ii.	Right-clicking a message displays a menu of actions to take on that message (e.g. Mark Read, Reply, Delete)
jj.	Right-clicking an email address displays a menu of actions to take on that address (e.g. view website, add/edit contact, create filter, search for messages)
kk.	Ability to export a set of messages as a ZIP file
ll.	Ability to toggle between Reply and Reply-All while composing a reply
mm.	Users can set their default preference for viewing messages in the reading pane
nn.	Users can set the default font family, font size and font color to use when composing email messages and Documents pages
oo.	Users can share their mailbox folders and set the permission levels to manage or to view-only.
pp.	Users can insert inline images in email messages and calendar appointments
qq.	Admin can configure the maximum number of characters used in a signature
rr.	Admin can define expiration policy for individual mailbox folders
ss.	Users will receive an email message warning of quota usage based on a threshold defined by administrator
tt.	Users can attach a URL to an email message
uu.	Users can double-click on a message in message view to expand the view pane to full view
vv.	Users can define multiple email signatures to use
ww.	Users can check multiple emails in the list view to mark as read/unread/tag, delete, or to move to a different folder
xx.	When sending a message, the priority is normal, but it can be set to high or low as well
yy.	Users can get immediate notification of new mail/
zz.	Multiple messages can be selected and forwarded in one email
aaa.	Users can right click on a folder to see the number of messages and the total size of items in folder
2.	Address Book
a.	Business card view of Contacts
b.	List view of Contacts with preview pane
c.	Ability to import/export Contacts in .csv format
d.	Ability to import/export contacts in vCard (.vcf) format
e.	Ability to print a single Contact or list of Contacts and see a print preview
f.	Right-clicking a Contact displays a menu of actions to take on the Contact (e.g. compose message, search for messages)
g.	Ability to drag a Contact to a mini-calendar date to create an appointment with that Contact

h.	Ability to create multiple Address Books in a single mailbox
i.	Ability to move/copy contacts from one Address Book to another (based on access privileges)
j.	Ability to create group contact lists in their user Address Books
k.	Address book displays individual contact information in tabbed view
l.	Photos and images can be uploaded to contacts in Address Books
3.	Calendar
a.	Ability to schedule personal appointments
b.	Ability to schedule meetings and view attendees' free/busy information
c.	Ability to create recurring meetings and exceptions to recurring meetings
d.	Ability to book resources (locations, equipment, etc.) for a meeting
e.	Ability to configure a resource to auto-respond to scheduling requests based on availability
f.	Option to enable an alert popup for upcoming appointments
g.	Appointments/schedules are automatically displayed in the users current time zone
h.	Ability to set an explicit time zone for an appointment
i.	Ability to view calendars in Day, Week, Work Week, or Month views
j.	User setting for the first day of the week; value chosen impacts the Week calendar view
k.	Ability to create an appointment and/or drag an appointment's boundaries inline in calendar views
l.	Ability to quickly mark Accept/Tentative/Decline from calendar views
m.	Declined appointments display faded so that the user remains aware of their occurrence
n.	Ability to print calendars in day, week, work week, or month views and see a print preview
o.	Hovering over an appointment in calendar view displays additional appointment details
p.	Option to display a miniature calendar at all times
q.	Hovering over a date in the mini-cal displays calendar information for that date
r.	Right-clicking on the mini-cal displays a menu of actions to take on the associated date (e.g. add appointment, search for messages)
s.	Ability for a user to create multiple calendars within a single account
t.	Ability for a user to designate which calendars will be included in the user's free/busy calculations
u.	Ability to subscribe to an external calendar in i-Calendar (.ics) format
v.	Ability to publish/export a calendar in i-Calendar (.ics) format
w.	Ability for a user to view multiple calendars overlaid in the same view, which each calendar optionally represented by a different color
x.	When viewing multiple calendars, option to view that indicates the degree of conflict at each potential time slot
y.	Users can import calendar i-Calendars (.ics)
z.	Appointments can be marked as private or public.
aa.	Administrators can configure the Calendar feature to be able to create only personal appointments
bb.	Users can search for appointments within their calendars
cc.	Public calendars display in HTML read-only format
4.	Tasks

a.	Add tasks and set the start and due date, set the priority and keep track of the progress and percentage complete
b.	Share task lists with internal and external users and set permission levels to manage or to view-only
c.	Users can organize task lists into folders
d.	Users can sort tasks by Status or Due Date
e.	Users can set the priority of tasks to high, normal or low
f.	Individual tasks can be tagged
g.	Files can be attached to a tasks
5.	Documents
a.	Ability to create rich web Documents with WYSIWYG or HTML editing
b.	Ability to create a notebooks as a Document repository and as a mechanism for navigating through Documents
c.	Ability to create multiple notebooks in a single mailbox
d.	Ability to create a notebook that is shared by everyone within a domain
e.	Ability to insert links in Documents to other Documents or to external URLs
f.	Ability to upload Attachments as Documents
g.	Ability to embed rich content objects as independently editable items inside a web Document
h.	Ability to embed an image as an ALE object inside a web Document
i.	Ability to embed a spreadsheet as an ALE object inside a web Document
j.	Ability to print a Document and see a print preview
k.	Pages show when last modified and version
l.	Users can upload files to their mailbox and can access them from any computer
m.	Users can add email attachments to a selected folder
6.	Search
a.	Server-side indexing of mailbox content, enabling fast and efficient search from g gg the web interface
b.	Ability for a search to include any number of conditions combined via Boolean-like expressions (AND, OR, NOT, etc.)
c.	Ability to use text commands to execute searches
d.	Advanced interface for building searches
e.	Ability to search for a specific item type (Mail, Contacts, Documents, etc.) or across item types
f.	Ability to search using a prefix plus a wildcard
g.	When using Search Builder, the search result set updates continuously as search conditions are changed
h.	Ability to save searches for subsequent one-click re-execution
i.	Ability to search for items that contain specific keywords
j.	Ability to search for items with a specific date or within a specific date range
k.	Ability to search for items that contain an attachment
l.	Ability to search for items that contain an attachment of a certain type(s)
m.	Ability to search for items that have a specific flagged/un-flagged status
n.	Ability to search for items that are in a specific folder
o.	Ability to search for items based on storage size
p.	Ability to search for items based on read/unread status
q.	Ability to search for items with specific recipients in the To /Cc fields
r.	Ability to search for items from a specific sender

s.	Ability to search for items based on subject
t.	Ability to search for items that include a specific Tag(s)
u.	Ability to search for items that were sent to or received from a specific domain
v.	Ability to search for Contacts in a Shared Address Book
w.	Ability to search for content inside attachments
x.	Can search for appointments in calendars up (up to 180 days)
y.	Administrator can disable the indexing of junk mail
7.	Domain-Level Management
a.	Ability to create and manage multiple mail domains within a single instance of Messaging Solution
b.	Ability to use different Global Address Lists for each domain
c.	Ability to use different authentication stores for each domain
d.	Ability to delegated domain-level administrators to manage users and other settings specific to a domain
e.	Ability to create domain-specific custom branding of the web interface
f.	Ability to enable a domain admin to update account quotas up to a maximum set value
g.	Ability to set quota for each domain (either unlimited or a maximum value per account)
h.	Ability to move a domain
i.	Ability to search across mailboxes from the administration console
8.	Storage
a.	Messages (including attachments) sent to multiple users are stored once to optimize storage space
b.	Ability to set quotas for mailbox size and number of Contacts
c.	View of mailboxes sortable by quota, total mailbox size, or % quota consumed
d.	Ability to define retention policies for all messages, trashed messages, and/or junk messages
e.	Ability to move a mailbox(es) from one server to another without requiring system downtime or affecting other mailboxes
f.	Ability to run a regularly scheduled process that moves older messages to a secondary storage volume
9.	System Health & Security
a.	Should have native anti-virus & anti-spam mechanism
b.	Administrator interface setting to specify spam quarantine and kill thresholds
c.	Messages that users mark as Junk / Not Junk are automatically fed into the spam training engine
d.	Administrator interface setting to define the update frequency for virus signatures
e.	Ability to enforce client authentication to the SMTP server before relaying mail (with option to require authentication over TLS)
f.	Graphical display of system activity including disk usage, message volume, and AS/AV results
g.	Ability to monitor the status of all core system servers/services in a single view
h.	Ability to block attachments based on criteria such as attachment type or size
i.	Ability to enforce that attachments be viewed as HTML, enabling risk-free attachment viewing without requiring attachment-native applications on the viewer's machine
j.	Install and manage certificates from the administration console

10.	Compatibility & Interoperability
a.	MAPI-based synchronization of mail, contacts, and calendar data between Outlook and the proposed solution server
b.	Online/offline status is automatically detected, enabling the user to work without having to specify their connection status
c.	Synchronization operations are cached and synchronized as an asynchronous process, enabling optimal Outlook performance
11.	Mobile Devices
a.	AJAX Mobile Web Browser
b.	i-Phone Email, Contact, Calendar sync
c.	Windows Mobile and other smartphone Email
d.	Email, Contact, Calendar sync
e.	Documents should be captured through mobile interface, it should fulfil following additional requirements: 1. Application should provide rules and validations in the built-in form to avoid wrong data entry 2. Mobile interface will also be used for Workflow based decision making applications. 3. Application should support3-tier architecture 4. Application should be integrated with any domain controller system i.e. LDAP 5. The application should merge multiple captured pages to one single page for each document type 6. The application should perform the imaging features like Noise removal, perspective correction , enhanced image quality 7. The application supports all the password policies. 8. The application should provide user as well device level rights management.

5.2.3.9. Functional & Technical Requirements for Identity Access Management

S.No.	Description
1	**Identity Management**
1.1	The Identity and access management should be able to provide complete user lifecycle identity management for all types of users.
1.2	The solution should provide identity management, governance and Identity management portal, including entitlement certification and role management
1.3	The proposed solution should provide user provisioning and de-provisioning on all target systems, automatic account provisioning, removal, and approval processes throughout the user's entire lifecycle.
1.4	The proposed solution should have customizable workflows to support the unique way environment approves, alerts, and schedules these activities.
1.5	The proposed solution should provide centralized control of identities, users, roles and policies across on-premise and cloud applications.

S.No.	Description
1.6	The proposed solution should provide User self-service to manage attributes of their own identities, reset passwords and request access to resources.
1.7	The proposed solution should support Password Synchronization to reflect changes in identity management systems and target applications
1.8	The proposed solution provide Privilege cleanup by examining existing system entitlements and highlights excessive or unnecessary privileges. Delivers details such as such as how often a resource was accessed or if an entitlement causes a security policy violation.
1.9	The proposed solution should provide Identity and access governance policies using centralized engine that helps establish and enforce a consistent set of business and regulatory compliance policies.
1.10	The proposed solution should support Entitlements certification by providing easy to use interface through which managers or resource owners can view and certify that privileges are appropriate or should be removed, thus helping meet compliance requirements.
1.11	The proposed solution should support Role modeling analysis to efficiently sort through extremely large volumes of user and privilege information to discover potential roles.
1.12	The system should be able to detect any changes in the target systems via the concept of reverse synchronization and associate various actions upon detection
1.13	The solution should have ability to perform bulk jobs for example user changes, scheduled jobs
1.14	The proposed solution should offer an easy-to-use, configurable user-centric Risk Model that identifies areas of risk caused by users with high risk scores.
2	**Single Sign on under Identity Management**
2.1	The solution should have a capability which helps to prevent unauthorized users from hijacking legitimate sessions with stolen cookies and assures that the client who initiated the session is the same client that is requesting access.
2.2	The solution should have capability to support various SSO architectures that can be used independently or mixed and match to meet various business needs such as: Agent-based policy enforcement points Centralized gateway enforcement points Support for today's open standards including SAML, OAuth, OpenID and WS-Federation Agent-less based approach to securely pass claims to applications without the use of proprietary APIs REST and SOAP-based Web APIs to allow applications to remotely call Single Sign-On as a Web service for authentication or authorization
2.3	The solution should provide secure single sign-on and flexible web access management to applications and Web services either on-premise, in the cloud, from a mobile device or at a partner's site.

S.No.	Description
2.4	The solution shall support SSO by passing the user's identity among heterogeneous servers securely. No additional authentication is required.
2.5	The solution should provide session assurance.
2.6	The solution should provide centralized session management to securely manage a user's online session.
3	**Privilege Access Management Under Identity Management**
3.1	The proposed solution should be appliance based and provide the capability to manage Password Vault, Access Management, Session Recording, Application to Application (allows dynamic password access from applications), etc. within a single hardened platform.
3.2	The proposed solution should supports a process to automatically synchronize with a DR site over a WAN and provide built-in replication of the password vault aiding disaster recovery
3.3	The Proposed solution should have ability to define a zero trust, explicitly allow only access methodology.
3.4	The proposed solution should provide built in Active-Active High Availability and Load Balancing along with built-in clustering without the use of a traffic load balancer.
3.5	The Proposed solution should have ability to provide real-time data synchronization among a cluster.
3.6	The proposed solution should not require using third party software or hardware such as Operating Systems, Databases, High Availability, Load Balancers, etc.
3.7	The proposed solution should be browser independent and there shouldn't be any browser dependency to manage and record the sessions.
3.8	The proposed solution should provide highly efficient integrated video session recording with low storage requirements.
3.9	The proposed solution should provides in-line command filtering using white lists/black lists for SSH, network devices command line operations.
3.10	The proposed solution should be able to support application based session via RDP protocol in which the user can be confined, rather than requiring RDP to a full desktop.
3.11	The proposed solution should support to require an approval by designated users as a condition of accessing the credentials for managed accounts. The Solution should also enforce users to specify reason when requesting access for a privileged account.
3.12	The proposed solution should provide tools/APIs for enabling applications that require access to privileged accounts to access credentials programmatically, eliminating the need to "hard code" credentials into the script or application. Password should be rotated automatically.

S.No.	Description
3.13	The Proposed solution should have ability to manage target OS, Databases, Network, security devices, Virtual and cloud environments local administrator credentials through single appliance.
3.14	The proposed solution should provide threat analytics that provides a continuous, intelligent monitoring capability that helps enterprises detect and stop hackers and malicious insiders before they cause damage.
4	**Host Based Access Control Under Identity Management**
4.1	The proposed solution should provide granular access control on critical Servers to protect the access even if the servers are accessed directly from the console.
4.2	The proposed solution should support all Unix, Linux and Windows platforms and should be agent based.
4.3	The proposed solution should control and monitor privileged user access to files, folders, processes and registries, enabling accountability, incoming/outgoing TCP/IP protection, integrity monitoring and segregation of duties.
4.4	The proposed solution should restrict super-user privileges with finer level of granularity than what is available in the host operating system.
4.5	The proposed solution should support authentication to Linux and Unix using Windows AD credential and also provide User ID management (including UNIX files and NIS)
5	**Authentication under Identity Management**
5.1	The proposed solution should provide PKI and Risk Based authentication. It should also support mobile OTP.
5.2	The proposed solution should have tight integration with proposed SSO solution
5.3	The proposed solution should have Pre-built rules that cover typical fraud patterns.
5.4	The proposed solution should support customization of pre-built rules or creation of new rules quickly and easily.
5.5	The proposed solution should Self-learning scoring engine based on statistical modeling
5.6	The proposed solution should have Device identification mechanism using multiple variable device fingerprinting
5.7	The risk based engine should also use geo location criteria
5.8	The proposed solution should have policy-based system to flag and manage cases of suspicious activity.
5.9	The proposed solution should Integrate data from multiple channels.
5.10	The proposed solution should learn end user behavior and suggests step-up authentication when there is a deviation from normal behavior.

S.No.	Description
5.11	The proposed solution should support out of band authentication via SMS, Email and Voice including mobile push.

5.2.3.10. Functional & Technical Requirements for Enterprise Database

S.No.	Description
1.	Database License should be un-restricted and perpetual, to prevent any noncompliance in an event of customization & integration.
2.	Databases shall support multi-hardware platform.
3.	RDBMS should support Unicode with Indian Language support
4.	RDBMS should have spatial capability and should be capable of storing vector (2D, 3D), raster data as well as the metadata.
5.	Database shall provide standard SQL Tool for accessing the database. The tool should be able to monitor, maintain and manage the database instance, objects, and packages.
6.	Database shall have built-in backup and recovery tool, which can support the online backup.
7.	RDBMS should support of seamless data transformation from on premise to public cloud and from public cloud to on premise.
8.	DB should have in built mechanism to balance the data across the available database files
9.	RDBMS should provide database clustering support for high availability
10.	Should be an enterprise class database with the ability to support connection pooling, load sharing and load balancing when the load on the application increases.
11.	Database shall have built-in DR solution to replicate the changes happening in the database across DR site with an option to run real time or near real-time reports from the DR site.
12.	RDBMS should have mechanism to recover from a disaster with no loss of data”
13.	Database shall provide native functionality to store and retrieve XML, Images and Text data types.
14.	Database shall provide native functionality to store XML, within the database and support search, query functionalities.
15.	RDBMS should support spatial data types.
16.	Database shall have Active-Passive or Active-Active failover clustering with objectives of scalability and high availability.
17.	Database shall provide control data access down to the row-level so that multiple users with varying access privileges can share the data within the same physical database.
18.	Database shall be having built-in provision to Administer database / database clusters, Monitor performance, Maintain database, Backup and recovery, Recovery management, Disaster recovery management.
19.	Database shall be having native auditing capabilities for the database.
20.	Database shall be having built-in provision to Administer database / database clusters, Monitor performance, Maintain database, Backup and recovery, Recovery management, Disaster recovery management.
21.	Availability of recovery/restart facilities of the DBMS.

22.	Automated recovery/restart features provided that do not require programmer involvement or system reruns.
23.	RDBMS should be able to recover after the DB restart and should have a consistent data for the application
24.	RDMS should have the ability to manage recovery/restart facilities to reduce system overhead.
25.	Provides extra utilities to back up the databases by faster means than record by record retrieval.
26.	The database should provide controls over who, when, where and how applications, data and databases can be accessed.
27.	RDBMS should be possible to prevent privileged IT users such as DBAs and administrators from accessing and modifying the data.
28.	Should provide adequate auditing trail facility. Audit trail should also be maintained at database level for any changes made in database and it should be ensured that these audit trails cannot be manipulated by anyone including super users and DBAs.
29.	System should have the ability record all system level changes for audit purpose.
30.	Solution should offer spatial analytic functions for data mining applications, such as binning, spatial correlation, co-location mining, spatial clustering, and location prospecting

5.2.3.11. Functional & Technical Requirements for Directory Services

S.No.	Description
1.	Should be compliant with LDAP v3
2.	Support for integrated LDAP compliant directory services to record information for users and system resources
3.	Should provide authentication mechanism across different client devices / PCs
4.	Should provide support for Group policies and software restriction policies
5.	Should support security features, such as Kerberos, Smart Cards, Public Key Infrastructure (PKI), etc.
6.	Should provide support for X.500 naming standards
7.	Should support that password reset capabilities for a given group or groups of users can be delegated to any nominated user
8.	Should support that user account creation/deletion rights within a group or groups can be delegated to any nominated user
9.	Should support that user account creation/deletion rights within a group or groups can be delegated to any nominated user
10.	Should support directory services integrated DNS zones for ease of management and administration /replication.

5.3. Data Centre and Disaster Recovery Centre

MSI has to implement City Data Centre to cater the requirements of Data compute, storage and for city analytics purpose.

a) BSCL shall provide the location to house the compute and storage infrastructure at the Data Centre facility being built in the premises of the Command and Control Centre.
b) The DR for the data centre shall be on an Active-Passive mode on Cloud on empaneled service providers by MeiTY and audited by STQC.
c) Various ICT equipment to be provisioned and maintained by MSI at the Data Centre as given in Section 5.2.
d) Only the minimum specifications for the active and passive ICT and Non-ICT components are specified.
e) Propose Data Centre Virtualization solution for price discovery and use all Bihar smart cities as virtual cloud to share the storage between the cities.
f) MSI shall peruse the same provide the BOM / BOQ required to meet the performance requirements as per the proposed business needs. MSI may also suggest additional components as per the solution requirements.
g) The information between the Smart DC and the DR cloud shall be synchronized over the network such that that the smart city solutions are high available on the network.
h) Operational and Uptime Requirements for Data Centre.
i) Minimum Tier Rating for Data Centre: **Tier 3**
    i. Availability Target (24Hr operation): 99.741%
    ii. Maximum Downtime Tolerated per Day: 4 minutes
    iii. Maximum Downtime Tolerated per Week: 27 minutes
    iv. Maximum Downtime Tolerated per Month: 1 hours 54 minutes
    v. Maximum Downtime Tolerated per Quarter: 5 hours 42 minutes
    vi. Maximum Downtime Tolerated per Year: 22 hours 43 minutes
j) Operational Compliance Requirements for MSI operations:
    i. PCI-DSS
    ii. ISO 27001
    iii. ISO 20000
    iv. Cyber Security Framework for Smart City (MoUHA)

Note: Operational Compliance applicable for Data Centre, ICCC and NOCs

5.3.1. Disaster Recovery and DR Cloud

a) MSI shall also be responsible for providing Cloud service for storing all applications at DR [minimum 50% production capacity, RTO – 30 mins, RPO – 30 mins] which will be implemented under BSCL Smart City project for the project duration. Performance SLA will be applicable while operations from DR site.
b) All applications need to have high performance clustering (redundancy) within the Data Centre with automatic fail-over, and redundant data storage in active passive or active-active configuration as per the high availability targets. The data replication should be continuous among all the servers and shared storage should not be used. All mission critical systems must be active-active configurations. Active-passive configurations may be permissible for supporting applications.
c) The proposed Cloud Service Provider (CSP) must be an empanelled cloud service provider by Meity (Ministry of Electronics and Information Technology for Public cloud, Virtual Private Cloud and Community Government Cloud.

d) The Cloud Data Centre Facility must be within India and must be Tier III or above. The DR site within India should be at least 250 Km away from the BSCL Data Center and in a different seismic zone.
e) MSI also need to ensure that the CSPs facilities/services are certified to be compliant to the following standards:
   - ISO 27001 – Data Center and the cloud services should be certified for the latest version of the standards
   - ISO/IEC 27017:2015 – Code of practice for information security controls based on ISO/IEC 27002 for cloud services and Information technology
f) The cloud service provider must have billing model of pay-per-consume where it will charge for amount of computing resources being consumed by application rather than for the allocated resources. MSI shall provide the rate chart of the cloud services to BSCL for per VM and per TB storage.
g) Cloud services should be accessible via Internet, Point to Point / MPLS, Leased Lines, OFC WAN etc. MSI must provide private connectivity between BSCL's network and Cloud Data Centre Facilities.
h) MSI shall be fully responsible for upgrades, technological refreshes, security patches, bug fixes and other operational aspects of the infrastructure that is in the scope or purview of MSI.
i) MSI shall provide interoperability support with regards to available APIs, data portability etc. for BSCL to utilize in case of Change of cloud service provider, migration back to Local Data Centre, burst to a different cloud service provider for a short duration or availing backup services from an alternate Cloud service provider.
j) 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 resources.
k) BSCL shall retain ownership of all virtual machines, templates, clones, and scripts/applications created for BSCL's applications. BSCL shall retain the right to request (or should be able to retrieve) full copies of these virtual machines at any time.
l) In no circumstances, the data accumulated and processed by Command and Control Centre should be compromised. Hence, provisions will be made to keep all the data stored in this platform highly secured with required multi layered security access control and authorization framework. Further the platform shall provide an open standards based Integration Bus with API Management, providing full API lifecycle management with governance and security features.
m) Additional Parameters

i. 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.
ii. 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.
iii. MSI should offer dashboard to provide visibility into service via dashboard.
iv. 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 approval of the BSCL.
v. Selected Video feeds from Police shall only be replicated

vi. Mission Critical applications are also part of DR Site including all the hosted applications

A High Level Design (HLD) for cloud deployment should be suggested by the MSI. MSI can suggest security stack & deployment method according to their recommendations;

5.3.2. Preparation of Disaster Recovery Operational Plan

The bidder should provide detailed operating procedures for each application during the following scenarios. These will be mutually agreed upon with BSCL 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
d) Configure proposed solution for usage
e) MSI can plan DR drill on its own or on the instructions of Client as and when required.

5.3.2.1. Functional & Technical Requirements for DR Management

S.No.	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 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

5.3.2.2. Periodic Disaster Recovery Plan

The service provider shall be responsible for–

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

5.4 GIS Survey, Mapping & Enterprise GIS

Overview:

a) Availability of timely and relevant information about cityscape, the physical growth trend taking place in different parts of the city is a very important input to the Smart City Development process. Geographical Information System (GIS) is for management, analyzing and displaying data of all areas within BSCL Smart city which are spatially referenced to earth for efficient and effective decision making, spatial planning, management of crisis/disasters and for monitoring of normal circumstances, thus providing an important tool to respond faster to incidents or even avert certain incidents. GIS platform is intended to provide common GIS capability to all other systems being deployed as part of BSCL Smart City initiative. The objective of architecting a common GIS layer is to keep a single repository of all GIS data (Pan City data) for easy maintenance, avoid duplication and easy dissemination of information to all the dependent systems. The dependent systems.

b) Include Smart Parking, City Wi-Fi, Pan City Network Backbone, Intelligent Transport Management and Utility Management Systems. More systems may be added in the future and therefore the GIS application should be able to integrate with such applications through standards based interfaces. GIS platform would be importing a lot of existing data from various sources into most industry standard formats. GIS platform would also need to exchange data with a number of external applications and therefore should be capable of exporting data in most industry standard formats including IIS, Apache Tomcat , Web Sphere, Web Logic etc. It should support minimum 100 concurrent Intranet web users and unlimited viewers on internet. Following services shall be configured through Web GIS software (but not limited to):

   i. Location Based Services
   ii. Traffic Management System, Vehicle Tracking and Management System (VTMS)
   iii. Mobile GIS Services – Integrated with Mobile alert, event monitoring and messages from ICCC.
   iv. “What if” analysis
   v. Mapping Gallery for Inter-Departmental use of Maps/ data Integration of Applications and disparate databases

5.4.1 Functional Requirements

a) GIS Base map Preparation

i. BSCL shall provide available GIS administrative data along with property layer to the selected MSI.
ii. MSI shall asses the quality of available GIS data and accordingly shall create the GIS data creation plan for remaining data layers in consultation with the BSCL.GIS data creation should support rule based model on industry standard such as Topology, Spatial connectivity rules, relationship, GIS layer domains and subtypes, GIS Geometric network, industry specific editing rules and future scalability.
iii. GIS base map shall be a common platform across all the solutions including City Wi-Fi, Video Surveillance, Smart Lighting, Intelligent Traffic, Smart Parking, ICT based Solid Waste Management, Intelligent Transport, Disaster Management, Incident Management & any other ICT component in consultation with BSCL.
iv. MSI shall develop GIS based Decision Support System for public safety & law enforcement.
v. MSI shall use spatial & non-spatial information from GIS database to develop real-time management of various surveillance systems like Traffic Management, VTMS, Smart Parking and incident management, etc.
vi. GIS database shall be in any OGC format;
vii. GIS base map shall include following, but not limited these data with attributes with necessary attributes which shall be finalized during study phase;

- Road Network
- Railway Network
- Administrative boundaries (BSCL Boundary, Ward Boundary etc.)
- Building footprints and names
- Points of Interest data includes:
    - Health Services (Hospitals, Blood Banks, and Diagnostics Centre, Ambulance Services, Other Medical Services etc.)
    - Community services (Fire stations, Police stations, Banks, ATMs, Post offices, Educational facilities, Govt. Buildings etc.)
    - Business Centres (Shopping malls, Markets, Commercial complexes etc.)
    - Residential areas (Individual Houses/Flats, Apartments, Housing societies etc.)
    - Transportation (Bus stops/Terminus, Parking areas, Petrol Pumps, Airports, Railway Stations, etc.)
    - Recreation facilities (Restaurants, Theatres, Auditoriums etc.)
    - Other utilities such as travel and tourism facilities, religious places, burial grounds, solid waste locations etc.

b) Local landmarks with locally known names.

- Land-Cover (Built-up, Green areas, Open Areas, Water bodies)
- Address layers (Pin code, Locality, Sub-locality etc.)
- Utility Networks (OFC, Water, Sewer, Drainage, Electric, Gas, etc.
- Locations of other Municipal Assets
- Education (Primary/Secondary/High School/Colleges)
- Religious structures

- Community centres

c) MSI shall capture Bhagalpur Smart City proposal related all Project/Sub Components in the GIS Map
d) Web GIS Decision Support System – to support predictive & advance Geospatial analytics.
e) User Creation and Security Management
f) Map Browsing Module
   i. Web GIS system should have the capability to change the web pages appearance, and to select services, base maps, templates, galleries to be used.
   ii. Web GIS application must easily integrate & embed with Microsoft Office application like excel, word etc. for management and city administrators.
   iii. Web GIS should be capable to display legends dynamically on the map that will dynamically change based on the visibility of layers, on zoom in and out.
   iv. Web GIS system should support GIS based dashboards to showcase the results and information in the form of pie charts, bar charts, histograms, threshold bars, query ,highlight and selections etc.
   v. 3D layers should capture multiple Levels of Detail (LOD) along with spatial indices, coordinate system information (Global, Cartesian, and Vertical), and even explicit LOD display information based on screen display parameters.

g) Data Editing & Search Module
   - Point
   - Line
   - Polygon

h) Data Analysis Module
   - Buffer
   - Spatial Overlay
   - Application Interface
   - Layers wise features labelling
   - Big Data Support - To analyse geospatial records with capability of aggregating points based on proximity. It should support spatial & temporal joins and trends in the cluster of points densities.

i) Citizen Location Services
j) Generating Reports & Graphs
k) Help File Creation
l) Thematic Mapping (On the fly)
m) User Creation and Security Management

   i. Shall facilitate to create, delete & modify different Enterprise GIS Users within BSCL
   ii. Shall be accessible only to System Administrator while all other modules/sub modules shall be accessible to individual users based on the access rights provided to them by System Admin
   iii. Create Application Interface
   iv. Create admin right and grant suitable viewing/data editing rights
   v. Monitor access rights to user departments

vi. Maintains Application Security
vii. Maintain Interface with BSCL Internal Departments to resolve technical issues
viii. Shall allow Active Directory, LDAP, or other security source
ix. Shall allow administrator to configure security to map service, layer and attribute levels
x. Shall allow group-based security policies
xi. Shall not require opening of any special protocols for connecting the user client to the web/application server used by the package. All communication shall be on HTTP or HTTPs.
xii. MSI shall suggest firewalls that natively support all protocols required between the various servers (database, application and web) in the package. No special configuration shall be required to configure the firewall.
xiii. Application users shall not have direct access to the database.
xiv. Any changes to data should be recorded in a separate table and should be stamped with the identity of the user/program and the date / time of the creation/change.
xv. Shall be possible to audit users at the form level, user level, application module level and at the organizational role level.
xvi. Shall provide reports on user activity based on the role and the application that was used.
xvii. Shall support configurable password policies including;

- Password expiry
- Password complexity
- Password history and reuse policy
- Forced password change on first log on
- Capability of self-service reset of passwords in case of forgotten passwords or locked accounts.

xviii. Shall support security system with a full-fledged Role Based Access Control (RBAC) model

n) Map Browsing

i. This module shall mainly comprise of the basic map navigation tools and the most essential tools for identification of features and attributes. Following are some of the map browsing functionalities :

- Zoom in: The user shall be able to select a particular portion of the map by drawing a rectangle on the map specifying the extent into which the map shall be zoomed in to see the features more closely and in more detail.
- Zoom out: The user shall be able to select a particular portion of the map by drawing a rectangle or just clicking on the map to see the map at a smaller scale.
- Full view (Full Extent): The user can view the map in full extent after zooming in or zooming out at different scales
- Pan: The user shall be given an option to pan the map, which shall be possible if the entire map is not fitting into the screen, i.e., after the user has zoomed in to the map at a certain extent.

- Identify: The user shall be able to view attribute information of the feature of interest.
- Find: User can key in the desired area and the application shall highlight the area on the map.
- Measure distance/area: Two options shall be provided to the user. The user shall be able to measure the area and to measure the distance as well as Latitude & Longitude of the particular location

ii. Refresh Map: All the selected features of the active map layer shall be cleared of the selection, by using this tool.

- Select Feature: User shall be able to select the features of active map layer
- Clear selection: User shall be able to clear selection that is there on map
- Activity indicator: Display notification while map/ data is being processed
- Scale input box: allow user to enter representative fraction scale for dynamic services - For cached services, scale box should contain dropdown menu of available cache scales (levels of detail)
- Show/hide co-ordinates: Show/hide mouse coordinates
- Print: The map can be printed in its current extent as viewed in the map window. The user would be presented with a layout for printing
- Descriptive Map Information Tool: When the mouse cursor hovers over each map feature, information should be shown based on the feature's attributes. Functionality should be available for all feature classes; should be able to display a combination of attributes and should not limit the number of features that can be included with the map tool. It should allow user to turn on and off as needed.

o) Data Editing & Search

i. Shall provide the data editing capabilities including new data addition and existing data up-dation for geographical features and its attributes.

ii. Shall provide user to edit GIS Features. However, for a bulk data editing, BSCL shall use Desktop GIS facility (at least two numbers of Desktop GIS Software), since web based data editing of large database may cause data corruption. Following are essential steps for editing any features through Web GIS, should be part of the system- -

- Add Features
- Delete Features
- Move Features
- Modify Features
- Select Feature to Edit
- Feature Locate by Manual Browsing
- Feature Locate by Entering Lat and Long
- Feature Location by search criteria.
- Identify Feature to Edit

iii. Shall allow users to search features by both pre-configured and dynamic based on unique values as follows;

- Search by Ward, Ward Zone Circle
- Search by area,
- Search by Plot/ CTS Number,
- Search by Building Number,
- Search by Sector,
- Search by UPID, Aaadhar etc.
- Search by Parcel ID etc.

iv. Shall allow user to run the custom queries on-the-fly and save those queries for shared future use
v. Shall allow user to run spatial query on multiple layers with spatial operators
vi. Shall also allow for a buffer to be applied to the search criteria allowing for features within a certain distance of the query feature to be selected.
vii. Shall have facility to run combination of attribute & spatial query
viii. Shall have facility to auto-complete text boxes based on either feature attributes or linked records

p) Date Analysis Module

i. Shall comprise of analytical tools such as spatial overlay, buffer analysis to generate results, and shall also provide geo-processing functions that will be finalized at the time of study stage.
ii. Visualization of Temporal Data
iii. Shall have facility to visualize time aware layers
iv. Shall allow user to add temporal data layer on-the-fly

q) Printing

i. Shall have ability to print maps to a printer/plotter with the selection of paper size (A2, A1, A0, Letter, Tabloid etc.) and page orientation (landscape or portrait)
ii. Shall have print preview option
iii. Shall be able to handle and process any redlining / mark-ups of the map.
iv. Shall have ability to export the map to a standard image format (BMP, TIF, JPEG and PDF file)
v. Shall have a variety of templates must be available which allow the user to add a custom map title and to decide which map elements (north arrow, scale bar, overview map, legend, etc.) will be visible.
vi. Print date and time shall be automatically added to output at application runtime
vii. Legend shall be automatically adjusted based layers displayed in print area

r) Red-lining Capabilities

i. Shall allow users to draw simple shapes (point, line, rectangle, polygon and circle) and add text to make annotations and mark-ups to the map that must be printable. It shall allow the user to provide supplemental information on the map.
ii. Shall allow user to set the redlining display style based on the following specification: Line: color, style, transparency and width. Rectangle, circle, and polygon: fill color, fill opacity, outline style, outline color and outline width.
iii. Add Map Layers

iv. Shall allow user to add GIS map layers
v. Added new map layer shall be overlaid on the existing map
vi. Hyperlinks
vii. Shall have ability to hyperlink to document, images, avi files and PDF files with the feature's attribute

s) Emailing

i. Shall allow user to Email map as an attachment

t) Reporting

i. Shall provide predefined report templates
ii. Shall allow user to create custom reports using SQL query interface and save those reports for shared future use
iii. Shall allow user to generate reports on selected features
iv. Shall be able track the history of reports a user has performed.
v. Shall be able to export reports into PDF and MS Excel
vi. Shall allow use to select different date ranges to view report information
vii. Shall allow user to print reports

u) Web-Editing

i. Support role based multi-user editing access and editing work flows.
ii. Shall allow authenticated user to validate spatial feature create/delete/edit/upload through Web-GIS application
iii. Shall allow administrator to Accept/Reject the changes made and a log shall be created for the same.
iv. Shall have easy-to-use map editing tools
v. Shall allow user to divide the polygon or polyline
vi. Shall allow user to amalgamate the two or multiple polygons or polylines
vii. Shall allow administrator to configure the edit/view security at the level of feature attribute
viii. System should provide feature for web editing for the users in separate version to keep the records of editors with undo/redo operations, and snapping of editing layers for proper spatial connectivity. Web editing (modify/create) of layers attributes with defined rules are also required for quality assurance. Enterprise GIS must support the quality assurance of GIS data with proper version and Session Management.

v) Select Feature

i. Should be able to select features by clicking on or by drawing a polygon around the feature
ii. Should allow user to generate URL for current view extents, visible layers, and active selection
iii. Should allow user to email the generated URL
iv. Should allow user to export data into KML/KMZ and Shape file

w) Bookmarks:

i. User should be able to save a map view and be able to return to that exact view at a later date
ii. User should have ability to email the current view extents, visible layers, and active selection in the form of image

x) Application Error Reporting:

i. Should allow user to report errors, with a screen capture, back to the BSCL GIS Coordinator

5.4.2 Technical Requirements

a) Layer and data security: It shall have a provision to configure user level access to data and layers.

i. Server COTS software should support Security, Authentication, and Authorization using
   - Web-tier authentication
   - GIS-tier authentication
   - Enterprise logins
ii. Shall be compatible for accessibility from any device (i.e. Mobile, Tablet and Laptop), Standard Operating Systems and Internet Browsers.
iii. Shall support One-Web functionality
iv. Shall have provision for flow of information and/or integration with existing and future applications (indicative) such as:
   - Smart Lighting,
   - Vehicle Tracking System
   - ICT based solid waste management
   - Intelligent Traffic Management System
   - Intelligent Transport Management System
   - Smart Parking Management System
   - Environmental Sensors
   - Wi-Fi Hotspots
   - Smart Water Supply Management
   - Property Tax management system
   - Building Plan Approval System
   - Enterprise Project Management
   - Any other Municipal e-Governance Application
v. It shall be a single window application to visualize MIS and GIS data on the same platform.
vi. It shall be have User Management component for defining user roles to control the access of tools and database as per BSCL's requirement.
vii. It shall have a provision to perform Quality Control activity on the data collected from the field before storing on the parent database server. Quality Control should be supported by version control and conflict detection and resolution mechanism.
viii. It shall have provision to generate custom reports.

ix. It shall have provision to generate thematic maps on-the-fly based on attributes details available in the GIS layers
x. It shall have a provision to store audit trail of user activities performed on the application.

b) MSI shall be sole responsible for creating an integration approach through integration service bus for message delivery, services based on standards such as SOAP, HTTP and WCS.
c) The integration service bus shall be designed to promote high throughput, compatibility, flexibility and scalability. Specific functionalities need to be configured for data retrieval from Web-GIS.

i. Shall provide a simple and easy to manage integration architecture for all external applications and should have functionalities to check for integrity and validity of data during import & export.
ii. Shall be able to toggle between Web-GIS and external applications.
iii. Shall allow user to view the maps and attribute data (in limited form) from external applications as well as from the Web GIS window and perform basic functionalities of external applications through the web-GIS window and vice-versa.
iv. Shall be supported with Internet Explorer 9 and above, Latest version of Chrome, Mozilla & Safari browser.

d) System is expected to realign and fit to the smart mobile devices (iOS, Android etc.).
e) Solution should be compatible with various open standards and technologies and should not restrict BSCL in using the solution data for any other applications, and should comply with National Data Sharing and Accessibility Policy (NDSAP) dated 17 March 2012, India's open Government data guidelines.
f) Standardization and Interoperability – the proposed Web GIS Map engine shall be OGC (Open Geospatial Consortium) and SWE (Sensor Web Enablement) compliant.
g) Distance and Area Measurement

i. Should have distance measurements tool to allow user to measure the length of irregular shaped lines
ii. Should have area measurements tool to allow user to measure irregular shaped polygons
iii. Measurements should be shown using the metric and the imperial system. The ability to snap to the edge or nodes of the feature being measured is desirable

h) Event based trigger

i. Ability to connect to Data Stream: Connectors for common data streams including in-vehicle GPS devices, mobile devices, and social media providers
ii. Process and Filter Real-Time Data: Detect and focus on the most important events, locations, and thresholds of operations without interruption. (data transmission without latency) Should be able to accommodate multiple streams of data flowing continuously through filters and processing steps that you define. (live event route mapping)

iii. Monitor Assets: Track most valuable assets on a map. Should be able to track dynamic assets that are constantly changing location (such as vehicles), or stationary assets, such as weather and environmental monitoring sensors.
iv. Respond to Events in Real Time: When locations change or specified criteria are met, automatically and simultaneously send alerts to key personnel, update the map, append the database, and interact with other enterprise systems. Alerts can be sent across multiple channels, such as e-mails, texts, and instant messages.

i) Hyperlink

i. Should have ability to hyperlink to document, images, avi files and PDF files with the feature's attribute

j) Dashboard

i. Should provide easy-to-understand, easy-to-use reports that use appropriate infographics (Charts) to present key indicators from the GIS database, to provide overall information to the key officials.
ii. Should have a GIS-enabled real-time dashboard to display dynamic charts & graphs.
iii. Dashboards must be dynamic with multiple options of display based on live geographic data defined in a web map.
iv. The application should support to configure views to run on multiple monitors or single-display devices.

k) Video / CCTV Surveillance Interface

i. User should be able to see the location of CCTV cameras installed and mapped on to the GIS map
ii. System should have provision to integrate with video feeds available from CCTV camera

l) Web portal capability:

i. Facility for display of spatial layers, query management like have various query tools for queries based on attributes, location, etc.
ii. Facility for basic Navigation tools like the software should have tools to Pan, Zoom, and Rotate the Map according to user requirements
iii. Facility for spatial data classification based on specific attribute value and report generation
iv. Ability to search and to zoom into the user specified x, y coordinates
v. Provision for definition of map projection system and geodetic datum to set all the maps in a common projection and scale.
vi. Facility to click on any feature of the map and return a select set of attributes for feature.
vii. Facility to perform the spatial intersection analysis like plot area with buffer zone to calculate road widening impact on adjacent land.
viii. Allow user to open raster images, or satellite images of various standard format.
ix. Ability to import / export data from / to various formats like shape, MIF, dxf etc.
x. Allow users to export query results to various file formats like bmp, Tiff, Jpeg, pdf, etc.

xi. Support printing spatial data at different scales and at adjustable print quality.
xii. ODBC compliance enabling interface with leading industry RDBMS should be there. WebGIS Software should Support all Industry Standard Database to ensure a truly interoperable GIS, like Amazon RDS for Microsoft SQL server or Amazon RDS for PostgreSQL, IBM DB2 or Informix, Oracle, PostgreSQL etc.
xiii. Allow user to create layers or shortcuts to geographic data that store symbology for displaying features.
xiv. Provision of hyper linking the GIS feature as well as its attribute fields with existing documents, drawing files or scanned maps related to that feature.
xv. Facility to create and organize user desired number of Spatial Bookmarks and should be able to share the same.
xvi. To have Control environment, feature functions, spatial relationship and geometric functions including math's and transformation functions
xvii. The software should support Map Services, Open Geospatial Consortium, Inc. (OGC) and open web services including Map, WMS, WFS, WCS, WMTS, WPS, KML and GeoJSON for interoperable solution.
xviii. The Application shall be able to serve multiple maps/layer with single/fewer configurations or shall have support for SQL Views
xix. The application Shall have support for CQL/SQL filters to obtain better Analytical capabilities

The WebGIS Application shall be highly scalable to serve increasing number of viewers with no extra cost.

5.4.3 Multi Utility GIS Based Property Survey, Base Map updation and GIS Integration with Property Tax

MSI shall undertake detail assessment for integration of the Smart Governance, Surveillance System and all other components with the Geographical Information System (GIS). GIS Base Map of the city prepared in 2012 through detailed survey and using High Resolution Satellite Data. BSCL will provide GIS Base Map (soft copy) in GIS format (shape file) to the selected consultant. The MSI shall update all the features of the GIS Base Map within BhagalpurMunicipal Corporation Boundary through field survey as per their attribute data and shall also create new thematic layers for the surveillance camera, Wi-Fi Hotspots, Environmental sensor and other related spatial features that developed recently. The SI shall also create geo-database of all the properties within the municipal limits of the city through field survey and will also take one photograph of each property that will be integrated with the respective property in GIS environment. Currently there are more than 3 lakh buildings within the Bhagalpur Municipal Area, and the total number of properties will be around 5 lacs. During the Property Survey the consultant shall collect all the basic information required for property taxation as well as other relevant details like use of various municipal services i.e., water connection, sewer connection etc.

SI is required to carry out the seamless integration to ensure ease of use of GIS in the Dashboards in Command Control Centres. SI is required to update GIS maps from time to time.

Scope of GIS Survey Work

The GIS scope at BSCL is proposed to provide a strong and reliable decision support system to BSCL officials by integrating the GIS, GPS Survey & Tax data and the proposed online Application Program.

The Scope of Various GIS services which need to be delivered by Agency are given below:

a. The MSI shall develop a field based Tablet PC (As required)/mobile GIS property mapping application using Mobile Cloud Computing which are in built GIS Based map (to be supplied by the client) in Bhagalpur City for Real time survey data capture, property database repository management and tax assessment and others as may be required from time to time
b. MSI shall provide required number having provision of Tablet PC to develop & install apps for Survey at their own cost
c. The system should be capable of capturing multiple GIS features database in the Applications which should be built and manage by the MSI
d. Mobile app shall provide critical data such as user identification and location information including latitude, longitude and altitude.
e. Property attribute data capture should be carried out in three stages using multiple screens enabling capturing and storing of Owner Details, Land Details, Draw Land Parcels including foot print of the existing building or cluster of building & Capture Image of the asset/ property etc.
f. The MSI shall make Door to Door Survey with the Tablet PC to enable on the spot data entry/drawing map/take picture and collect the up-to-date property details such as, owner details, tenant details, plot area, built-up area, No. of floors, floor area, front road width, existing status of utility services viz. water and electricity etc.
g. The MSI shall provide a 3D layers using LIDAR or any other mapping technologies to capture multiple Levels of Detail (LOD) along with spatial indices, coordinate system information (Global, Cartesian, and Vertical), and even explicit LOD. display information based on screen display parameters. It should be viewed as separate module.
h. The MSI will transfer such detail survey data at Mobile Cloud or server placed in centrally located GIS Enterprise database.
i. The MSI shall prepare up-to-date large-scale (Scale 1:2000) base map (to the extent of Ward Boundary, Road, Building, land use, Point of Interest, etc. Other features which are not available in Base map including all up date) of all the wards/zones of Bhagalpur City using satellite imageries and Apps, topographic survey and verification of features through ground trothing & all Property Buildings (Households) incorporating the data collected, processed and digitized after survey process and all the ward wise validation will be done in GIS Map by MSI.
j. All the survey details should be in shape file format (geo-referencing with geo coding) to be saved in GIS enterprising Server of the proposed ICCC and it should be open & editable in GIS software & built topology, Edged matching, parcel to parcel Snapping, Spatial connectivity, data base relationship, GIS Geometric network etc. All validation will be done by MSI.
k. The MSI shall prepare a Pilot phase of 1 Ward

l. The MSI shall be responsible for Enterprise wide Implementation after the success of the pilot phase
m. The MSI shall be responsible for Quality & Accuracy of survey, data capture & preparation of Map.
n. MSI shall ensure that unique user ID and Password for use by the owner should be there but it will not allow Access for simultaneous and multiple logins for security purpose.
o. The MSI shall also be responsible for appropriate geo referencing & geo tagging of the map covering all Tax properties, Households, Land Cove and Land Use.
p. The MSI shall develop the Multi Utility GIS Based Property Tax software which will be integrated to GIS Server &ICCC at their own cost.
q. All data procured shall be imported into a central database.
r. The system shall be able to support geocoding and reverse geocoding
s. The system shall allow the user to find details of the tax payer as much as possible.
t. The System shall be able to show the real-time published spatial data in the client's domain.
u. The solution shall integrate with GIS and map information in such a way that it shall be able to dynamically/ automatically update information progressively on the GIS maps to show status of resources.
v. GIS maps shall be comprehensive showing detailed up to date existing Road Network, Building Foot Prints and Land use level. Solution shall ensure that the GIS Map provides complete Spatial and Attribute Information Pertaining to All the features of the city as various digital vector layers and allows for zoom in/out, searching and retrieving information capabilities.
w. GIS Base map Preparation- the MSI must provide a Unique Identification Numbering system to each property in the existing area of interest. The unique property ID number should include Latitude and Longitude of the property.
x. Geo-Referencing should follow the reference below:

Projected Coordinate System	:	WGS_1984_UTM_Zone_45N
Projection	:	Transverse_Mercator
Datum	:	D_WGS_1984
Prime Meridian	:	Greenwich
Linear Unit	:	Meter/Degree

Validation & Integration in GIS Map

- MSI shall check the source and reliability of the collected data from BSCL.
- **Positional Accuracy:** The MSI shall check the positional accuracy of the existing data available with BSCL with the Satellite Imagery.
- MSI would have to carry out Geo-referencing of the available data by using Ground Control Points (GCP) and DGPS survey instruments as required for the purpose and also for adjustment of spatially vectors Data. The MSI also needs to prepare Base Map using the available and fetched data and validation of the same will be carried out by the authorized officials of BSCL.

- **Accuracy Requirement**: The GCPs will be randomly checked for the accuracy by BSCL. In case of inaccuracy in any sample, the entire work of GCPs shall be rejected and MSI shall be required to rework.
- **Reliability:** The MSI shall also check from the available data with BSCL, whether the data (spatial or non-spatial) is recent or accurate enough to be used and not obsolete.
- The MSI is primarily responsible for generating/ gathering the data through other sources like Google Maps, Physical Survey etc. along with authenticated data input from BSCL.
- **Attribute Validity:** The MSI shall make sure authenticity of the non-spatial attributes for any geographical feature taken from any department or other.
- MSI shall Integrate House hold Survey & Tax Data
- The MSI shall be responsible for Solution finding and application update
- The MSI shall be responsible for All Data handover to SPV in secured manner- this is the property of SPV
- The MSI shall be responsible for Support, Maintenance, User Training & Annual update of the GIS database 3 months after completion of the hand.

Map Creation & Utility mapping activities:

- BSCL will provide (if available) the GIS Based Map (Geo-reference) in Shape file. As on date the boundary demarcation of the wards under Bhagalpur Nagar Nigam is not done. MSI will develop in concurrence with the Bhagalpur Nagar Nigam officials and complete this work – this is well within the scope of work.
- The MSI needs to procure latest High Resolution Satellite Image (0.3 m), License GIS Software's, GPS Devices, GPS Devices at their own cost which shall be property of BSCL.

Property Tagging with Property Assessment Mobile App:

The MSI has to undertake property tagging for all the properties registered with Bhagalpur Municipal Corporation and validate the existing data available with Bhagalpur Municipal Corporation. This activity is to be completed by MSI team with support from Bhagalpur Municipal Corporation field officials. The tagging of properties has to be carried out in ward wise manner. MSI can also take the print of the available data sets and base map, validate the same in the field, MSI may be required to confirm on the area of the property and other related parameters and identify any available details in the area of the property under survey. This exercise aims to validate and update the existing property tax database available with Bhagalpur Smart City Limited.

Collection of Survey Data through Tablet PC Apps

The data required to be collected for each Property Assessment activity shall be as follows (but not limited to):

Property Owner Details-1	
Owner ID*	***To be identified by MSI**
Owner Name	
Date Of Birth	
Occupation	
Email ID	
Contact No.	
Street	
Area	
Ward No.	
Ward Zone	
Pin No.	
City	**Default**
District	**Default**
State	**Default**
Country	**Default**
Remarks-1	

Land Details-2	
Property ID*	
Existing Tax ID	
Building/Shop/Company Name	
Society/Mohalla	
Flat/House No.	
Floor No.	
Floor Area/Carpet Area(Sq. Ft.)	
Plot Number	
Plot Area (Sq. Ft.)	
Title Deed No.	
Land Use Type	**Res./Comm./Open**
Description of Property	**House/Shop**
Year Constructed	
Building Use	
Residential/Non Residential	
Water Connection	
Gas Connection (Optional)	**Details from existing DB**
Telephone (Optional)	

Setup Box (Optional)	**Details from existing DB**
Professional Tax No. (Optional)	
Government Property	
Drainage Connection	
Building Height	
Solar Usage (Solar Rooftop/Street Light/Solar Heater/Solar Cooker etc.)	
Parking Area (Yes/No)	
Remarks-2	

Map Property-3	
Map Using Satellite Map	**Draw Land Parcels**
Map Using GPS	**Capture GPS Coordinate/Draw**
Take Picture	**Take from Device**
Date	**DDMMYYYY**
Surveyor Name	
Remarks-3	

** Property Id like that: State Code/City Code/Area Code (Zone)/ward No/Road ID/Property No.(Plot No.) /Building No./create Unique No. like owner Aadhar No., PAN No., Voter Card, Elec. Bill etc. Example ID like: 1010370301093403(combination of a few digits of any ID given by GoI/ State Govt.)

Process of Work

This section describes how the implemented mobile GIS application is operated and used. The first task in the property mapping process involves the capturing of the property attribute which includes owner details, land and property details. Property attribute data capture is carried out in three stages using three different screens.

Task-1:
The first screen that is used for capturing details that pertain to the property owner. Validation checks are performed to ensure that data is entered correctly and that all mandatory fields are not left blank. When the create button is clicked the property owner record is saved in the Postgres SQL database/Server and a unique owner identity number is generated.

Second screen that is used to capture land attribute data. When a valid Owner Identity Number is entered and focus moves to the next field, property owner names and national registration card number (NRC) are retrieved. The rest of the fields from the land use type to ward require the user to fill them manually. As data is entered in the fields, appropriate validation and mandatory checks are done. When the create button is clicked, the land record is created and a unique land identity number is generated.

Task-2: The third screen of second task involves the capture of spatial data and property image data.

The Third screen is display used to select the property mapping mode and also to capture images of the property like as

i. Map Using Satellite Map→Draw Land Parcels,
ii. Map Using GPS→Capture GPS Coordinate/Draw,
iii. Take Picture→Take from Device

Satellite image of the property mapping area when the Map Using Satellite Map option is selected. The mapper zooms in on the property using the (+) zoom icon. When the property is located, the mapper uses the line tool bar to draw the land parcel. When the Finish menu item is clicked, the GPS coordinates represented by the white squares are then saved to the database and an appropriate message is displayed.

Next screen for the Map Using GPS option. The GPS Blue Marker is displayed for ten seconds. As the mapper moves around, the marker also moves. When the approximate visual position of the GPS marker is on an approximate beacon location as guided by the underlying Open Street Map roads, a white square is placed on top of the marker to capture the GPS coordinates. This process is repeated for all the beacons. When the finish menu item is clicked, the GPS coordinates represented by the white squares are then saved to the database and an appropriate message is displayed. The take picture function invokes the mobile device camera to enable the mapper take pictures of the property. A picture is transmitted to the webserver for storage immediately which is taken. The application allows the mapper to take as many pictures as possible. All data should be captured in shape file format.

5.5 Functional & Technical Requirements for Database Layer

The database layer should provide the power and flexibility of the most advanced and secure database on the market deployed on premise or in cloud with the choice of a dedicated database instance, with direct network connections and full administrative control, or a dedicated schema with full development and deployment platform. The database must be a great option for Smart City solutions to consolidate and manage databases as platform and accelerate analytical performance while achieving new levels of efficiency, security, and availability. The database should provide capabilities such as:

i. Database should be available and function in multiple operating systems like Linux, and Windows.
ii. Database must ensure inter-dependency of user concurrency and data consistency. Should provide non-escalating lock mechanism and multi version read consistency for the transaction processing.
iii. The enterprise database should standardized across multiple key functionalities delivered over web and mobile channels as much as possible, but not mandatory. For example for City Web Portal and content management, ICCC operations, mobile apps, BI/analytics/reporting integration, IoT events storage, any packaged solutions.
iv. The enterprise database must have capabilities like plug ability, DB consolidation, optimized resource utilization by applying in-built multitenancy architecture realized using latest technologies e.g. containerization.

v. To protect against modern security threats, the database must support advanced security features like transparent encryption and redaction of data, encryption of data at rest
vi. Ability to service concurrent multiple read and write requests without the need of building separate replicated environments. Should have the ability to handle deadlock situations, without any application slowing.
vii. Should have built-in parallelism, Backup & Recovery feature, Disaster Recovery Feature, recovery for tables, rows accidentally deleted, and Mechanism to transfer data across to other database.
viii. The database software should be able to scale up multiple terabytes in decentralized and centralized environment. The database should be able to store gigabytes of data in single row.
ix. Should be able to provide database level storage management mechanism, which should enable the availability by means of creating redundancy, automatically balance the data files across the available disks, I/O balancing across the available disks for the database for performance, availability and management.
x. The high availability solution should be able to scale to multiple nodes and available 24*7.
xi. The solution should support vertical & horizontal scalability with minimal downtime and without repartitioning or changes to the database objects or 3rd party transaction routing mechanisms.
xii. The database should provide concurrent access from multiple servers to the single database image.
xiii. The database solution should have built-in DR solution to replicate the changes happening in the database across multiple DR Sites with an option to run real-time reports from DR Sites without stopping the recovery mechanism.
xiv. Database should have mechanism to protect data against human error.
xv. Should support different partitioning schemes within the database to split large volumes of data into separate pieces or partitions, which can be managed independently. The partitioning should enhance the performance, manage huge volumes of data and should provide foundation for Information Life Cycle Management (ILM).
xvi. The database should have option to create, use the logical partitioning of the objects (like Tables, Indexes) and use them. The option should be able to help in creating / managing the logical components online and be independent of the application solution being deployed.
xvii. Database should have automated/manual performance analysis with detailed diagnosis of the cause of performance related issues with possible resolutions.
xviii. Database should have option for automated/manual identification and tuning of high load SQL Statements. Provide details about dynamic tuning capability of the database depending on workload requirement, system resources etc.
xix. Should provide single system management view for database / database cluster. Should be using client independent, centralized database management console over network for monitoring database resources.
xx. Should be having built-in provision to administer database / database clusters, monitor performance, maintain database, backup and recovery, disaster

recovery management, diagnosis, performance tuning with the SQL analysis, finding the events, advisory based tuning mechanisms with the history.

xxi. End-to-end performance management and self-tuning tooling must be provided. Configuration and management should be performed from a unified user interface, preferably web-based. The administration UI should interface with the IT infrastructure to facilitate the management of heterogeneous data centers.

xxii. Fine grained and policy based auditing should allow users specify the conditions necessary for audit records to be generated.

xxiii. Database should provide highly efficient and flexible compression algorithms (e.g. compress partitioned tables at the individual partition level, reading compressed data without retrieving additional data etc.).

xxiv. In terms of partitioning, the database should allow adding, dropping, exchanging and moving partitions for disaster recovery purposes and administrative tasks.

xxv. High performance and scalability without additional management overhead should be provided.

xxvi. Integration of in-memory capabilities for all applications should be seamless and transparent. It should be fully compatible with all existing functionality and it should not require any changes to the application layer.

xxvii. Hot/online backup must be supported by the database.

xxviii. Real-time and zero-latency analytics should be supported by a multi-version read consistency data architecture, combined with in-memory capabilities.

High performance database appliances should be proposed to support high volumes of data processing and fast access to data.

5.6 e-Governance Applications and ERP Solution

Government data, made available in machine-readable, linked datasets that can also be searched and manipulated using standard tools, is a critical new resource for fuelling changes in value creation (economic, social and political) of a Smart City. The following are the benefits to opening of Government data for a city:

1. Improving government accountability, transparency, responsiveness and democratic control
2. Promoting citizens self-empowerment, social participation and engagement
3. Building the next generation of empowered civil servants
4. Fostering innovation, efficiency and effectiveness in government services
5. Creating value for the wider economy

These five benefits place a great emphasis upon the need for a city's governing body to engage with its citizens and listen to their needs when developing the Smart City. In general, governance has been defined "as regimes of laws, administrative rules, judicial rulings, and practices that constrain, prescribe, and enable government activity, where such activity is broadly defined as the production and delivery of publicly supported goods and services."

Thus, based on the five benefits outlined above, opening up government data to citizens encourages good governance. Good governance, in turn, encourages public trust and participation that enables services to improve. However, it is not only engagement between government and citizens that is essential to the success of a city becoming smart, all stakeholders need to engage and work together towards growing the city to meet their own.

An important factor is the role of policy making and city governance. Governance not only involves the implementation of processes for constituents but also for all the stakeholders within a city. The stakeholders' relations is one of the critical factors to determine success or failure of such projects. If we consider smart city projects as closely related to e-government projects then it is not impossible to wager that stakeholder relations may also play a key role in the success of smart cities.

One way of ensuring all stakeholders have access to digital services within a city is to ensure all platforms offering public e-services are open and available to the entire population. By using a fully integrated open system, which allows application developers within the community to develop software applications for the community based on the demand of the community, all stakeholders in the community can participate on an equal footing. Such an integrated system, when deployed by local government, can provide an open space for government, businesses and citizens to interact at a community level. This would allow each smart city or region to adapt their interaction between stakeholders according to their specific needs and the needs of the city, as voiced or demonstrated through the community platform. This in turn will foster innovation and increased participation from local stakeholders as they reap the benefits of their initial inputs.

ERP provides an integrated and continuously updated view of core business processes using common databases maintained by a database management system. ERP systems track business resources—cash, raw materials, production capacity—and the status of business commitments: orders, purchase orders, and payroll. The applications that make up the system share data across various departments (manufacturing, purchasing, sales, accounting, etc.) that provide the data ERP facilitates information flow between all business functions and manages connections to outside stakeholders. Following ERP modules need to be covered by MSI :

i. Finance and Accounts(including General Ledger, Payables, Receivables, Assets, Cash Management),
ii. Budgeting,
iii. Procurement,
iv. Inventory Management,
v. Contracts Management,
vi. Asset Management,
vii. Projects Monitoring,
viii. Human Resources Management (including Payroll, Employee Performance, Employee Self Service etc.)

Various features envisaged for the proposed ERP system in Authority, are being elaborated here:

c) Architecture

xxix. Centralized Server Architecture (n-tier architecture with web enabled user interface)

xxx. The presentation logic should be decoupled from the business components logic

xxxi. Data access layer should be on RDBMS platform. Backend RDBMS should be of latest proven version of leading RDBMS.

xxxii. Single Database (No Heterogeneous Database to be allowed as part of the proposed solution.

d) User Interfaces

xxxiii. The solution proposed should be Unicode compliant. Authority envisages requirements for both English and regional language for Data Entry, Display, Input and Output

xxxiv. Single Sign-on (for all the users) for accessing all the modules

xxxv. Any data entry needs to be carried out only once and further it should be made available as often as necessary to all the systems by providing pre-fill feature

xxxvi. All modules should be homogeneous with respect to Keyboard use, screen layout and menu operations with Graphic User Interface (GUI) support

xxxvii. GUI Form Administration should support

xxxviii. Changing fields or tab labels

xxxix. Hiding fields or tabs.

xl. Changing the position or size of field or labels

xli. Adding restrictions like mandatory or not

xlii. Setting default value in a field

xliii. Changing list of value contents

xliv. Capability to setup logic to trap conditions to pop messages in response to conditions like logical data entry errors, certain conditions etc.

xlv. Ability to provide various configurable parameters down to the end user level so that the user screens can have different functionality for a given user.

xlvi. Disparate information can be consolidated from a number of systems as required to produce reports and carry out ad hoc analysis and reporting

e) Access & Data Security

xlvii. Role based authentication for accessing various functionalities of different modules with encrypted passwords. Access Rights can be given to Individual Users or Groups

xlviii. Flexibility to define separate Role and Designation to the users. Upon transfers of officers / employees, applications / letters / complaints pending with the employee shall remain to the role and new employee will be able to take action on these applications / letters / complaints.

xlix. User rights to various forms should be Create New Record, View existing Record or

l. Edit existing record.

li. System should be able to capture exceptions to detect frauds / mistakes

lii. An audit trail of changes to data in the system should be maintained to identify the users responsible for the modification. There should be a facility to create reports on audit logs

f) Following minimum functional requirements are been envisioned in the ERP implementation:

liii. User – self registration and first time password change prompt.

liv. System would allow user to login and avail services from any of the modules.

lv. System would allow user to view any Service information from Departments displayed on Web portal.

lvi. During user id creation system would ask for Security question for any password reset request by user in future.

lvii. System would prompt user to create password as per security policy.

lviii. Alphanumeric passwords would be asked.

lix. System would ask user to create a transaction password to be used for performing any financial transaction with the concerned departments or while making any changes in the profile.

lx. During user id creation, system would ask user to furnish all personal details like

- Name
- Gender
- Age
- Address
- Phone No.
- Email ID
- Occupation
- Family details
- PAN/License/Passport/Voter Registration No./UID No. or any other ID proof details.

lxi. System would prompt user to login using user ID and password created and verify them.

lxii. On successful password match, system would allow the user to login to the portal and allow him to access his/her profile. On unsuccessful password match, System would generate password error message and ask user to enter correct password in order to login to his/her profile.

lxiii. System would allow user to edit his/her personal details like Name, Address etc.

lxiv. System would display the service related information/Instructions to fill up requested details in the entry forms like applicable fee and documents to be attached/submitted along with application request.

lxv. For CCC Operator, system would initially allow CCC operators to login using their login IDs and passwords as given by System administrator. After first time login by all CCC operators the system would ask them to change their password (alphanumeric) as per the security policy.

lxvi. After successfully changing the password and verifying the same on to the system, CCC operator would get access to all the modules, can accept and insert details of the requests received by the citizens for specific modules.

lxvii. System would display instructions to CCC operators at the time of inserting details in the request form for various applications.

g) For the design and development of intranet portal for the Authority for having exclusive access to employees of the Authority, same rules of user creation and authentication may be followed in addition to provisioning of device MAC No. being used by the official and also the domain in which the user is accessing the system. Messages and alerts would also be required to be provided on mobile and other user interfaces. It will also have system administration module for creation of user ids for various roles and responsibilities as per the official levels of officials for access to various privileges. Important applications in the intranet portal would be

lxviii. Employees Information System having unique Employee ID

lxix. Payroll Package

lxx. Leave Monitoring System

lxxi. Biometric based Attendance System

lxxii. Employee Performance Monitoring System, etc.

h) Profile Management:

lxxiii. Enable registered users to manage their accounts and profiles and as appropriate

i) Security

Based on ISO 27001/BS 7799 standards, user access to the system must be through a single sign on process, which should involve specification of a user Identification, a password and the applications displayed must be as per the user profile and authority. The system should allow user to change his/her password based on a given time frame as well as give the user the option to change his password at any time. The system should disable the user profile after five unsuccessful log-on attempts. The system should be able to log successful and failed attempts to the system.

j) General Requirements

lxxiv. Information, hardware and software would be secured to both internal and external parties (such as through password encryption).

lxxv. The security measures adopted should be of wide range and of high quality, to create confidence in the systems security and integrity. The system should be protected against deliberate or accidental misuse that might cause a loss of confidence in it or loss or inconvenience to one or more of its users.

lxxvi. System level and application level authentication between portal and between applications within portal, if any, to ensure against security attacks

There should be four levels of security considerations as described below:

f) Key Security Considerations at the User level:

vii. User authentication
viii. Role based access to services, transactions and data

g) Key Security Considerations at the Network/ Transport level:

ix. Network Link Encryption (IPSEC)
x. Encrypted HTTP session using SSL (HTTPS)

h) Key Security Consideration at the Infrastructure Level:

xi. Firewall to filter unauthorized sessions/traffic
xii. Intrusion Prevention System to detect/ prevent unauthorized activities and sessions

i) Key Security Considerations at the Application & Database level:

xiii. Secure storage of user credentials
xiv. Server–to-Server communication encryption
xv. Secured/ encrypted storage of data/ data elements in the Database & DB Backups
xvi. Comprehensive logging & audit trail of sessions and transactions

General conditions of Proposed Solution.

1 Fully integrated system
2 Real-time update and access of detail data
3 Facility to provide centralized key corporate services
4 Accurate and flexible mapping of organizational roles in the ERP
5 Accurate and easy availability of information with drill downs, drill ups with supporting data
6 Easy to set-up, learn and train. Facility for instant help.
7 24 X 7 system availability
8 Authentic, reliable, accurate and timely data
9 Business intelligence, MIS from the system (reports daily/weekly/monthly) comparison of data (Past / Current)
10 Robust System architecture
11 Scalable for future growth
12 Change management & control
13 Web enabled features

5.6.1 Unified Messaging System

a) SMS: The Web-Portal shall have facility to send SMS to Mobile number of a citizen which was provided while requesting certain information or service. The SMS shall be auto generated based on the information or service requested on occurrence of its change of status. All the application needs to be integrated with SMS gateway.
b) E-mail: The Web-Portal shall have facility to send e-mails to

   i. The e-mail address of a citizen, provided while requesting certain information or service.
   ii. The e-mail shall be auto-generated based on the information or service requested on occurrence of its change of status.
   iii. Reporting Officials maintaining the hierarchy, in cases of delay (as per the Citizens' Charter) in providing services.

5.6.2 Workflow Management System

Workflow Management System would serve as an integrated functionality across all the departmental modules to receive and process the request / applications received via any of the service delivery channels. Each request/application should be processed via workflow engine mechanism i.e. each of the application should be routed to the respective department official's activity dashboard. WMS should also have a facility of delegation of powers.

BSCL intends to have Workflow Management System implemented for all of the Government departments with at least 400x5 concurrent users (ie total 2000 Decision Maker Logins) and unlimited logins for portal users.

Below mentioned modules will be the part of proposed above ERP system to provide service delivery. The system will be flexible to scale up and configure the solutions and modules as and when required based on city requirement for governance and service delivery.

a) Citizen Service Module:

   i. Citizen Help Desk
   ii. Facility to lodge New Complaints, Check Status
   iii. Facility to check citizen data, Bill Dues, Application Status,
   iv. Payment Status, Renewal Status, Certificates issuance
   v. Internet & Intranet
   vi. Citizen Charter MSC, Authority

b) Application Acceptance & Delivery of Outputs

   i. Department-wise categorization
   ii. Allow system to accept service specific inputs
   iii. Capture of Mobile No. of Applicant
   iv. Re-submission of rejected application after compliance
   v. Check-list for documents to be submitted along-with application
   vi. Define citizen charter (list of the officers & duration for service delivery) Authority
   vii. Fees to be accepted Accounts

viii. Generate Token of Application acceptance
ix. Rejection Note in case of inadequate application
x. Delivery of the output through CCC / Internet / KIOSK
xi. SMS alert to applicant upon decision SMS Gateway

c) Payment Acceptance

i. Property Tax
ii. Accounts,
iii. Departmental
iv. Modules,
v. Property Tax
vi. Water Tax
vii. Professional Tax
viii. Vehicle Tax
ix. License
x. All Departmental Services
xi. Tender Document Fees
xii. Any other Services

d) Citizen Services (General) [Such services won't have any department specific functionality. CCC module, by using Workflow Management System should be able to deliver these services]

i. Marriage Certificate
ii. NOCs for other govt. departments
iii. Booking of various Corporation premises such as Halls,
iv. Community Halls, Open air theatre, Amphitheatre, Auditorium,
v. Ground, Party Plot, etc.,
vi. Issue of health license for shop having area
vii. Any other services

e) Marriage Registration Sub-Module

i. Design of Forms & Database for the Marriage Registration
ii. Functionality
iii. Capture of Thumb Impressions of the Applicants & Witnesses
iv. Capture of the Photograph of the Applicants & Witnesses
v. Scrutiny of the Applications

f) Professional Tax

i. Enrolment and Registry Enrolment of firms. (PEC & PRC) Property Tax,
ii. GIS
iii. Details of firms along with their contact details, address, etc. Property Tax,
iv. Outstanding Professional Tax details for different firms. Property Tax,

g) Vehicle Tax

i. Capturing Vehicle details such as Engine No/ Chassis no,
ii. Capturing type of Vehicle for collection of taxes.
iii. Capturing details of the Vehicle owner (Name, Address, Contact details, etc.)

h) MIS

i. SMS alert to applicant upon decision
ii. Services Statistics, CCC / KIOSK, Department-wise
iii. Officer-wise list of services pending HRMS, WMS
iv. Marriage Registration periodic / statistical reports
v. Professional Tax collection / outstanding report
vi. Interest calculation for outstanding Professional tax
vii. Defaulter list for Professional Tax payment GIS
viii. Property Tax collection report
ix. Report containing license issued details and payment
x. collected for the same.
xi. Vehicle Tax collection report

i) Modules for Government Office Functioning
i. File movement & tracking system
ii. Correspondence Movement & Tracking System
iii. Office Note Approval System
iv. Legal Case Management System
v. Parliamentary Query Management System
vi. Committee & Meeting Management System

j) Helpdesk System:
Workflow Management System should be integrated with Helpdesk System as mentioned at Section 8.1.2 with facilities like Auto-Routing, Auto-Escalation, User Management, Password Management, In-Built Form Builder & Process Designer etc.

k) Additional Functional Scope after validation

i. RTI
ii. Issuing License: Gumasta License, Hawker's License, Health license etc.

Workflow Management System is to cater various Internal & External Process Automations in terms of Citizen Centric Services, required solution should come up with following functionalities:

i. The system shall facilitate re-engineering of processes and act as a platform for building specific application and have a workflow engine to support different types of document routing mechanism including Sequential, Parallel, Rule Based & Ad-Hoc Routing.
ii. The system shall support Inbuilt Graphical workflow designer for modelling simple & complex Business Processes using drag and drop facilities.
iii. The interface shall be easy to use so that Process owners can change the business process as and when required without any programming knowledge.

iv. The system shall provide inbuilt facility to design Custom forms that can be attached at one or more stages of workflow.

v. The system shall provide facility to define variables in the process or in external database tables, which can be linked to fields defined in the form for efficient data entry.

vi. The system shall provide facility to define custom triggers like Emails, Word template or launching executable etc. on predefined conditions.

vii. System shall provide a facility to configure dashboard for individuals as per User Role or Group.

viii. The workflow management system shall support extensive password validations i.e locking of user account after specified number of unsuccessful login attempts, password history, password expiry, passwords must be alphanumeric and of minimum character length etc.

ix. The required workflow solution should comply to various open workflow standards such as BPMN, BPEL, WFMC.

x. The proposed solution should have the capabilities such as graphically modelling the processes or workflows, process simulator, integrated rules engine, inbuilt form designer, reports/dashboard tool and integrated Document Management System for storing documents.

xi. The solution should come with a Business Activity Monitoring System to facilitate users by providing a privilege based Dash-Board view.

xii. The proposed Workflow system must support advanced integration capabilities with support of SOAP and REST API's, Web services, XML and shall support interoperability.

xiii. Proposed Workflow Solution should act as Active-Active Clustering with DR site.

xiv. DMS & Workflow Management Solution need to be integrated with the all proposed & existing applications, which also includes:

1. Portal
2. Active Directory
3. SSL
4. SMS
5. Email

5.6.3 Document Management System

As the smart city concept includes paper less offices and digital information to the citizens and officials both, a Digital Knowledge Library shall be set up on the scalable and secured Document Management System in smart city solution and work a personal knowledge vault for the citizens and departments. It shall have all the functional capabilities of inbuilt viewer, metadata indexing, taxonomy, advanced and free text search, API and web services to integrate with all the feasible system.

Document Management System will manage huge load of documents in a digitized way. In addition, MSI has to provide Record Management System (Tightly integrated with DMS application) for the following objectives:

1. Implying various Retention Policies on the preserved documents as per Government Mandate

2. To locate the physical location of any documents during requirement Please confirm whether this understanding is correct

MSI has to provide Enterprise Document Management System with Industry Standard functionality having below key features:

i. Solution should be compliant to ODMA, Web Dav open source standards.
ii. Categorization of documents in folders-subfolders just like windows interface.
iii. There should not be any limit on the number of folder and levels of sub folder
iv. Document Version Management with Check Out / Check In
v. The System shall support Automatic full text indexing for Text search.
vi. Extensive document and folder level operation such as move / copy, email, download, delete, metadata association etc.
vii. Support archival & view of PDF/A format documents (open ISO standard for long term archival of documents)
viii. Repository should be format agnostic
ix. Indexing of the documents on user defined parameters
x. Association of the key words with the documents
xi. The Image applet shall support comprehensive annotation features like highlighting, marking text, underlining putting sticky notes on documents, and support for text and image stamps etc.
xii. Server based Inbuilt Document Image Viewer for displaying image document without native viewer
xiii. Viewer should be platform independent
xiv. Support comprehensive annotation features like highlighting, marking text, underlining putting sticky notes on documents, and support for text and image stamps etc.
xv. Automatic stamping of annotations with user name, date and time of putting annotations
xvi. Securing annotations for selective users
xvii. Content based Full Text Search should be available in English/Hindi language
xviii. DMS needs to be architecturally scalable and secured i.e. it shall have a separate image storage and only metadata to be stored in RDBMS.

xix. Documents need to be encrypted while being saved at the file server

5.6.4 Document Digitization

i. Should provide an integrated scanning engine with capability for centralized and decentralized Scanning & Document Capturing. The scanning and document management solution should be from same OEM so as to provide an integrated solution right from capture to archival of documents.
ii. The proposed solution should provide for automatic correction of parameters like format/ compression not proper, skew, wrong orientation, error in automatic cropping, punch hole marks etc. during scanning. The scanning solution should provide support for automatic document quality analysis. There should be an independent software quality check service available as part of overall scanning solution which can be used to audit scanned documents for resolution, format/ compression, orientation etc.
iii. The software solution should include the Rubber band feature for the extraction of the data using OCR technology so that user can mark a zone on image at runtime during scanning stage & map the extracted data with the indexing field.
iv. The proposed solution should have the proper scanning capability to produce an output with maximum visibility with minimum size.
v. The proposed solution should have a configurable interface so that adjusting scanning process i.e. Scan Mode, DPI, Automatic Record Segregation etc., can be easier.
vi. The proposed solution should have the facility to associate metadata with the respective scanned images.
vii. The proposed solution should have a tight integration capability with Document Management System.
viii. The proposed scanning solution should take care of automatic correction of parameters or image enhancement quality such as improper resolution, format/ compression not proper, skew, wrong orientation, error in automatic cropping, punch hole marks etc. so that the quality of scanned documents is ensured.

Functional Specifications - Secure Access	
1. Security Features	
1.1	Authentication and authorization must happen on a separate channel before allowing user to connect to any service / applications - i.e. only authentication and authorization controls to communicate via a specific port or control channel.
1.2	All authentication and authorization must happen over an encrypted channel and use mutual TLS.
1.3	Access to applications / services must only be allowed from pre-authenticated and pre-authorized devices and users
1.4	Devices must be verified on various factors to arrive at a set trust level (e.g.between 0 to 10). Factors to arrive at a trust level will include the device holding a valid client certificate, belong to the organisation domain, is assigned to a particular user, has updated AV signatures, has run AV scan in the last 1 day, has the latest OS patches installed and any other specific criteria required by organisation
1.5	IP address of application not to be revealed to end-user

1.6	The Gateway must employ Single Packet Authorization protocol (RFC 4226) with additional controls, like packets being signed using HMAC or certificates.
1.7	The Controller must employ Single Packet Authorization protocol with HMAC or certificates.
1.8	The client to connect to the Controller using SPA protocol followed by mutual TLS protocol to begin the device verification process followed by the user authentication process.
1.9	All users must be authenticated either locally by the Controller or via a 3rdparty authentication system such as AD, LDAP, RADIUS, SAML, 2FA providers etc.
1.10	Based on the authentication of the user and the trust level of the device, a final trust score must be assigned by the Controller
1.11	The Controller must check the available services to the user based on the final trust score and inform the endpoint / client on the available services.
1.12	When a client initiates an access to the available service, the Controller to be notified first, and the Controller in turn to notify the Gateway to accept the connection from the client.
1.13	The client to connect to the Gateway using SPA protocol followed by mutual TLS protocol and if both SPA and mutual TLS are successful, the Gateway accepts the connection and provides access to the application / service.
1.14	Any endpoint device without the client software should not be able to connect to the Controller or the Gateway nor discover/scan the services/applications running behind the Gateway as the SPA will fail. Hence Gateway is invisible, without a valid client software and valid client certificate. This will potect against network attacks such as Denial of Service (DoS), MITM and others.
1.15	Security against password-based attacks
1.16	Solution should provide protection against Eavesdropping
1.17	Solution Should Protect against Application-Layer Attack
1.18	Solution Should protect against Identity Spoofing
1.19	Solution Should Protect against Web based attacks like SQL injection, broken authentication and session management
1.20	Solution should Prevent Attacks from DDOS & DOS Attacks
1.21	Solution Should Prevent Web based attack :Insecure Direct Object References
1.22	Solution Should prevent Web based attack :Sensitive Data Exposure
1.23	Solution Should Prevent Web based attack :Cross Site Request Forgery (CSRF)
1.24	Solution should be able to detect Bad Packet detection ,there by detecting External network and cross domain attacks
1.25	Solution Should PreventWeb based attack :Using known Vulnerable Components
2. Scalability	
2.1	It must be possible to install / deploy the Gateway in any location to protect applications located in that location or in any other location. Essentially, the Gateway must be able to secure/protect applications / services irrespective of where the application is located. E.g. application may be located on-premises, in a private hosted data center, in a Public Cloud / IaaS platform (e.g. AWS, Azure etc.)
2.2	There must not be any limitation on the number of Gateways that can be deployed as part of the solution

2.3	The Gateway must be able to serve tens of thousands of requests per second – Specific performance requirements may require 3rdparty traffic management tools (e.g. Load balancers).
2.4	The Gateways being critical in enforcing access control must not be a SPOF. Hence, the Gateways must support full HA functionality to ensure continuous availability of services to users.
2.5	Endpoint agents should support Linux mint, RedHat,Ubuntu, Windows(Win Xp,Win7, Win8,Win10), Centos, Unix, Mac, Android, iOS.
2.6	The solution should be software based and gateway can be deployable on Open Source platform (Ubuntu. Centos) Or windows. The Platform should be scalable to 50000 concurrent users and Cloud ready software from day one
2.7	Solution should be based on Open standards
2.8	The solution should have inbuilt multi factor authentication, Mail, SMS (OTP), Smartphone tokens. Also it should support google authenticator as additional layer of security for the application access
2.9	The Gateways must continuously monitor the availability of the applications / services and provide alerts or notify Controller to redirect traffic to other locations as per configuration
3. Manageability	
3.1	The solution must support deployment of Gateways in multiple locations with minimum human interaction.
3.2	Gateways must support silent deployment methods using popular software distribution systems
3.3	Gateways must support simple and silent deployment into IaaS environments using popular tools such as Chef, Puppet etc.
3.4	The client agents must be lightweight and support silent deployment using popular software distribution systems
3.5	The solution must allow simple self-service style with user sign-up and activation method of deployment
3.6	The client agent must not require Administrator privileges to be installed
3.7	The solution must provide a single web based management console to manage user provisioning, device provisioning and policy management across all Gateways deployed in the enterprise
3.8	The solution must support access policies to be configured centrally irrespective of the location of the applications / services or the location of the Gateways.
3.9	The solution must NOT require solution administrator to configure individual access policies per Gateway
3.1	The solution must support bulk import of different objects such as users, groups, devices, ACLs etc.
3.11	The solution must support bulk management of various configuration details.
3.12	The solution must support role based administration. This will ensure that different administration tasks can be delegated to different administrators / teams.
3.13	The solution must support multi tenant architecture
3.14	The solution must support local datacenter
3.15	The software agent must be capabe to run as service
3.16	The software solution must have load balancing capabiities
4. Reporting, Monitoring, Logging and Alerting	

4.1	The solution must support live monitoring of all user activities including failed logins, invalid access attempts etc.
4.2	The solution must provide alerts for specific incidents over Email, SMS and/or SNMP
4.3	The solution must provide detailed logs for all solution administrator activities including login details, configuration changes, etc.
4.4	The solution must provide detailed logs for all user activities including application / services accessed, bandwidth consumption etc.
4.5	The solution must support forwarding of all logs to Syslog and popular SIEM solutions
4.6	The solution must provide customizable Dashboards to allow continuous monitoring of the health of the solution
4.7	The solution must provide multiple reporting templates (especially compliance related templates) with support for charts and graphs as well as the ability to drill down into the detailed logs
4.8	The solution must allow creation of custom reports using combination of different log tables through an intuitive wizard
5. Two Factor Authentication	
5.1	Solution must provide 2FA which shall have provision to assign single & multiple type of tokens to a particular user. (SMS, Email, Google Authenticator)
5.2	Solution must provide 2FA which shall be able to support self provisioning system.
5.3	Solution must provide 2FA which shall log all transactions & logs and shall support standard reporting packages for generating reports
5.4	The 2FA Solution Should be tightly inbuilt feature with SDP Principles (Software based Defined Perimter) to provide Encrypted communication to the applications hosted on the Datacentres which are invisible to oustide world & 2FA Should be on the Single Console for Ease of Administration
5.5	Soft token of 2FA Solution shall have following features:
5.6	Token shall generate password dynamically within every two minutes or less.
5.7	Token Application that generates the password shall be PIN protected.
5.8	Token shall have atleast six digit numerical passwords.
5.9	Token shall be available as a software form factor. Mobile token shall be able to install on mobiles with iOS, Android.
5.1	Every token shall have unique identity & shall be unique to user.
5.11	Token shall be time synced with authentication server.
5.12	Token shall be time synced with authentication server.
5.13	Solution should be built on open source platform.
	6. Others
6.1	The solution must support automated and encrypted backup of configuration using a configurable schedule.
6.2	The solution must support backup of configuration to local disk or network location using SFTP or HTTPS or a mapped network drive.
6.3	The solution Database must be automatically backed up regularly as per configurable schedule without any downtime.

6.4	The user agents must be simple to install & resinstall , The Soft agents on the Endpoints should be light or less than (1.7MB) , requiring almost zero resource consumption
6.5	Application performance after installing the agent should not hinder the performance & Should work on the Broadband internet based access
6.6	Solution should be built on open source platform (Software defined perimeter)framework, cyber security framework

Functional Specifications - Continous Vulnerability Assessment	
1	Solutions should provide a platform for managing vulnerability report submission and vulnerability report assessment with full transparency and activity history
2	Data residency of the platform should be in India and operated by Indian Solutions provider
3	Provision for role-based access for the organisation to add their users and provide different access based on their roles (Developer, Manager, Testers, operations, etc)
4	Able to define the list of scoped digital assets to be tested, the testing guidelines on the platform, Scope and Out of scope vulnerabilities to be tested, and any other instructions to be disclosed to security researchers for testing
5	Enable add or remove any security researchers/testers for reporting
6	Have provision for receiving vulnerability reports from security researchers through the invite-only program or through public vulnerability disclosure programs in accordance with ISO /IEC 29147:2014 standard
7	Solutions should maintain a record of all security researchers with their valid Identity proof, legal contracts, communication address, and user activity
8	Able to evaluate vulnerability submission as Valid, In-Valid, or Duplicate submission
9	Allow communication between organisation users and security researchers under each vulnerability report submission
10	Real-time notification to organisation users for every submission of vulnerability reports
11	Awarding and making payment to security researchers based on the report submission. Maintaining a record of all payment transactions with details of bugs, security researchers, amount paid with the date of payment
12	Provide a comprehensive report of the final delivery with numbers of bugs reported, Bug severity, Bug open/ closure status, Payment details

5.6.5 Functional Requirement Specification- Trade & Market License

1	System should be able to capture/ edit/ delete the details of inspections done by a market license inspector.
2	The system should have facility to assign the application to the respective Inspector for survey and verification.
3	System should allow the inspector to enter the field visit details and filed visit report should be generated and automatically routed to the superintendent.
4	System should allow the approving authority to approve or reject the report.
5	Inspection work flow, cancellation or change in ownership information etc. process will be as per standard defined workflow in the proposed system.
6	System should allow the SMS alerts to the applicant regarding the date of inspection / visit by the inspector, approval / rejection of the application.
7	The system should generate the reports for which data was submitted after each inspection.
8	The system should have Facility to create/edit/update the deficiency/Inspection report against the application.
9	The system should facilitate Inspection Entry
10	System should have ability or facility to prepare and allow to verify the report prepare by inspector.
11	System should have ability to allow approving or rejecting the report.
12	System should able to maintain& generate the records of show cause notice.
13	System should have facility for Generation of Show cause Notice
14	System should be able to generate hearing notice.
15	System should maintain the details of Hearing
16	System should have facility to enter the details of dishonoured cheques.
17	Capturing of the license fee/late fee details (Cheque/DD details, online, through banks etc.)
18	System should have the facility of Cancellation of License by Force.
19	System should have provision to Issue new trade license
20	System should have ability to do the scrutiny of applications
21	The system should have provision for routing of the documents through the ULB Counter and online approval/rejection by market license department.
22	System should have the facility to assign unique identification number based on license type, which will be used for all future transactions of the license.
23	System should allow the applicant to apply for a license for multiple years.
24	System should allow generation of license and intimation to applicant through SMS or e-mail.

25	The system should allow generating paper based license.
26	The system should have provision to issue license for Rickshaw. This can be handled by parameterization process in common master module.
27	System should have facility to allow generating paper based license.
28	The system should have provision to record NOC, if required, for a new business.
29	The system should have provision to issue duplicate market license
30	The system should have provision to renew the existing market license.
31	The system should have provision to change the name of the business
32	The system should have facility for Change in Business
33	The system should have provision to cancel the market license by application
34	The system should have provision to transfer the license under nomination (hereditary)
35	The system should have provision to transfer the license via any other mode than nomination.
36	The system should allow the online payment of license fee.
37	System should have the facility to define the rates for generic taxes on basis of various parameter like Flat / Slab wise, Value types – (percentage-Amount-Multiply) , depend on tax sub criteria,
38	System should have ability to Add / Edit/ Search / Delete charges.
39	System should be able to link the services with the charges associated with the services.
40	System should have ability to Add / Edit/ Search / Delete charges
41	System should have facility to define rates for taxes specific to particular license category.
42	System should have facility for Maintenance of matrix for license fee details with an option to keep the records even after new rates become affective
43	System should have ability to Add / Edit/ Search / Delete charges
44	System should allow provisions for rebates/discounts etc.
45	System should be able to define the renewal schedule of the license on the following criteria: • Calendar Year wise • Financial Year wise • For a fixed period from the date of license
46	System should be able to identify and define the charges to be taken from Tax Master or Rate Chart for a particular service.
47	System should be able to define the Ward-Zone-Block Hierarchy.

48	System should have facility to define license type - sub type, category – sub category.
49	The system should be able to print new market license based on the application number selected.
50	The system should re-print market license based on the license number selected.
51	The system should be able to generate reminder notice for market license renewal based on individual license number
52	The system should be able to generate reminder notice for market license renewal based on license category
53	The system should be able to generate the list defaulters who have not renewed their license after the license renewal date has expired.
54	The system should be able to generate the renewal notice for the defaulters who have not renewed their license after the license renewal date has expired.
55	The system should allow intimating the applicant about the payment of license fee through SMS/ email.
56	System should automatically send the alerts to the License holder 30 days before the license/registration expiry.
57	The system should be able to generate the report containing: • License details • License holders details • Business details
58	The system should maintain the details about License holder details, like, owner name, shop /rickshaw, address, purpose, date of issuance, license number etc.
59	The system should be able to generate report showing the summary of demand/Collection/outstanding amount of market department revenue.
60	The system should able to generate any other fixed format and Ad-hoc reports as desired.
61	System should print Reports showing Changes in License Types, Business Partners, Cancellation Licenses, etc.
62	System should have Facility to forecast the impact of reduction / deduction of License Fee.
63	System should print Reports w.r.t. Bills / Notices generated
64	System should allow the Generation of receipt for the payment.
65	System should generate the Reports showing the number of licenses approved/rejected.
66	System should generate the Report showing the number of license pending for approval/rejection.
67	The system should have Integration and Interface to use digital signatures on various resolutions passed, estimates approved and proposals rejected.
68	System should print reports related to E-Mail / SMS to be sent to the owner upon transactions
69	System should allow printing the license, sending the license through e-mail.

70	System should automatically send the alerts to the License holder 30 days before the license/registration expiry.
71	System should allow the SMS alerts to the applicant regarding the date of inspection / visit by the inspector, approval / rejection of the application.
72	System should allow generation of license and intimation to applicant through SMS or e-mail
73	System should sent reminders for renewal of license 30 days prior to the expiry
74	System should allow officials to send the digitally signed certificate to applicants through e-Mail and send details of license through SMS.
75	The system should have the facility to deliver the service online & through Municipality Counter.
76	The portal should have all the information including the processes and documents required for the convenience of the citizen.
77	System should capture all the details required for application.
78	System should have the facility to apply online and through the ULB Counter.
79	System should have a facility for online payment and through the ULB Counter.
80	System should have the facility to download form, online filling and submission of form.
81	System should ability or allows the online payment of license fee.
82	The system should have a facility for online payment and through the ULB Counter.
83	The system should provide the functionality for checking of non-payment cases and issue notices and forward these further for court cases, if required.

5.6.6 Functional Requirement Specification–Land and Estate Management

Sl. No.	Requirement Description
1	**Masters**
	▪ The master for booking services and rent and lease should be common masters to carry out transactions.
2	**Booking Services**
	▪ All services under the Booking Modules are to be used under the Rent and Lease Module.
3	**Lease Rent Payment / Quick Pay**
	▪ Lease Rent Payment option will be for online payment and direct debit with total flexibility. ▪ Lease Rent Payment will be for offline using challan at ULB or Bank or CFC. ▪ By using contract number, the customer will get the outstanding amount, the name of property/estate, estate name, property name, unit no. etc.

	▪ The system will ask for the mobile number and email address before submission of payment. ▪ The system will show the outstanding payment but, the customer can edit the amount whatever he/she desire to pay. ▪ The system will notify the client in case of failed transactions through SMS or Email. ▪ Successful payment alert will be sent through SMS and Email to the customer.
4	**No Dues Certificate**
	No Dues Certificate is the letter that certifies that the property has paid all his/ her dues/ outstanding. ▪ This service will be applicable to leased properties. ▪ This service will be certificate based service. ▪ The system will have provision to define service as immediate or period base. ▪ The system will check dues before accepting the application. ▪ The system will have provision to generate No Dues Certificate for multiple years. ▪ The system will intimate applicant to pay the dues and link of bill payment will be provided which will be redirected to bill payment form. ▪ Later after successful payment applicant will be able to apply for No Dues Certificate. ▪ The system will be able to accept application through Web Portal, Agency Login, Citizen Facilitation Centre/ULB Counter and Department. ▪ The system will have the facility to accept application in Regional Language. ▪ The system will allow modification in application form until application charges are paid. ▪ The system will have provision to apply new rates which are currently active or applicable. ▪ Applicant will be able to select the service from his dashboard against No Dues Certificate. ▪ Application Number will be generated once all the required details in the mandatory fields are entered and submitted. ▪ After submission of application, the system will Auto Generated Application Number. ▪ After successful submission of application, Applicant will be notified via SMS and Email with the details of service, payment and application number. ▪ The system will have the facility to generate Acknowledgment Receipt for applicant's reference. ▪ Acknowledgment Receipt will be generated if the application is accepted through Web Portal, Agency Login, Citizen Facilitation Centre/ULB Counter and Department.

5	**Contract Agreement**
	▪ The system will have the facility of contract agreement as a common component to be used wherever a contract is needed. ▪ The system will have a facility to create a Contract Agreement before assigning the work to a vendor. ▪ The system will generate a contract with unique contract number. ▪ The system will have the facility to search contract number. ▪ Contract creation form will have provision to show the history of the contract created against a contractor/vendor. ▪ Contract Number will have a combination of alphabets and numbers. ▪ Contract number will be auto generated on submission of contract. ▪ The contract will be created in between two parties. and each party will have the facility to add multiple witnesses. ▪ The system will have the facility to capture and read Photo and Thump impression. Also, manual process of uploading is required. ▪ The Party I will be treated as ULB representative and will have the facility to capture Department and Designation and Name of the representative. ▪ The Party II will be treated as vendor/supplier/contractor/vendor. The vendor information will be fetched from vendor master. ▪ Provision requiredto add multiple vendors under single contract and select primary vendor ▪ The system will have provision to enter the tender number, tender date, resolution number and resolution date. ▪ The system will have provision to define various contract types. Such as contract against the lease, contract against services, contract against supplies etc. ▪ The system will have provision to define contract term by providing contract from date and to date. ▪ The system will able to create a commercial or non-commercial contract. In commercial contract, the system will ask for contract amount payable or receivable, contract amount, security deposit and its details, payment terms in weekly, monthly or yearly or whatever values defined. ▪ The system will have provision to enter No. of Installment of payable or receivable. ▪ The system will split the rows of payment schedule according to entered number of rows. ▪ In payment schedule, the system will allow the user to select the payment mode as per amount or percentage. ▪ If selected amount the system will allow the user to enter an amount or if selected percentage then the system will allow the user to enter the percentage. The percentages will not more than 100%. ▪ The system will also allow the user to enter milestone for the payment schedule defined.

	▪ In non-commercial contract, the system will not ask for any amount related details. ▪ The system will have the option to select for allowing renewal. If the user selects the option then, the system will allow renewing the contract. ▪ On completion of contract tenure, the system will auto close the contract. ▪ The system will have the facility to upload documents against the contract. ▪ The system will have provision to enter terms & conditions. ▪ After submitting the contract, the system will send the contract to higher authorization as per workflow defined. Authorization procedure will be parametric. In case if rights of contract creation are given to authorised person then, he/she will have permission to generate contract him/herself. ▪ The system will have a facility to generate repayment schedule on submit button. ▪ The termination of contract will be taken care by the department where the contract is assigned any work, service, area etc. ▪ In the case of contract termination, the process will be done through the respective department. ▪ Printing of contract will be done through the respective department.
6	**Contract Mapping**
	▪ The system will have the facility to map the contract against the property given on lease. ▪ By searching the contract number the user will be able to view the contact details. ▪ The system will provide facility to select location and estate. On basis of estate, the user will able to search and select the property. ▪ The system will have the facility to map multiple properties against a contract. ▪ Once the property is assigned/mapped against contract then the property will not be searchable until the contract period is finished or terminated. ▪ The system will have the facility to print the contract. ▪ The user will be able to select the unmapped contract no in contract mapping ▪ The print button will the facility to display a preview of the contract before printing.
7	**Demand Posting And Repayment Schedule**
	▪ The system will have the facility of posting demand at the time of contract agreement creation. ▪ Various contract type will separate estate or property. For example, Lumpsum Amount Contracts for example Parking Lot, Public Toilets, Municipal Gardens (amusement parks) Fix rent collected periodically (monthly, quarterly, yearly) e.g. Shop Rent ▪ Considering same, the system will generate repayment schedule of contract amount or rent as per contract term.

	▪ For example, if monthly rent is fixed for INR. 1000 and lease out for three years then, after generating repayment schedule 36 entries will post in demand table with the date of instalments. ▪ The system will also consider the calculation of the appreciation percentage if rent is change by ULB after a period. Accordingly, the schedule will generate. ▪ If the contract is terminated in the middle of the contract term, then pending entries of demand will be marked as "Terminate" and accounting entries will reverse. ▪ Auto reminder through SMS, Email will be sent monthly (as configured) for the outstanding amount. ▪ The system will consider a due date for the outstanding amount. ▪ The system will have provision to calculate interest on the due amount after the due date. ▪ Interest will be calculated as defined in Tax Rule. ▪ The department user will have the facility to define interest rate and interest calculation method.
8	**Rent Notice Generation And Printing**
	▪ Provision of Rent Notice generation and printing for the estates or properties having the outstanding amount. ▪ The outstanding amount will be the sum of all the rents which are due. ▪ A notice printed will show all the details of rent which are not paid as per repayment schedule. ▪ The system will have the facility to print rent notice for a single as well as for many Estate or Property. ▪ The system will have the facility to print duplicate rent notice for the individual as well as for many Estate or Property. ▪ The system will have the filter options for Estate type or Subtype and department user will have the choice to choose selected properties. ▪ Facility of Digital Signature, the Scanned Signature option will be provided on Rent notice. ▪ The system will have the facility to define a location hierarchy wise scan signature. ▪ The notice will have the facility to be printed in English and Regional Language. ▪ The system will maintain a history of every generated notice. ▪ The historical data of notice will be used for further communications by providing a previous reference number on notice generated each time.
9	**Contract Renewal**
	▪ Contract renewal will be allowed for those contract which is marked as "Allow Renewal" at the time of initial contract. ▪ A contract renewal form will have provision to search according to contract number, contract date, department or vendor name. ▪ A contract renewal form will have provision to view contract details.

	▪ A contract renewal form will have provision to view previously renewed entries. ▪ The system will auto fetch FROM DATE and the user will able to enter TO DATE of renewal according to contract period. ▪ The system will allow changing following the information at the time of renewal: o Contract Amount o Security Deposit Receipt No. o Security Deposit Date o Security Deposit Amount o No. of Installments and details of instalment. o Document Uploading o Terms and Conditions o Renewal Details – Renewal To Date ▪ Here in renewal, the mapping form will not be considered as the property or the asset is not going to change. ▪ Therefore, the bill generation/repayment schedule will be created on RENEW button itself. ▪ The provision of renewal will be entitled to department user.
10	**Contract Revision**
	▪ In the case of a change in the contract in between the contract period, the system will have Revision process, and its functionality will be as follows: ▪ Provision to do the multiple revisions within contract term. ▪ Changes modified in the contract will be tracked. ▪ Provision to regenerate repayment schedule as per effective modification within same contract duration. ▪ Demand will be modified accordingly with effective changes. ▪ Original contract will remain same and the revision done will be stored separately. ▪ The system will allow modifications for following fields: o Contract Amount o Security Deposit Receipt No. o Security Deposit Date o Security Deposit Amount o No. of Installments and details of instalment. o Document Uploading o Terms and Conditions ▪ The system will have provision to print revised schedule. ▪ The system will have provision to capture remark/reason against the revision. ▪ The system will consider revision only if the last payment is paid by the vendor. The system will not allow revision in case outstanding. ▪ If the revision is done in the middle of rent duration then, the system will consider the 1st date of that month, quarter, semester, and year.

	○ For example, if vendor applies for revision on 15th August of the month, then rent duration will be considered from 1st August in the monthly billing cycle. ○ In the case of quarterly billing cycle, 1st April to 30th June – vendor applies on 31st May then, the rent duration will be considered from 1st April. ○ Same logic to be used for rest of the billing cycle. ▪ Revision will be allowed only in case of initial contract. ▪ There will not be a facility to revise the contract in case of renewal contract.
11	**Contract Transfer (Sub-Lease)**
	▪ Contract Transfer or Sub-Leasing can be optional service dependent on ULB decision. ▪ Contract transfer will be allowed for an only remaining period of the initial contract. Department user will not be able to change the duration of the contract. ▪ Contract transfer form will fetch information of previous vendor/occupant information with contract number, date, validity from date, validity to date and documents. ▪ Contract transfer form will have the facility to enter new vendor/occupant information along with name, address and contact details. ▪ Old contract details will remain same and new vendor name will be additionally added. ▪ Contract transfer form will have the facility to upload a document of the new occupant. ▪ Contract transfer form will have the facility to make the payment online or offline through generating challan. ▪ Provision to show charges applied while making the payment. ▪ After submitting the application will be sent to higher authorization as per workflow defined.
12	**Freeze Rent Property**
	▪ The system will have the functionality to mark the rented property as Non-Available for a specified period. ▪ Department user will be able to choose the property and define the period and time to freeze the property (make it unavailable). ▪ The functionality will also have a facility to revoke or roll back the non-availability status as available at any instance. ▪ This feature shall be used when the property is under renovation or ULBs internal use. ▪ The system will have provision to capture remark/reason for freeze property.
13	**Refund**
	▪ The system will have provision of refund for security deposit and booking cancellation.

	▪ The system will have provision to calculate the refund by deducting the brokerage charges against the security deposit and cancellation charges according to slab as defined in BRMS. ▪ The refund will have facility of maker and checker workflow. ▪ On the approval of checker, the system will generate refund letter containing all details of refund along with deductions.
14	**Collection**
	▪ The system will be able to collect the rent as per contract and generate receipt as per process. ▪ The system will be able to generate a receipt number for every collection made. ▪ The vendor will able to pay the rent online, offline using Challan, at CFC using various modes like CASH, DD, CHEQUE etc. ▪ The system will auto post the transaction if integrated with accounts module. ▪ The system will able to generate a report of collection done against the rent and contract. This report can be later used for accounting reference in the case of accounts module not integrated.
15	**Receipt Entry For Bill Collection**
	▪ The system will allow collection of rent through ULB counter, online using a payment gateway and Online through agency login. ▪ In the case of Collection from ULB counter, payment will be accepted against an outstanding bill or as an advance against a particular contract. ▪ The system will show the current outstanding amount due while collection entry. ▪ The system will allow acceptance of Cash/Cheque/Demand Draft/Pay Order. ▪ Partial payment, as well as excess payment, will be allowed against the contract. ▪ Interest will be applied and accordingly bill tables and receipts tables will be updated. ▪ If Interest at the time of receipt is generated within the repayment cycle of the last bill, then Interest to be posted (stored) in the current column of that bill. ▪ If receipt date is not within the period of the last bill then, interest will be stored in a table and applied to the bill when the bill is generated for that period. ▪ The vendor will be able to pay bills for more than one contract in the following combinations. o Single Contract – Single Payment Mode o Multiple Contract – Single Cheque/DD ▪ The system will have parametric setup to accept full or part payment against payment done choosing Cheque/DD. ▪ The system will allow Full/Part/Excess payment.

	▪ In the case of **Full Payment** sequence/order of collection will be considered. ▪ The system will have parametric setup to accept part payment against current bill. Arrears Bill will not be allowed to make part payment. Also, it will not allow accepting the Cheque and treating the last bill as part payment. ▪ In the case of **Part Payment,** sequence/order of collection will be considered. ▪ **Excess Payment** received earlier will be treated as credit amount and it will be adjusted while issuing the next bill. ▪ The system receipt will have details such as Receipt Number, Receipt Date and Time, Department, Received from, Payment mode, Charges Details, Amount etc. ▪ The system will generate receipt in 2 copies i.e. Office Copy and Customer Copy in case applicant makes the payment at ULB counter. ▪ Sample format of receipt is given below for reference. It might change as per details which need to be displayed. ▪ The system will have SMS and Email facility for Receipt with details of tax breakup.
16	**Cheque Clearing and Dishonour Cheque Details**
	▪ The system will have two options against cheque collection i.e. Cheque Clearing and Dishonour Cheque. ▪ The system will capture Cheque Clearing Date (Reconciliation Date) once the cheque is realised by the bank. ▪ The system will have the facility to import cheque clearing date from.CSV or .XLS format provided by the bank. ▪ The system will import the.CSV and.XLS file bank-wise. ▪ The system will capture Dishonour Cheque Date if in case the cheque is bounced. ▪ Department User will able to search all the cheque entries whose cheque clearing or dishonour date entries are not done. ▪ Searching will be provided as per Organisation ID, Department, From Date, and To Date. ▪ For the grid, following list of fields will be shown by the system: o Cheque Cleared – Checkbox o Enter Cheque Clearance Date – Date field using Calendar selection o Cheque Dishonour – Checkbox o Enter Cheque Dishonour Date – Date field using Calendar selection o Enter Penalty Charges – Textbox (numeric with two decimal formats)
17	**Special Exemption**
	▪ The special exemption will be applicable to define exemption on charge calculation.

	▪ The special exemption tool will have provision to define the criteria for exemption on basis of estate/property, subtypes, purpose, applicant type, applicable period, applicable times. ▪ The system will calculate and provide the details of exemption as per the criteria define in special exemption tool. ▪ The system will able to provide exemption on the charges calculated through BRMS. ▪ The exemption will be provided on selected criteria and by providing the exemption either in percentage or amount. ▪ The system will allow to add multiple exemptions for single estate/property. ▪ The system will also allow to choose ALL option for estate or property.
18	**Legacy Data Import And Export**
	▪ This facility will be used to import and export old contract details into the newly implemented database. ▪ Data import and export will be done using excel file. ▪ The defined template will be used to import and export data.
19	**Arrears Entry**
	▪ Provision for arrears entry during the initial implementation of software/application. ▪ Provision for adding arrears amount with respect to previous outstanding pending against taxes.
20	**Contract Deletion**
	▪ Provision to delete a contract for a selected contract number. The deletion of the contract will not be possible in case a receipt is generated for the contract i.e. the user will delete the contract before generating a receipt for it. ▪ The wrongly generated contract will be deleted through this tool. All these deleted contracts will be maintained in History table having the same table structure as that of the actual contract.

5.6.7 Functional Requirement Specification- HRMS

1	The system should have following defined masters. This is tentative masters, additional masters and sub masters are to be defined to ensure maximum configurability of the system. • Location Master • Department Master • Calendar Year • Holiday Master • Cadre Master • Reservation Master • Sanction Post & Opening Balance Master

	• Pay Band & Grade Pay Master • Pay Scale Master • Leave Master • Loan Advance Configuration Master • Employee Master • Bank Master • IT Section Master / Taxation Rules • Allowance/Deduction Master
2	The system should have provision for adding online the sanctioned post for recruitment.
3	System should have facility to maintain Vacancy Computation details year wise and class wise.
4	Indent Should be classified in Sanctioned Post, Contractual Appointments, Outsourced Employees, and Daily Wages &Deputation Indent Post.
5	System Should have facility to store and Print the Job Advertisement Details
6	System should have provisions to Apply & receive the Job Application documents/information Online.
7	System should have facility to capture the Candidate details from Application.
8	System Should have facility to generate and Print the Admit Cards
9	System should have facility to capture the Candidate details from final Merit List & Application Store (Roll No, Name, Post Address Grade Pay and Other Details).
10	System should have the facility to generate the offer letter
11	System should have facility to generate and print the selected candidate Joining Documents Details.
12	System should have facility to generate and print the Joining Letter along with the list of selected candidates
13	System should have facility to generate and print the list of selected Appointment Letter
14	System should have facility to generate and print the list of selected Appointment Documents
15	System should have facility for Addition, Modification, Cancel, and Search of Employee Details.
16	System should assign the unique ID to each Employee.
17	System should capture the Standard employee
18	System should have facility to assign the basic pay band & Grade Pay
19	Systemshouldhavefacility to add /Modify/Cancel and Search the Pay Fixation.
20	System should have facility to capture the Candidate details from Employee Data (Employee ID, Name, Post, Address, Grade and Other Details) & Pay Fixation

21	System should have the capability to manage the employee transfer.
22	System should have the capability to manage Annual Performance Assessment Report (APAR)
23	System should have facility to capture the Employee Feedback against the predefined Criteria / Points.
24	System should have the facility to manage the increments for the employees
25	System should have the facility to manage Modified Assured Career Program (MACP) for the employees
26	System should have the facility to manage Compassionate employment
27	System should have the facility to manage Employee Demotion/Reversal
28	System should have the facility to manage Employee Ad-hoc Promotion
29	System should have the facility to manage Employee Suspension
30	System should have the facility to manage Employee Separation
31	System should have the facility to manage Advance Request / Advance Adjustment for the employees
32	System should have the facility to manage the events for the employees
33	System should have the facility to manage the payments for the Utility Bills of the employees with auto deduction form salary
34	System should have the facility to manage Telephone Bills payment for the employees
35	System should have the facility to manage the Rent Payment of the employees
36	System should have the facility to manage the Reimbursement Request of the employees
37	System should have the facility to manage the Request for Higher Education by the employees
38	System should have the facility to process the request for NOC for Passport / Visa
39	System should have the facility to manage Asset Declaration process / Asset Purchase Request of the employees
40	System should have the facility to manage the advances and loans request by the employees for events like house construction, marriage, medical purpose, etc.
41	System should have the facility to manage the Request forEmploymentOutsideOrganization
42	System should have the facility to process the leave request and approval
43	System should have the facility to process the compensatory off request and approval
44	System should have the facility to manage the daily attendance of the employees

45	System should have the facility to manage the tour program and travel advances for the employees
46	System should have the facility to manage the festival advance request by the employees
47	System should have the facility to process the Employee complaint & Grievance
48	System should have the facility to generate Show Cause Notice
49	System should have the facility to generate Charge Sheet
50	System should have the facility to manage the Departmental Enquiry
51	System should have the facility to manage the penalty levied on the employees along with the details of the final penalty imposed
52	System should have provision for employees to appeal against any penalty
53	System should have the capability to generate the MIS reports and as per the finalized requirements

5.6.8 Functional Requirement Specification- Payroll& Pension

01	System should have provision for Payment rules for department / location / personal level along with the following definitions • Define Pay Code • Define Deduction Code • Define Basis Formula • Define Reimbursement • Define Benefit Code • Define Loan and Advance • Define Provision Master • Define Perquisites Category • Define Deduction Details • Define Professional Tax Slabs • Define TDS Calculation Slabs
02	System should generate & Print Employee Subscription details
03	System should have facility for managing Employee wise Loans & Recoveries details
04	System should have the functionalities for the Investment Declaration for Income Tax
05	System should have the functionalities for the Monthly Payroll Processing considering the following parameters: • Flexible periods for pay calculation • Exception definition for salary processing for department / location / personal level

	• Salary processing based on roles and responsibility assignments. • Automatic calculation of deductions / earnings based on leave, bonus declaration, Loan, tax deductions, etc. • Rule based salary calculation in case of pay hikes / pay commissions with retrospective effect • Classification of all salary elements as Earnings, Reimbursements, Deductions, Tax Deductions, PF, etc. • Tax calculations as applicable • Periodic / specific deductions as applicable • Reprocessing of salary prior to authorization • Authorization of salary processing • System should have ability to pay an employee from more than one Department and split salary and benefits among Departments, including retirement benefits • System should have ability to report retirement deductions by employee. For Widow, Dependent, Old Age and Handicap Scheme, there must be provision to apply and approve it online. • System should have facility to automatically update the service book In case the leave is paid or unpaid along with salary details. • System should have facility for pint Salary Register details report.
06	System should have facility to manage the Employee wise PF Subscription details
07	System should have facility to add/modify /Search the Pension Detail for the employees
08	For pension matters the personnel management system and accounts must be integrated. There must be provision in system to route the pension application in the portal for approval.
09	System should have facility for Proper audit of reports to make pre audits regarding the pension and retirement benefit calculation.
10	System should have facility to generate and Print Pension Copy.
11	System should have the capability to generate the MIS reports and as per the finalized requirements

5.6.9 Functional Requirement Specification– Property Tax Assessment& Billing

Service	Functionality
01	**General** ▪ System should allow citizens to register their property on-line ▪ Assign the unique property ID based on the Process defined in the ULBs ▪ System should have interface with GIS system ▪ System should have facility to deliver the service online & through CFC/Kiosks ▪ Portal should have all the information including the processes and documents required for the convenience of citizen ▪ System should capture all the details required for application ▪ System should have the facility to apply online and through CFC or at ULB ▪ System should have facility to download required forms ▪ System should have facility for online payment and through CFC. ▪ System should have facility to send the alerts through SMS and email ▪ Capture description of property like mutation number, number of floors, area covered, land owner, co-owner, correspondence & permanent address, built year, Category of holdings (Residential, Commercial or industrial, Mixed Use, Government/Semi-Government, Education Institutions, Others), category of road, Mode of collection, Contact number, individual room measurements, etc. ▪ Facility to classify the property based on its type ▪ Allow changing the category of holding ▪ Provide tax calculator for users to calculate the property tax on a particular holding at any given rate and with multiple combinations of variables ▪ Capable of exporting data stored in the database to excel as and when required by the user. Similarly, provision of data import from excel to the system should be there. System should support templates for defining the import and export structure ▪ Calculation of rebate and Penalty to be shown as "others" and distinct from total Demand (TD) and Total Collection (TC). Within others, rebate, penalty, interest and adjustments to be clearly identified ▪ En Masse demand generation needs to be made possible. It should be done for total, circle, revenue circle and ward wise ▪ System should have a provision to tag property as suspect. Additional tags will be required for properties with incomplete data, and which have been marked as potentially incorrect size, as distinct from property does not exist ▪ Batch mode upload of data collections required ▪ Provision to provide incentives based on advance annual payment, as well as writing off or decrease of arrears based on payment to be provided ▪ A complete audit trail for all transactions, as well as master updates ▪ Provision for bar code on the demand

	▪ Capable of adding schemes for recovery of arrears ▪ Mail merge exports and imports ▪ Back up archival functionality ▪ Dashboard display of status ▪ Provision to make a qualitative and quantitative assessment of the tax paid and arriving at logical decisions that will help in decision making on which raids, inspections and imposition of penalties on the defaulters can be made possible ▪ System to keep history of payment defaults, penalties imposed, discounts given etc. related to each holding
02	**Filling of Property Tax Returns** ▪ Integration with the Self-Assessment software available with the Purchaser ▪ System should accept digital certificate of the citizens for filling online return ▪ System should generate acknowledgement receipt regarding filling of property tax
03	**Inclusion of New Assesse** ▪ Entering/ adding the applicant details for new assessment ▪ Entering / adding the details of SAF (Self-Assessment Form) for existing holding ▪ Generation of a new assessment application acknowledgment receipt ▪ Facility of modifying an existing record ▪ Generation of the special notice to the assesse indicating the amount of tax to be paid ▪ Entering of the revision petition application into the system ▪ Generation of the acknowledgement for the appeal petition application receive
04	**Assessment of Property** ▪ System should calculate applicable tax liabilities for properties for which returns have been filled. And, flag those properties which have discrepancies. ▪ System should allow ULB officials to do sample checks of the returned filed ▪ Calculation of Property Tax to be levied based on the building type, area, usage details etc. ▪ Facility of modifying an existing record ▪ Accommodate different tax rates depending on the 27-cell matrix structure ▪ Enter/add the assessment details and property tax levied ▪ Property tax demands should be generated for those properties for which returns have not been filled and also for those properties against which less tax have been paid in the return ▪ Frequency of generation of Demand should be flexible. It should be user defined (defined at admin level) and could be quarterly, half-yearly or annually ▪ Enter/add the Arrear details and property tax levied for assessment ▪ Generation of enter/ add the application details for exemption from property tax

	▪ Facility of entering/adding application details for write-off from property tax ▪ Facility of issuing an acknowledgement ▪ Facility for citizen to raise the objection (if any) after getting the demand notice ▪ System should have the facility to send SMS alert to citizen for payment & due date ▪ System should have the provision for online payment of property tax through portal & CFC ▪ System should have all the irregularities in tax payment predefined; to automatically detect any suppression of fact and details on the part of the citizens in paying the tax. MIS should be generated listing suspect cases and reasons citing irregularities ▪ System should have interface with to track the defaulters of house tax payment ▪ System should have inbuilt check and balances to enable the Enforcement authorities to track citizens evading tax payment ▪ System should have provision to make a qualitative and quantitative assessment of the tax paid and shall arrive at logical decisions that will help urban local bodies in decision making on which raids, inspections and imposition of penalties on the defaulters ▪ System should have the facility to analyze and forecast revenue trends based on tax collection ▪ For house tax assessment, the system should provide the complete flow of data of approval/rejection by Inspector, RO, EO, etc.
05	**Change of Ownership / Mutation** ▪ Facility of entering/ adding the application details for title transfer of property ▪ Facility of issuing an acknowledgement. ▪ System should ask for NOC from departments/sections before processing the service request ▪ System should follow the numbering of holding ▪ Facility of modifying/ deleting an existing record ▪ Facility of entering/ adding the field verification details for title transfer property ▪ Enter/add the approval details for title transfer property ▪ Enter/add the fee payment details for title transfer property ▪ Facility of generating the endorsement for the title transfer property after the property is transferred and the fees is paid
06	**Collection of Property Tax** ▪ Change property tax computations and determinearrears/refunds etc. ▪ Generation of the details of Property Tax paid for the assessment ▪ Generation of enter/ add the application details for exemption from property tax ▪ Enter/add the application details for vacancy remission from property tax ▪ Facility of entering/ adding the application details for write-off from property tax ▪ Facility of issuing an acknowledgement ▪ Integration with Accounting Module

07	**General Revision** ▪ Accepting requests for Revision. ▪ System should provide information related to general revision and documents required for the same ▪ Updation of the assessment database based on the field verification details. ▪ Entry of the property modification details ▪ Entry of the penalties details ▪ Capturing of the approval details
08	**Action Taken for Recovery of Taxes** ▪ Add/Edit details of action for distrait ▪ Flagging for legal cases filed, and information on these cases ▪ Flags for investigation based on grievance filed by the assessee ▪ Information on auction of property and recoveries
09	**Indicative List of Master** ▪ Details of Circle(Addition/Modification/Search) ▪ Details of Wards (Addition/Modification/Search) ▪ Details of Revenue Circles (Addition/Modification/Search) ▪ Details of Locations (Addition/Modification/Search) ▪ Details of Apartments/ Complexes (Addition/Modification/Search) ▪ Details of Use Factor (Addition/Modification/Search) ▪ Details of Tenancy Factor (Addition / Modification / Search) ▪ Details of Building Classification Type (Addition/Modification/Search) ▪ Details of Roof Type Master (Addition/Modification/Search) ▪ Details of Floor Types (Addition/Modification/Search) ▪ Details of Tax Rates along with validity (Addition/Modification/Search) ▪ Details of ARV matrix along with validity (Addition / Modification / Search) ▪ Details of Discount along with validity (Addition / Modification / Search) ▪ Details of Bill Collector Master Addition/Modification/Search) ▪ Exemption details master (Addition/Modification/Search) ▪ Occupier details (Addition/Modification/Search) ▪ Details of Bank Master (Addition/Modification/Search)
10	**MIS (Minimum)** **A**. Overview Report 1. Data Fields for the report are given below – 1.1. No. of holdings 1.2. Total arrears 1.3. Total demand 1.4. Total collections and 1.5. Total arrears: The report should be generated as Overall, by circle, by revenue circle, by ward, by collector. Collectionsneed to be shown against Arrears, current FYDemand and total. The figures for penalty and rebates are to be shown separately.

	B. Checklist for status of submission of SAF by theassesses **C**. List of Defaulters (Assesses who have not paid taxesalong with SAF by "particular day" every year) –Circle/ward/revenue circle/Locality-wise **D**. Field Verification Checklists **E**. Checklist for Holding Data **F**. Special Notices **G**. Collections: 1. Bill Collectors Collection 2. Counter Collection, Direct bank remittance, CFC wise collection 3. Mode of payment wise collections 4. Ward wise Collection 5. Revenue Circle wise Collection 6. Locality wise Collection 7. Penalty on Late Payment Collection 8. Penalty on Unauthorized Construction **H**. Registers 1. Arrears Register 2. Area Base Register 3. DCB Register 4. Defaulter register 5. Exemption Details Register 6. PT Register 7. Register of Appeals for the Year 8. Register of Distrait 9. Register of Warrants 10. Remittance/Daily Collection Register 11. Receipts/Payments Register of PT for the Year 12. PT Demand Register 13. Vacancy Remission Register 14. Write Off Register **I**. Certificates

1. Ownership Certificate

2. Valuation Certificate.

J. Other Notices

1. Final Notice

2. Warrant Notice.

K. Apartment Details, Complex Detail

L. Building Age wise Assessment List

M. Monthly List of Buildings Requiring Levy of PT or Revision of PT

N. Occupiers Other than Owners

O. DCB (Demand-Collection-Balance) Report –

1. Data Fields for the report are given below –

1.1. Opening Balance (arrears as at end of last period)

1.2. Current year demand

1.3. Collection

1.3.1. Collection against arrears

1.3.2. collection against current year Demand

1.4. Closing Balance as at end of period: The report should be generated as Overall/summary and also by Holding Category, Municipal Circle, Revenue circle, and Collector.

P. Ageing Report: Should report on total arrears as at end of any period in a classified category.

Categories	**Arrears (in INR)**	**No. of Holdings**	**Avg. Value per Holding**
Current Demand			
Demand between x year to y year			

Drill down of this MIS to be available at the property level. This report should be generated as summary report for whole ULB and also by each collector, ward and circle.

Q. ABC Analysis with data fields such as Holding ID, Name, Addresses, and Total Arrears. The report should be classified in different Value Bands. The report should be generated as summary report for ULB and also by collector, Ward, Circle, holding category (Purely Residential, Purely Commercial/Industrial and Others) , By type of Construction (Pacca, Asbestos, Others) and by category of Road (Principal, Main and Others)

R. Projections of Annual Demand with Revised 27-cell Matrix Rate structure :

1. Data Fields for the report are given below-

1.1. Total no. of Holdings

1.2. Current rate

1.3. Projected rate

1.4. Actual demand with current rate structure

1.5. Projected Amt.

1.6. Difference (Increase / Decrease)

The report should be generated as summary report for ULB and category wise sub-total for

type of use (Purely Residential, Purely Commercial/Industrial and Others), by type of Construction (Pacca, Asbestos, Others) and by category of Road (Principal, Main and Others).

S. Query

System should be capable of generating any information as and when needed by querying the database e.g.

- ABC Analysis, List of all default customers [amount range, location (ward/centre)]
- List of all flagged assesses where legal action is being taken and their status
- List of flagged customers where recovery action being taken under section 155 b to g
- List of all flagged assesses from whom payment by cheques are received and cheques dishonoured when presented
- Ward wise holding details as defined
- Ward wise demand details.
- Holding details as according to the criterion of valuation laid down under sub-section 4 of section 127 of the BMA, 2007
- Collection report based on mode of payments i.e. Cash, cheque, cards etc.
- Collection report based on channel of collection – collector, CFC, internet, online etc.
- Category wise list of all properties whose assessable area has changed (in percentage) as per user input
- Details of payments / commissions paid for collection

T. The system should able to generate Collector's Performance & Movement in the Holdings report with figures from previous year, current year, % change and having following data fields:

- Collector's Name
- No. of Holdings
- Total Demand (Current and Arrears)
- Total Collection (Against Current and Against Arrears)
- Efficiency of Collection (in %)
- No.Holdings Payment Received

	U. Trend Reports 1. Demand 2. Realization 3. Timely realization 4. Method of payment 5. Arrear recovery 6. No. of holdings 7. Collection channel 8. Collection of penalty and interest The report should be generated as summary report for ULB and also by collector, Ward, Circle, holding category (Residential, Commercial/Industrial and Others), By type of Construction (Pacca, Asbestos, Others) and by category of Road (Principal, Main and Others). **V**. Time Series Reports 1. Change in assessable area – 1.1. For a particular holding - original and revised area 1.2. Category-wise list of all the holdings whose assessable area has changed (in percentage or range of percentage) as per user input 2. Ownership change - for a particular holding with tenure **W**. Exception Reports 1. Difference between amount of tax return filled and actual tax liability calculated by the system based on the data available in the database 2. Status of Flagged/suspected holding - Overall, municipal circle wise, revenue circle wise, ward wise, and collector wise list of property which have marked as suspected along with the remarks and other details. 3. Incomplete data reports 4. Reports where data not received consistently 5. Reports for areas where data changed often 6. Property size and demand decrease reports 7. Report for occupancy details changed often

	X. Dashboard needs to offer various drill down and graphical report associated with property tax related data i.e. self-assessment, demand, collection, arrear etc.
PT 11	**Interface with Other System** ▪ Interface with workflow/document management system ▪ Interface to use digital signature certificate ▪ System should interface with Mailing & Messaging System and SMS application

5.6.10 Functional Requirement Specification– Engineering Department / Works Management

1	The system should have provision for Mapping of Administrative ward with Election ward
2	The system should have masters for Project type
3	The system should have masters for Work type
4	The system should have masters for Locations
5	The system should have masters for Project Status
6	The system should have masters for Scrutiny Process
7	The system should have masters for Items / Special Items (For Estimation)
8	The system should have masters for Rate type (SOR /Market Rates / DSR / ESR /WSR Rates / Special Item Rates)
9	The system should have masters for Milestone
10	The system should have provision for Rate & Rate Schedule Detail Updation
11	The system should have provision for Rate Analysis & Rate Estimation
12	The system should have provision for Selection of SOR / Market Rates / DSR / ESR / WSR / CSR Rates
13	The system should have provision for Updation of Project Progress / Measurement Book
14	The system should have provision for Estimate Preparation After Field Visit
15	The system should have provision for Data Entry of all components for Preparation of Estimates
16	The system should have provision for Estimate Review and Approval (On-line / Off-line)
17	The system should have provision for Updation of Project Progress / Recording of Measurement Book
18	The system should have provision for Verification of Project Progress / Measurement Book

19	The system should have provision for Updation of Site Inspection Details along with Photograph of work
20	The system should have provision for Review and Approval of Bills Raised by Vendor
21	The system should have provision for Payment to Vendor via all modes Cash / Cheque / DD/ PO etc.
22	The system should have provision for Capturing Receipt via all modes Cash / Cheque / DD/ PO etc.
23	The system should have provision for Billing for Extra / Excess Items
24	The system should have provision for managing Advance Payment to Vendor
25	The system should have provision for Abstract Sheet Generation
26	The system should have provision for Rate Analysis
27	The system should have provision for Recapitulation sheet Generation.
28	The system should have provision for recording details of Negotiation
29	The system should have provision for updating details of Tendering, Bid evaluation, and Agency fixation.
30	The system should have provision for DSR Maintenance
31	The system should have provision for Recapitulation of Electrical & Civil work
32	The system should have provision to manage Excess Quantity
33	The system should have provision to manage Extra Items
34	The system should have provision to generate Completion Certificate
35	The system should have provision for managing the Extension of Period
36	The system should have provision for Addition of Specifications not included in Standard DSR for Special Item
37	The system should have provision for Defining various Milestones / Time Limits & its updation along with reason of delay
38	The system should have provision for managing and updating the Project Scheduling
39	The system should have provision for sending Notice to Agency / Vendor (For delay , Poor Quality, any other reason)
40	The system should have provision for Calculating the penalty based on the pre-defined parameters
41	The system should have provision for Agency / Vendor Status updation (Black listed , Restricted for period)
42	The system should have provision for Project-wise comparison of Budgeted Expenditure Vs Actual
43	The system should have provision for updating information for (Bridges, Sewerage treatment plants, Roads etc.) along with annual maintenance details for the projects

44	The system should have provision for managing Quality Control (PMC / TPIA Report)
45	The system should have provision for generating Work Comparison report - Plan vs. Actual
46	The system should have provision for generating Payment Detail Report - Invoice raised, Payment made , Tax Deducted , Balance Payment, etc.
47	The system should have provision for Work order Printing
48	The system should have provision for generating Milestone Monitoring Report
49	The system should have provision for generating Project Summary Report
50	The system should be able to generate reports for the following; – Measurement Sheet – Rate Analysis Sheet – Abstract sheet – Recapitulation sheet – Tender Checklist – Tender Notice – Estimate sheet – No dues Certificate – MB Abstract Report – Extra Item Report – Contractor wise pending Bills – Ward wise pending Details – Project-wise comparison of Budgeted Expenditure vs. Actual – Contactors Register – Confidential Register of Contractors – Road register (Traffic / Road history / Defect liability) – PWD register (Works manual/ accounts manual/) – Bridges register (history / annual maintenance / Continuous monitoring) – Technical Bid Comparison – Financial Bid Comparison
51	The system should be integrated with Purchase and Store Department (Invoice Processing with respect to GRN)
52	The system should be integrated with e-Tender / e-procurement Module
53	The system should be integrated with Solid Waste Management System
54	The system should have provision for data entry suite for MB history data entry
55	The system should have provision for Upgradation of Contractors data (Black listing of Contractors)
56	The system should have provision for managing Support Parent / Child Relations for Project and Sub-Project

5.6.11 Functional Requirement Specification– Solid Waste Management

1	The system should have masters for location and should have provision to enter location details
2	The system should have provision to select the hierarchy of ULB in Administrative, Electoral, Revenue and Operational.
3	The system should have the facility to Import and Export location details
4	The system should have provision to display error messages and validation messages while importing the data
5	The system should provide facility to define population.
6	The system should be able to capture population at ward level.
7	The system should be able to define details of disposal site master which are falling within the municipality which might include dumping group and transport centers.
8	The system should capture location and address of disposal site
9	The system should capture size of disposal site in sq.kms./sq.mtrs.
10	The system should have facility to capture and display multiple waste type against each disposal site
11	The system should provide facility to define Vehicle details in vehicle master
12	The vehicle master should have facility to capture Vehicle Type, Vehicle Registration, Vehicle Capacity, Owned by, Vehicle Weight and Carriage Capacity.
13	Vehicle Master should have option to select Department Owned Vehicle or Rented Vehicle and accordingly the details should be captured.
14	The system should use vendor master developed in Accounts module as a common component
15	The system should be able to provide facility to capture Vendor details
16	The system should be able to provide unique vendor code for each vendor register within system
17	The system should be able to define route with route number
18	The system should able to define starting point and ending point of the route from location master
19	The system should have facility to enter KMs covered within the route from starting and ending points
20	The system should capture vehicle type which shall be used on that route
21	The system should capture nearest disposal site and distance from disposal site
22	The system should able to define refuelling pump station within the municipal area
23	The system should able to select the type of pump i.e. Government or Private along with its name, address and location
24	The system should able to capture type of items sold by the pump along with its unit

25	The system should be able to define vehicle maintenance as per the vehicle type
26	According vehicle type the system should be able to capture its maintenance due period and downtime period for estimation
27	The system should have the facility of contract agreement as a common component to be used wherever a contract is needed
28	The system should have a facility to create a Contract Agreement before assigning the work to a vendor.
29	The system should generate a contract with unique contract number.
30	The system should have the facility to search contract number.
31	Contract creation form should have provision to show the history of the contract created against a contractor/vendor.
32	Contract number should be auto generated on submission of contract.
33	The contract should be created in between two parties and each party should have the facility to add multiple witnesses.
34	The system should have the facility to capture and read Photo and Thump impression. Also, manual process of uploading is required.
35	The system should have provision to define various contract type; Such as contract against the lease, contract against services, contract against supplies etc.
36	The system should have provision to define contract term by providing contract from date and to date.
37	The system should able to create a commercial or non-commercial contract. In commercial contract the system should ask for contract amount payable or receivable, contract amount, security deposit and its details, payment terms in weekly, monthly or yearly or whatever values defined.
38	The system should also have provision for appreciation amount under commercial contract mode. If selected appreciation applicable, then the system should ask for appreciation type where the user should able to choose whether the appreciation should be a percentage or amount and user should able to enter the appreciation value in percentage or amount.
39	The system should have the option to select for allowing renewal.
40	On completion of contract tenure, the system should auto close the contract.
41	The system should have the facility to upload documents against the contract.
42	The system should have provision to enter terms & conditions.
43	After submitting the contract, the system should send the contract to higher authorization as per workflow defined.
44	The system should have facility to set vendor target.
45	The system should have facility to assign target for multiple contract of single vendor.
46	The system should have provision to define route for each service and volume of collection.

47	The system should have provision to track vendor wise, contract wise, date wise, vehicle type wise trip sheet
48	The system should have provision to capture target of vendor against which the collection is done
49	The system should provide trip number and date to each trip against each vendor and vehicle for the particular target period
50	The history of all the trips within the target period should be displayed with breakup of collection waste
51	The system should have provision to capture Time and Weight at the entry and exit
52	The system should have provision to enter the total garbage collected against that trip and have provision to break up the collection into various waste type
53	The system should have provision to enter multiple trips against each transaction number. The transaction number should be one for each day
54	The system should have facility to enter the details of inspection according to inspection type defined through prefix i.e. regular inspection or inspection against complaint
55	The system should capture inspector's details with name and designation
56	The system should have facility to capture inspection date and time
56	The system should have provision to capture inspection remarks
57	The system should have provision to levy penalty to vendor for not following the contract terms and condition
58	The system should have functionality to generate and print show cause notice and reminders
59	The system should have provision to send notification on Email and SMS to vendor
60	The system should have facility to hold the payments against schedule and should have provision to revoke it later in vendor payment with valid remark
61	The system should have provision for making the vendor payments. Vendor payment can be revoke with specifying valid remark.
62	Vendor payment should be integrated with the Accounts module so as to include the effect of same in Accounting entries
63	The system should have facility to set employee target according to name or designation
64	The system should have facility to assign target for multiple employee of against same route
65	The provision to set employee target should be on the basis of period and volume of collection
66	The system should have provision to set the target for multiple routes and multiple employees
67	The system should have provision to search, edit previous target and add new employee target
68	The system should have the capability to generate the following reports • Vendor Target

	• Vendor Trip Sheet • Day Wise Dumping • Ward Wise Collection of Garbage • Performance Register • Vehicle Schedule Execution • Employee Schedule Execution • Disposal Site Wise Collection • Vehicle Schedule Execution • Expenditure Incurred on Transportation

5.6.12 Functional Requirement Specification– Birth & Death Certificate

Sl. No.	Requirement Description
1	Hospital Master
	• System should have facility for Addition, Modification, Deletion, and Search of Hospital Data. • System should be able to print list of hospital. • Hospital Master should get automatically updated after the hospital registration.
2	Service Charges Master
	• System should have facility to define fees for Birth & Death registration as defined in process. • System should have facility to define charges as per Slab (data range) /flat/year / lump sum basis.
3	Details of Registrar
	• System should have facility to maintain the details of Registrar. • System should have facility to define designation of the employee. • System should allow role wise authorisation to user.
4	Authorization of Birth / Death Registration / Correction
	• System should have facility at designated level to check the registration details entered in the system to avoid typographic mistakes as well as mal-practice before generating registration number. • The use of the facility should be at the discretion of ULB. • System should provide functionality to authorize/ Reject / on Hold Birth & Death registration. • System should have facility to request for Birth Certificate by the empaneled Hospitals. • System should have facility to generate online certificates by empaneled hospitals. Empaneled hospital can issue the birth certificate to citizens but

	nursing homes cannot issue directly. For nursing homes approval of registrar is required. • System should authorize registered nursing homes to enter details of the new born but should not allow the issue of birth certificate. • System should allow citizen to apply online for birth certificate in case delivery taken place at home. • System should have facility to pay fees online. • System should have facility to update citizen about the status of their application through SMS/ Email alerts. • System should have facility of multilevel approval system. Should be configurable. • System should have facility to upload important documents like Adhaar card, photo Ids etc. • System should allow edit of parent names in case of adopted child. • System should allow edit of details to authorize user in case data entered is wrong.
5	Birth and Death Data Upload
	• System should have facility to upload Birth and Death registration data available in soft format through data upload facility.
6	Birth registration correction with certificate
	• System should allow the Birth registration correction through ULB counter / Online through web portal. • System should have the facility to capture Applicant details from the user profile in case of Citizen Login ID, Otherwise application form should have the facility to capture the applicant details in case on CFC/ ULB counter. • System should have facility to upload service related required document online. • System should have facility for Govt. official to add/modify/delete the Birth and Death details by based on the approval/right as per process.
7	Death registration correction with Certificate
	• System should allow the Death registration correction through ULB counters / Online through web portal. • System should have the facility to capture Applicant details from the user profile in case of Citizen Login ID, Otherwise application form should have the facility to capture the applicant details in case on ULB counter. • System should have facility to upload service related required document online. • System should have facility for Govt. official to add/modify/delete the Birth and Death details based on the rights assigned as per process.

	• System should have facility for online payment as well as through ULB counters for this service. • System should have facility to collect charges through online payment. • System should have facility to collect payments in offline mode • System should have the provision for Registrar to approve or reject the request • System should have facility to resubmit the required doc or to correct the application details in case of rejection / on hold status through citizen log in. • System should have facility to send email and SMS alerts to the applicant about the status of the process. • System should have facility to track online application with Unique ID. • System should have facility to make online/offline payments for the issuance of new Birth/Death certificates
8	Non Availability certificate
	Cremation Certificate
9	Statutory Reports
	• System should generate the critical statutory reports related to Birth and Death based on record maintained in database for same.
10	Birth by Level of Education of Father and Birth Order
	• System should have facility to generate report on the basis of Birth by level of education of father and birth order. • System should have facility to generate reports on Father's Literacy wise in a particular year
11	Birth by Level of Occupation of Father
	• System should have facility to generate report on the basis of Birth by level of Occupation of father. • System should have facility to generate report on Father's Occupation wise in a particular year.
12	Birth by Level of Education of Mother
	• System should have facility to generate report on the basis of Birth by level of education of mother. • System should have facility to generate reports on Mother's Literacy wise in a particular year.
13	Birth by Level of Occupation of Mother
	• System should have facility to generate report on the basis of Birth by level of Occupation of mother.

	• System should have facility to generate reports on mother's Occupation wise in a particular year.
14	Hospital wise Birth Details
	• System should have facility to generate Hospital wise Birth details report.
15	Sex and Month of Occurrence
	• System should have facility to generate Sex and Month of occurrence Birth details report.
16	Other MIS/Ad-hoc reports
	• System should have facility to generate Other MIS/Ad-hoc report as desired
17	Monthly Summary Reports of Births
	• System should have facility to generate Monthly Summary Reports of Births as per captured data.
18	Summary of Birth wise Sex Ratio
	• System should have facility to generate reports for Summary of Birth wise Sex Ratio as per data captured.
19	Death Related Statutory Reports
	• System should have facility to generate different Death related statutory reports.
20	Child Mortality Report
	• System should have facility to generate reports for Child Mortality Report as per data capture in the system.
21	Sex and Month of Occurrence
	• System should have facility to generate reports for Death as per sex and month of occurrence.
22	Birth and Death Application Status
	• System should have facility to generate report for Birth and Death Application Status.
23	Native Mobile Apps (Android/ I-Phone/ Windows)
24	Portal should be multilingual (English & Hindi)

5.6.13 Functional Requirement Specification– Store Management

1	System should have facility for Addition, Modification, Deletion, and Search of **Item Group** Details.
2	System should have facility for Addition, Modification, Deletion, and Search of **Unit of Measurement** Details.
3	System should have facility for Addition, Modification, Deletion, and Search of Item Details.
4	System should have facility to classify item based on type, capital equipment and cost above (Defined Range).
5	System should have facility to Manage the Item using method (FIFO/LIFO/Not Stated)
6	System should have facility to Manage the Stock Level (Minimum, Maximum & Reorder Level)
7	System should have facility for Addition, Modification, Deletion, and Search of Vender Details.
8	System should have facility for Addition, Modification, Deletion, and Search of Bin Details.
9	System should have facility for Addition, Modification, Deletion, and Search Store Master.
10	System should have facility for Addition, Modification, Deletion, and Search of Location.
11	System should have facility to search the Item by Item Code & Name.
12	System should provide facility to display the Available Item Stock & Print the Stock Details.
13	System should provide facility to search item with store details.
14	System should have the facility to print all the available lists.
15	System should have facility to add/modify /Search / Cancel the Indent.
16	System should have facility for Raise the Indent from various Departments.
17	System should provide facility to raise request for multiple items in one Indent.
18	System should generate & Print Indent Copy.
19	The system should capture the following details and store in the system: o Indent Details, o Indent Raised Department Employee Details, o Item Details and
20	System should not allow deleting the Indent.
21	System should provide the list of indent received date wise
22	System should allow stores person to issue material as per intent received.
23	System should ensure that while issuance of material FIFO must be adhered to

24	System should have facility to flag a particular item from indent and issue other items as per request if that particular Item of indent not available.
25	System should provide facility to request particular item from other stores, if same is available at another Store.
26	System should provide facility to grant the request or reject. • If request rejected then system should intimate to requester via system, mail or SMS. • If request is consider then system should allow transferring stock from one store to another via process of material transfer.
27	System should provide facility to capture all materials received at stores. • Unique number must be generated for Good Received Note Inspection • System should provide facility to capture item wise Inspection details • If rejected then rejection reason and quantity of same.
28	System should provide facility to return rejected Goods to vendor, for Rejected Quantities.
29	System should provide facility to generate Invoice for accepted goods and should intimate same to accounts for release of payment.
30	System should have facility to add/modify /Search /Cancel the Issue / Dispatch Note, as well as capture and store the following details in the system: • Issue/Dispatch Details, • Indent Raised Department Employee Details, • Item Details and • Cost Centre Details
31	System should have facility to add/modify /Search /Cancel the Transfer Voucher, as well as capture and store the following details in the system: • Transfer Voucher Details, • Transfer Voucher Raised Department Employee Details, • Item Details • From Store Details • To Store
32	System should have facility to add/modify /Search /Cancel the Disposal of Dead Stock (Scrap Material), as well as capture and store the following details in the system: • Disposal Note Details, • Disposal Note Raised Department & Employee Details, • Item Details • From Store Details
33	System should Manage the material using first in first out method
34	System should not allow deleting the Issue /Dispatch Note, Transfer Voucher, Disposal Note.
35	System should have facility to generate Item Details Report.
36	System should have facility to generate Material Consumption Report. • Material-wise • Department-wise
37	System should have facility to generate Disposal Note Report.

38	System should have facility to generate Material Inspection Detail Report.
39	System should have facility to generate the Un-used material report.
40	System should have facility to generate the Goods rejection / Return Detail report.
41	System should have facility to enter Item wise Opening Balance and their location of storage (bin).
42	System should have facility to pop up Message for Team Minimum Level, Reorder Level
43	System should have facility pop up Reminder to User in case of delay in Item delivery from Vender
44	System must have Facility of upload the Item Master.
45	System should have Integration and Interface with workflow / document management system.
46	System should have provision for integration with Procurement Module. Purchase order needs to link with Good receipt and subsequently with Accounts module.
47	System should have interface with Mailing & Messaging System along with SMS application.
48	System should have facility to show the item wise stock and their valuation.

5.6.14 Functional Requirement Specification- File Management System

1	The system should have provision for Scanning & Marking the inward to the respective department
3	The system should have provision for Incorporation of separate hierarchy for RTI letter movements & Commissioner Office
4	The system should have provision for Capturing of Fresh applications & Appeals
5	The system should have provision for Tracking of the Inward and outward correspondence
6	The system should have provision for File Closure to be carried out as per the final decision of respective authorities
FM 7	DAK and File Management system should build using robust Document Management and Workflow Management and should comply with the Manual of Office Procedure

5.6.15 Functional Requirement Specification- Asset Management System

1	System should have the provision to select the required Asset Type Name (such as Movable or Immovable) from the drop- down list.
2	System should have provision to define the required Classifications in the Asset Classification section for each Asset Type Name.
3	System should have provision to enter or remove the Classification records by using the Add or Delete buttons respectively.

4	System should have provision to update the Asset Classification records from the Active list whenever needed.
5	System should have the provision to define the Location Code and the corresponding Location Name.
6	System should have the facility to not allow the duplicate record of having the same Location Code and Location Name.
7	System should have the provision to define the Department Code and the corresponding Department Name.
8	The system should have the facility to not allow the duplicate record of having the same Department Code and Department Name.
9	System should have the provision to enter the required Group Code in the specific format and define the required Group Name
10	System should have the provision for the Transaction Type to select the required Type (i.e., Debit or Credit) from the drop-down list.
11	System should have the provision for each Process Type to have one Debit and Credit Transaction types.
12	The System should have the facility to define the Value Type for the selection of each record based on the respective Process Name.
13	Asset Registration section should have the provision to enter the values for in the following fields such as Asset Id, Asset Name, and Serial Number and Description..
14	System should have the provision to select the required Asset Type and Classification Name from the respective drop-down fields.
15	The System should have the facility to select the source of the Asset (i.e., either Direct Fixed Asset or Integrated from Stores).
16	The system should have the facility to mention to whom the Asset has been assigned in order to track the Ownership of it.
17	The system should have the facility to capitalize the Asset during the Asset Registration and the Asset Registration Date should be lesser than the Asset Capitalization Date.
18	System should have the facility to map the asset's Latitude and Longitude Coordinates through GIS integration or as an entry values.
19	The System should have the facility to maintain the Opening Balance for of the Asset received from the legacy system.
20	The System should have the facility to auto- populate the Asset Life in Years based on the inputs of Asset Life Start and End Dates.
21	The System should have the provision to select the required Schedule Type for the registering Asset.
22	System should have the facility to get the Appreciation Percentage based on which the Schedule count to be auto- populated.
23	System should have the facility to get the Depreciation Percentage based on which the Schedule count, Salvage Value to be auto- populated.
24	The System should have the facility to define whether the Asset is Sellable or Not.
25	The System should have the provision to enter the Procurement Details of the Asset such as Purchase Date, Vendor Name and Procured Value etc., if that Asset has been procured from Stores.

26	The System should have the provision to auto- populate the improvement details done on the Asset through the integration from Works module.
27	The System should have the facility to provide the Construction Details of the Asset such as Construction Start Date, Completed Date, Constructed Value etc., if that Asset belongs to the Classification of Building.
28	System should have the provision to enter the Insurance Details of the Asset such as Insurance No, Service Provider and Insured Amount etc.
29	System should have the provision to add or attach the details of any Legal Documents including information such as Document Name, Document Number, Document, Details etc., for the Asset.
30	The System should have the provision to select the required Asset Type, Classification, Schedule Period and the Financial Year for which the Appreciation/Depreciation Schedule to be generated.
31	The System should have the provision to post the Schedule information for Appreciation/Depreciation into General Ledger with appropriate approvals.
32	The system should have provision to manage the process of Asset Revaluation and record reason.
33	The system should have the provision to record the General Ledger posting details once the Asset has been revaluated.
34	The system should have provision to manage the process of Asset Retirement.
35	The system should have the provision to record the General Ledger posting details of the Asset Retirement.
36	The system should have provision to manage the process of Asset Sale and record posting in General Ledger.
37	System should have the capability to generate required MIS Reports as finalized

5.6.16 Functional Requirement Specification- Workflow Management System

1	Movement of Proposals on various parameters
2	Facility to mark the application to pre-defined hierarchy
3	Inbox for officers (listing applications received)
4	FIFO principle for taking action on application
5	Creation of a Note Sheet for Scanned Documents
6	Alerts for delay in action
7	Compliance to workflow standards: BPMN, BPEL and WFMC
8	Shall support Inbuilt Graphical workflow designer for modelling complex Business Processes using drag and drop facilities
9	Information/Alert to be sent to higher authority in case of delay in action by specific employee of the department

10	Pre-defined scrutiny for citizen applications
11	Display of all application data during scrutiny process
12	Check-list for rejection
13	Should have inbuilt Rule Engine for defining rules
14	Facility to mark the application to other officer
15	Facility to mark the application to other department for their NOC / Comments / Input
16	Final Decision by the Decision Authority
17	Shall provide graphical and tabular tools to create reports and view progress of each individual process

5.6.17 Functional Requirement Specification– Online Grievance Compliant Services

Sl. No.	Requirement Description
1	**Departments**
	• The department master should be used as a common component to define a department across the organisation. • The system should be able to create the department through department master. • The department master should have the facility to define department code, short code and make the department active/inactive. • The system should check active transaction before marking inactive; if the active transaction is pending the system should not allow the user to inactive.
2	**Complaint Categories**
	• The system should be able to define complaint types against each department. • Department created under department master should be linked with the complaint type master. • The complaint type master should have the facility to add multiple complaint types against each department. • Department user should have the facility to add, delete and edit the complaint types as a when required. • Department user should have the facility to make the complaint type active or inactive. • For inactivation and deletion, validation should be checked if the complaint type of said department is not having in progress complaint/application.
3	**Workflow**
	• The workflow master should be used as a common component to define workflow for scrutiny based services as well as care services.

	• The workflow master should have provision to define workflow as per Organization, Department, Services and Location, Role/Employee, Event and Application No. • For **Is Complaint** the services should be fetched from the complaint type. • Mapping of workflow should be multiple and as per event, organization, department and role/employee. • The workflow could be crossed organizational or cross departmental therefore, workflow master should have provision to select each event as per organization or department. • There should be provision to configure auto escalation at service level or complaint type level. If auto escalation is true then, the service should be followed as per SLA define and SLA should be mandatory in this case. If it's false then, the SLA should not be mandatory. • The Role/Employee Name should have Role and Employee Name values in selection. - When selected Role then, the value in Select Details column should show Roles from Entitlement Master. - If selected Employee then, the value in Select Details column should show Employee Name from Employee master. • Each event should have provision to select multiple roles or employees in select details column. • Mapping should have functionality to define SLA for each role/employee with user define units. • For each role type, the workflow should have a facility to assign URL which need to recall for the task to be done. • The workflow should be flexible enough to incorporate or remove events and role/employee against the service whenever there is a change in the workflow of service.
4	**Holiday Master**
	• The flow of complaint and escalation depends on working days. • The system should be informed about non-working days to ignore the same while auto escalation of complaints and while generating an acknowledgement. • This Master is used to define bank holidays or any other holidays declared by the ULB. • The system should provide Add, Edit, Delete and View facility. • The system should have import facility to export the holiday as per the calendar year wise. • The user should click on the respective date on which holiday is to be declared. On Clicking following pop-up should be displayed by the system. • This form enables the user to add Holidays. • User should edit the entered Holiday description and click on "Save Changes" button

	• This form enables the user to edit the assigned Holiday description. • To view the list of the defined Holidays, the system should provide "View Holiday List" button.
5	**Locations**
	• The system should have provision to enter location name and should accept alphanumeric characters. • This location name should be used in application form of services wherever required. Applicant/Citizen does not need to select Zone, Ward as he/she is not aware of the administrative hierarchy. • Location name should concatenate with area name. At centralise level city should be appended. • Through the concatenate functionality user can search exact location. • Location name in application form should have provision to search as per "display as you type result". • The system should accept unique Area name. There can be multiple locations of the same name but the area name should be unique for those locations. • Each location should have the facility to add GIS No. which should use for GIS integration. • The system should be capable enough to adjust five level of Ward, Zone hierarchy. • The system should have provision to select the hierarchy of ULB in Administrative, Electoral, Revenue and Operational. • The administrative location should have provision to identify department location. • When the user selects operational hierarchy then the system should ask to select the department name. • The system should have the facility to Import and Export location name. • In export, the system should export all the records available in the system or a blank file with the structure of a table in case no records are present. • In import, the system should import through the export file. The system should check the table structure before importing. • While import, the system should insert/append new records only. • For any change or update, the user should use EDIT option. • The system should have provision to display error messages and validation messages while importing the data.
6	**SMS and Email configuration**
	• The system should have the facility to configure events for SMS and Email. • The system should have the facility to send SMS and Email to all the services and departmental events. • The system should have the facility to send the SMS and Email as per user login language selection. • The system should be able to maintain sent history of SMS and Email.
7	**Complaint Registration Online**

	• The system should be able to accept application through online. • The system should have the facility to accept application in Regional Language. • The system should have the facility to lodge a complaint by selecting the desired department, and complaint type. • Applicant should be able to upload the necessary document at the time of application via Web Portal. • The system should have the facility to upload document up to the size of 5MB maximum. • The system should have the facility to upload a document in a various format such as PDF, DOCX, JPEG. • The system should have the facility to upload multiple documents. • The system should able to capture location coordinates via GIS for allocating Complaint Location from the map. • The system should provide facility to upload Photograph. • Token Number should be auto generated by the system once all the required details in the mandatory fields are entered and submitted. • After successful submission of application, Applicant should be intimated via SMS and email with the details of complaints and token number. • The system should have the facility to generate Acknowledgment Receipt for Applicant reference if the application is accepted through Online.
8	**Complaint Registration Department**
	• The system should be able to accept application Citizen Facilitation Centre/ULB Counter and Department. • The system should have the facility to accept application in Regional Language. • The system should have the facility to lodge a complaint by selecting the desired department, and complaint type. • Applicant should be able to upload the necessary document at the time of application via Web Portal. • The system should have the facility to upload document up to the size of 5MB maximum. • The system should have the facility to upload a document in a various format such as PDF, DOCX, JPEG. • The system should have the facility to upload multiple documents. • The system should able to capture location coordinates via GIS for allocating Complaint Location from the map. • The system should provide facility to upload Photograph. • Token Number should be auto generated by the system once all the required details in the mandatory fields are entered and submitted. • After successful submission of application, Applicant should be intimated via SMS and email with the details of complaints and token number.

	• The system should have the facility to generate Acknowledgment Receipt for Applicant reference if the application is accepted offline.
9	**Reopen Complaint**
	• The system should have the facility to open the previous complaint. • By providing old/previous complaint number/token number the user should able to search the complaint number. • The only closed complaint should be eligible to reopen. • By choosing Reopen option the user should able to write new complaint description. • The system should have the facility to upload document against the complaint. • The reopen complaint workflow should be reset from the initial level.
10	**Acknowledgment**
	• The system should auto generate Acknowledgment after successful submission of the application. • Acknowledgement should be generated for online and offline complaint registration. • The Acknowledgment should have details such as Token Number, Applicant Name, Service Type, Complaint Subtype, Location, Complaint Description, Escalation Charter etc. • The sample format of Acknowledgment is shown below.
11	**Complaint Status**
	• System should allow knowing the status of the Complaint registered by the applicant • The system should accept "Token Number" which is generated after submission of the complaint application and display the Complaint status to the applicant. • Complaint Status Path • If Applicant wishes to know the status via SMS, then the system should intimate the Status via SMS to the applicant.
12	**Complaint Feedback**
	• The system should allow the applicant to provide feedback on the Complaint Action for **Resolved and Closed**.
13	**Complaint Resolution**
	• On successful submission of application, the application should be displayed in the selected department's designated officer login for further processing. • The system shall send an SMS to ULB official to whom the complaint is assigned. • Designated officer should take necessary action on the registered complaint by the applicant. • Intimation should be sent to the applicant via SMS and Email of complaint resolution.

	• If designated officer does not take any action in given stipulated time frame as defined in the workflow, then system should auto escalate the complaint to the higher authority to take further action and intimation should be sent to designated officer for the same. The Auto-escalation should be parametric • In case the complaint has already been escalated, the system shall have facility to calculate the days of escalation accordingly • The designated officer should enter the necessary remarks and upload the supporting documents if required and resolve the complaint. • In case of Manual Escalation, the designated officer should manually forward the application to the higher Authority • If the complaint is not of concern department, then designated authority can forward the complaint to the concerned department by selecting Department from the drop-down list. While forwarding to concern department same copy should be sent to Head of the department by the system. • If the employee to whom the complaint is assigned got Retired/Transferred/Resigned, then this should be handled through the workflow. • For each action selected by the designated officer from "Action on Application", SMS and Email should be sent to respective Authority/Employee/Officer and to applicant by the system
14	**Action on Application: Resolved and Closed**
	• The system should have the option to choose an action as "Resolved and Closed". • When selected the option then, the system should ask for the remark as mandatory. • The system should also have the option to upload a document. • When the department user submits the action then it should be intimated to citizen/applicant via SMS/Email along with the status and remark.
15	**Action on Application: Hold**
	• The system should have the option to choose an action as "Hold". • When selected the option then, the system should ask for the remark as mandatory. • The system should also have the option to upload a document. • When the department user submits the action then it should be intimated to citizen/applicant via SMS/Email along with the status and remark. • On hold the task should be reassign to applicant/citizen to update the discrepancy reported by department user.
16	**Action on Application: Rejected**
	• The system should have the option to choose an action as "Rejected". • When selected the option then, the system should ask for the remark as mandatory. • The system should also have the option to upload a document.

	• When the department user submits the action then it should be intimated to citizen/applicant via SMS/Email along with the status and remark.
17	**Action on Application: Forward to Relevant Department**
	• The system should have the option to choose an action as "Forward to Relevant Department". • When selected the option then, the system should ask department name and Ward, Zone hierarchy as per departmental configuration • The system should also have the option to upload a document. • When the department user submits the action then it should be intimated to citizen/applicant via SMS/Email along with the status and remark.
18	**Action on Application: Forward to Employee within Department**
	a. Location: • The system should have the option to choose an action as "Forward to Employee within Department". • When selected the option then, the system should ask to choose one option from Location and Employee within Department. • If chosen Location then the system should ask Ward, Zone hierarchy as per departmental configuration for the same department against which the complaint is logged. • The system should also have the option to upload a document. • When the department user submits the action then it should be intimated to citizen/applicant via SMS/Email along with the status and remark. **b. An employee within Department:** • The system should have the option to choose an action as "Forward to Employee within Department". • When selected the option then, the system should ask to choose one option from Location and Employee within Department. • If chosen Employee within Department, then the system should ask to select Employee name for the same department against which the complaint is logged. • The selection option should only show the employees within same department and hierarchy. • The system should also have the option to upload a document. o When the department user submits the action then it should be intimated to citizen/applicant via SMS/Email along with the status and remark.
19	**Auto Forwarding**
	• The system should have facility to set auto forwarding option in case the department user is on leave. • The user should able to enter the period "From Date" and "To Date" he/she is on leave. • The user should able to select the employee name to whom the task should be forwarded in his/her absence.

	• The system should auto forward the task to select employee for assign period automatically. • The system should also maintain the tracker of all the forwarded complaints.
20	**MIS Dashboard**
	MIS (Management Information System) reports show graphical form, Complaint Redressal Performance data. The system should display the MIS Reports on Complaint and Redressal Management System dashboard. Dashboard should display the Registered Complaints, Resolved Complaints, Pending Complaints, Rejected Complaints, on hold Complaints details. All data should be auto-refreshed on each transaction and displayed on the dashboard by the system. • The dashboard should also consist of following links. 1. Feedback Rating 2. Trend Analysis 3. Social Analysis
21	**Feedback Rating**
	• Feedback Ratings should display the percentage of feedback from the Citizen and total Count of feedback. • The feedback rating data should be fetched from Complaint Feedback database by the system.
22	**Customer Satisfaction**
	• The system should fetch the customer satisfaction data from the Complaint feedback provided by the Citizen. • The system should display Excellent Percentage by default. • If the user desires to see rest of the review percentage, then the system should provide "Rating" dropdown so that user can select the rating from the drop down list and generate a report. • The system should display the report of the selected rating by the user.
23	**Total Feedback counts**
	• Total feedback section system should display out of total resolved complaints how many applicants gave feedback on the resolution. • The system should show a total number of feedbacks as well as the percentage of total feedback.
24	**Pendency Pie Chart**
	• The system should display how many complaints are pending to be resolved in time and out time in Pie chart format
25	**Pendency distribution Pie Chart**
	• System should show the pendency distribution of the complaints within specified time spam in the form of Pie chart
26	**Trend Analysis**
	• The system should display Ward wise, Zone wise graphical report.

	• System should provide facility to select following options so that user can generate Report as desired 1. 1 Week 2. 1 Month 3. 3 Month 4. 6 Month 5. 1 Year 6. 2 Year 7. 5 Year 8. Max 9. From Date and To Date
27	**Ward & Zone Wise Complaint Report**
	• Systems should display Ward Wise & Zone Wise percentage of Resolved and Pending Complaints out of Total in the graphical format.
28	**Social Analysis**
	• The system should display the count of resolved and pending complaints that are logged via SMS, Email, The Web and CFC/Department. • The system should have integration with SMS and Email Gateway.
29	**Telephone**
	• Systems should display the Total number of Complaints that are logged via Telephone. • Out of the total Complaints logged via Telephone, the system should display the count of Pending and Resolved Complaints.
30	**SMS**
	• Systems should display the Total number of Complaints that are logged via SMS. • Out of the total Complaints logged via SMS, the system should display the count of Pending and Resolved Complaints.
31	**Email**
	• Systems should display the Total number of Complaints that are logged via Email. • Out of Total Complaints logged via Email, the system should display the count of Pending and Resolved complaints.
32	**Web**
	• Systems should display the Total number of Complaints that are logged via The Web. • Out of Total Complaints logged via The Web, the system should display the count of Pending and Resolved complaints.
33	**Citizen Facilitation Center**
	• Systems should display the Total number of Complaints that are logged through CFC/Department • Out of Total Complaints logged via CFC/Department, system should display the count of Pending and Resolved complaints

34	**Reports**
	• Each report should be previewed before printing or generating. • The report should have the facility to generate in PDF and XLS/XLSX format. • The report should have the facility to align the size of the report as per the data. • Report size should be flexible and not fix to default page size. • The system should be able to generate multiple reports at the type. • The report should be flexible and can easily adjust to the pre-printed format.
35	**Complaint Register**
	• The Complaint Register should have filter criteria as From Date to Date, Complaint Status, Ward and Zone. • The Report should display data per the search criteria selected by the user.
36	**Complaint Report (Department wise)**
	• This Report should have filters From Date to Date, Department, Ward and Zone. • System should allow generating report Department wise for the selected ward and zone
37	**Complaint Report (Service type wise)**
	• This Report should have filters From Date to Date, Department, service type, Ward and Zone • System should be able to generate report service type wise for the selected department, ward and zone
38	**Complaint Report (Complaint subtype wise)**
	• This Report should have filters From Date to Date, Department, service type, Ward and Zone • System should be able to generate report complaint subtype wise for the selected department, service type, ward and zone
39	**Complaint Report (Within SLA/Beyond SLA)**
	• This Report should have filters From Date to Date, Department, Ward, Zone and Status • The system should display the complaints that are resolved within SLA and Beyond SLA.
40	**Complaint Feedback Report**
	• This Report should have filters From Date and To Date • The system should display the feedback report based on the selected Date range.
41	**Complaint Summary Report (Registration Mode Wise)**
	• This Report should have Filtered from Date and To Date and Registration Mode. • The system should display summary report per the Registration Mode selected by the user.
42	**Complaint Log Report (Ward/Zone/Dept./Service Type/ subtype)**

	• This Report should have filtered from Date and To Date and Radio buttons – Ward, Zone, Department, Service Type and Complaint Subtype. • The system should display log report per the selection made by the user within specified date range.

5.6.18 Functional Requirement Specification– Online Building Plan Approval System

Sl. No.	Requirement Description
1	**General**
	• System should have facility to categorizethe building plan under Cinemas,Multiplexes, Marriage Halls, Commercialcomplex, Housing and Hospital, etc. • System should have facility to deliver theservice online & through CFC. • The portal should have all the information including the processes and documentsrequired for the convenience of citizen. • System should capture all the detailsrequired for application. • System should have the facility to applyonline and through CFC. • System should have facility to downloadrequired forms. • System should have facility for onlinepayment and through CFC. • System should have facility to send thealerts through SMS and email. • System should track delays in approval steps and maintain an audit log of the approval process steps. • Interface with Mailing & Messaging System andSMSapplication • Integration withPaymentgateway • Integrationwith othermodules
2	**Empanelment of Architects**
	• System should have facility to capture theempanelment process for the Architects. • System should maintain the records ofempaneled architects for all the ULBs. • System should have facility to import thelist of empanelled architects • System should allow Architects to makepayment online for empanelment • System should allow de-listing of any of theempanelled Architects from the list • System should capture actions takenagainst any Architects for any violation
3	**Sanction ofBuildingPlan**
	• System should have facility for uploading the soft copy of the building plan alongwith the application. • System should allow uploading other necessary document along with theapplication. • System should allow municipal officials and empanelled architects to access/downloadthe same for verification of particulars.

	• Owner of the land /Applicant will upload the building plan as per Building bye-laws with other supporting documents • ULB will verify the documents and drawing and may give their comments within 15days • Owner / Applicant may have to upload the revised drawing after incorporating thecomments given by the ULBs • If there is no comment from the ULBs within 15 days of submission of comments, software will automatically generate a challan for the owner of the land to pay theprescribed fee • Owner / Applicant will make the paymentof the prescribed fee online/offline • Empanelled certified Architect will approvethe plan with their digital signature • Based on these an acknowledgement should be generatedand given to the applicant. • System should generate application reference for Building Plan Application/ Layout Application for the applicant and facilitate online tracking of the status of theapplication. • System should sent e-mail/SMS notification to the applicant and empanelled architectsto whom that application has been sent • System should allow empanelled architects to ask for additionaldocuments/information from the applicant. • System should allow architects to approve/reject plans and give commentson the same • System should have provision to generate digitally signed notice and communicatethe same through SMS/Email. • System should generateunique ID for each approved building plan. • System should link Holding Tax and Utilitydata with Building plan ID. • System should have facilities for Online Feecalculation • The detailed workflow of approval of the plan needs to be mapped in the documentmanagement system. • Online help should be available to the user for each system function. Topics covered inthe user manual shall also be availablethrough the online help.
4	**Issuance ofCompletionCertificate**
	• System should allow the owner of the property to upload the progress of construction (photographs of the property)at pre-defined stages. • In case of violation of the above, system should send alerts (SMS / e-Mail) to theconcerned ULBs. • System should have provision for designated officer to lodge the details of the site visit. Following which the documents needs to be approved by thedocument management system • System should have provision to generate digitally signed notice and communicatethe same through SMS/Email.

	• System should have integration with property tax module to update the detailsof the property after issuance ofcompletion certificate.
5	**Approval ofModification andAdditionalConstruction**
	• System should allow the designated officerto enter the field visit details. • System should be able to generate notice to the concerned property owner. The same should be communicated throughemail and SMS. • System should have the facility to applyonline or through CFC for compromise. • System should be able to generate composition fee assessment report as perthe details entered. • In case of no compromise; the systemshould have the facility to update theaction taken.
6	**Registrationof Builders**
	• System should allow registration of builders under various categories defined by theULBs. • System should allow builders/promoters toprovide details about the sale of the flats/plots etc. • System should allow tracking ofsales/transfers of flats / plots etc.
7	**MIS Reports**
	• System should generate list of empanelled architects and no. & details of building plans approved / rejected by any particulararchitects. • System should be able to generate a full range of reports relating to sanction of building plan, change of ownership, Issuance of completion certificates,violations, Lat-Longs, etc. • System should able to generate the any other fixed format and Ad-hoc reports asdesired. • Dashboard needs to offer drill down andgraphical report regarding plansapproval,rejection, Architects etc.

5.6.19 Functional Requirement Specification– Water Supply & Sewerage Connections

Sl. No.	Requirement Description
1	Manage licensed plumber
	Adding/editing licensed plumber list associated with MC.
2	New Water & Sewerage Connection (Residential, Commercial)
	• Procedure/Workflow approvals to set up water and sewerage connection • Regular Water Connection (Up to 15mm ferrule size) • Regular Water Connection (20mm to 40mm ferrule size) • Regular Water Connection (Above 40mm ferrule size) • New sewerage connection without road cut permission • New sewerage connection with road cut permission

3	New shallow water tube well connection for non-potable purpose
4	Temporary Water & Sewerage Connection
	Setting up of bill criteria for under construction/temporary connection
5	Tertiary Treated Water Connection
6	Transfer of Water & Sewerage Connection
	▪ Conversion from Commercial Water Tariff to Domestic Water Tariff ▪ Change of name for water connection
7	Temporary and Permanent Closing of Water & Sewerage Connection
8	System should have facility to define / view / update Meter Readings as per the user role.System should have facility to view the meter reading to citizen.
9	System should have facility so that user would be able to view their accounts, payment history, last six months bill details, last six months payment made.
10	System should have facility to apply for Refund of water security
11	System should have facility to apply for plinth level certificate
12	System should have facility to Sending acknowledgement mails/ SMS to applicant after submission / approval / rejection of application.
13	System should provide facility to pay bill and connection fee submission online.
14	Recovery of the defaulter's bills
15	MIS Reports and Dashboard
16	Mobile apps(Androids/I-Phone/Windows)
18	Data Digitization and Data migration.
19	Portal should be multilingual (English & Hindi)
20	System should provide facility to resubmit the application if it is rejected by the approving authority.
21	System should send notification of application to approving authority.
22	System should provide facility to approving authority to reject or approve theapplication.
23	System should generate unique application and connection number after submissionof form and final approval respectively.
24	System should also record offline application in the system.

5.7 Web Portal and Mobile Application

Overview

a) At the core of the stakeholder's service experience will be citizen portal of BSCL which will be a gateway to citizens, tourists and businesses for disseminating information and engagement. It will be accessed by citizens, investors and corporates alike and shall provide factual and attractive information to investors. The portal should clearly communicate a sense of 'identity' at first glance. The Portal will have an intuitive user interface for rendering various services and providing role based access to various systems in use. Through the Portal, any user can seek information, request for services and status check on service request, lodge an incident/complaint and provide suggestions. Portal shall exhibit enriched info graphics on various parameters of smart solutions.

b) Portal should serve as a cutting-edge communication tool that clearly conveys its mission, vision, offerings and purpose. The site shall help prospects and citizens to better understand and engage with the BSCL's mission. Portal shall be a useful tool for the target audience, while being visually appealing, user-friendly, and state-of-the-art. It must allow easy navigation. Portal must have an attractive mix of text, images, audio and video.

   The portal should:

   i. increase traffic and visitor engagement through architecture, design, and other features such as social media integration
   ii. help visitors easily understand the corporation's mission and obtain information about BSCL's offerings
   iii. deliver content concisely and clearly; includes dynamic information

c) The portal should have links to log-in for visitors (through APIs of Gmail/Face-book etc.) and employees. This log in shall redirect the user to the portal with rights to view or update content as per user status. The home page shall be clean and visually compelling that quickly conveys to the visitor, corporation's mission and what the BSCL does. This shall include dynamic 'Call-Outs' which highlight what's new on the website as well as information sliders. The portal should primarily be available in Hindi & English.

d) Mobile enablement framework will be deployed for BSCL, which deals with both rendering the portal in mobile devices through necessary UI components as well as making hybrid mobile apps or a single common hybrid mobile app supporting all standard mobile platforms including Android, iOS, Windows. App shall be available on App store (iOS), Google play store (Android) etc. for freely downloadable for interested stakeholders.

e) Mobile application software is applications software developed for handheld devices, such as mobile phones, tablets etc. These applications can

be pre-installed on phones during manufacture or downloaded by users from various mobile software distribution platforms, or delivered as web applications using server-side or client-side processing (e.g. JavaScript) to provide an application like experience within a Web browser.

f) Mobile Application Dependency on Handset and O/S Mobile Application software developers also have to consider a lengthy array of screen sizes, hardware specifications and configurations because of intense competition in mobile software and changes within each of the platforms.
g) Data Collection: m-forms Mobile Application can also make use of the various forms for data collection. Many data collection systems are built from existing commercial or open source components, or even come packaged as an end-to-end solution. The data collection may be done by various methods. Details are provided in Annexures of RFP.
h) The Citizen Mobile Application will receive grievances and inputs from both citizen and the Government, using multiple channels (including external social media) to drive the different redressal services, and in turn disseminate information using external media and the platform itself as channels. All the discussion topics, surveys, polls, blogs are specific to discussion groups. Hence, separate Government departments can create and moderate different discussion groups and the discussion topics, surveys, polls and blogs can be created within these discussion groups and moderated by the concerned Government department using the admin console. The solution also boasts of a robust analytical engine, a dedicated team to monitor and update the collaboration platform and BSCL stakeholders about the citizen sentiment/feedback on various discussion topics/polls on regular intervals.

There would be central development of all e-Gov Applications including the Mobile Applications in Bhagalpur, which would be replicated in all other Cities of Bihar State with the same Source Code.

Integration with existing and proposed ICT systems within BSCL ICT landscape, not limited to:

a) Smart Lighting
b) ICT Enabled Solid Waste Management
c) Intelligent Transportation System
d) E-Challan System
e) Public Bike Sharing
f) Smart Water Supply System
g) Smart Education
h) Smart Health Management System
i) e-Municipality
j) SCADA
k) Smart Road Network
l) eBuses Live Tracking and Monitoring System
m) eToilet Monitoring System

n) ICT component of eLibrary System
o) ICT component of Smart Bus Stop System
p) ICT component of Smart Parking System

5.7.1 Web Application in Bihar e-portal

a) I-BHUGOAL - It is a Geomantic Oriented Application Model for Bihar infrastructure mapping using GIS. It is meant to visualize MIS data spatially through thematic maps. A GIS / GPS / Remote Sensing based project for Bihar Infrastructure Mapping of educational facilities has been initiated to cover through a project GPS based data collection for GIS enabled school mapping for approx 75000 schools, 80000 Anganwadi Kendra, ITIs, Polytechnics, Engineering Colleges, Colleges and Universities of Bihar.
b) PHEDMIS - It is an integrated portal for supporting MIS and Android Apps developed for monitoring the progress of various ongoing schemes/projects of the department.
c) Transport MMP - Transport department has been computerized since last two decades. In order to facilitate e-Services, software namely VAHAN and SARATHI have been implemented in all 38 districts of Bihar. These applications have been developed to provide e-Services like issue of Smart-Card based Registration Certificate of Vehicles, Smart-Card based Driving License, Dealer-point-Registration, Computerized Tax Token, National Permit Authorization (NPA) etc.
d) ELECON - ICT Interventions in Election Management for Randomization, Force Deployment, e-Counting, GIS Mapping of Booths etc. were implemented during recently held Assembly Election 2015.
e) Land Records - Data of eighteen (18) districts have been captured through Bhu-Abhilekh software and published on http://lrc.bih.nic.in.
f) NLRMP - A number of efforts has been undertaken under NLRMP that includes capacity building programme on NLRMP for Assistant Settlement Officer, Kanoongo and Amins to make them master trainers focused on different activities carried out under NLRMP program.
g) E-Prisons - Prison Management System (PMS) captures the data pertaining to prisoners in a prison. Visitor Management System captures visitor's records. Stock Management System, Hospital & Wages management System, Gate Management System, Arms & Ammunitions Management System have been developed for better utilization of the data captured by PMS.
h) E-PDS MMP - Under E-PDS MMP, a National e-Governance Programme, Bihar is the first state who generated Ration Card after implementation of National Food Security Act. 1.45.
i) IVFRT MMP - The purpose of Immigration, Visa, Foreigners Registration Tracking System is to develop a secure and integrated service delivery framework and to facilitate legitimate travellers.
j) E-Panchayat MMP - e-Panchayat Enterprise Suit (PES) has been launched on August 2013 in Bihar for 3-tier of Panchayati Raj Institutions (PRIs), viz,

Zila Parishads, Panchayat Samitis and Gram Panchayats. Geographical coverage / Demographic coverage spread in all the 38 Districts.

k) NREGASOFT - NREGASOFT has been implemented in 534 blocks of 38 districts in Bihar for Rural Development Department. This covers various processes of MGNREGA such as issue of Job cards, Scheme details, Muster Roll, Fund Transfers, Bills and other expenditure. AWAASoft for delivery of IAY houses has been implemented across the state. SAMVIDA, online Recruitment Portal for Contractual and Volunteer Services has been implemented by the departments.

l) Chanakya - e-University popularly known as Chanakya is for automation of university business processes related to Registration and Examination module. It has been deployed in MMHAPU to cater to the need of enrolment, pre & post examination activities of institutions and university. The software implementation has been initiated to be implemented in Aryabhatta Knowledge University (AKU).

m) National Database of Arms License (NDAL) - The purpose is for creation of National Database creation of Arms License by Arms License Issuing Authority using NDAL Application Software to provide Unique ID to each License Holder.

n) E-Gazette - E-Gazette (http://egazette.bih.nic.in) is an online application for viewing, printing and downloading of published Gazettes of Govt. of Bihar.

o) Mukhyamantri Kshetriya Vikas Yojana (MKVY) - It is implemented in Planning & Development Department for MLA Local Area Development Schemes.

p) National Animal Disease Reporting System (NADRS) - This project is being implemented by NIC for the department of Animal Husbandry, Dairying and Fisheries. 574 locations in Bihar have been identified to access the information from blocks. Disease reporting is being done from 510 locations to provide instant alerts to all concerned about Animal Disease Outbreaks, Remedial measures etc.

q) Jeevan Pramaan - Jeevan Pramaan is a biometric enabled digital service for pensioners. Pensioners of Central Government, State Government or any other Government organization can take benefit of this facility. First camp of Jeevan Pramaan at Danapur Cantt generated 367 numbers of Digital Life Certificates.

r) Court Informatics - It has been implemented at Bhagalpur High Court, the leading High courts in India to Computerize Cause List Management System. Daily Cause lists are published on http://causelists.nic.in.

s) Case Information System – It is in Divisional Commissioner, Bhagalpur Court and BHRC, Board of Revenue and DCLR Courts. The software is integrated with SMS facility. Recently, "Mobile App for Commissioner Court Case Information System" was also launched.

t) Online Farm Mechanization Application System (OFMAS) - It has been implemented for Agriculture Department. This is an online system for filling application for availing subsidy on farm equipments by farmer, dealer registration.

u) Online Application for Govt Quarter Allotment - It has been implemented in Building Construction Department, Govt. of Bihar.
v) Forest Management Information System - Forest Department is using this application for administering and monitoring e-Asset, e-Nursery and e-Plantation.

5.7.2 Web Portal

Functional and Technical Requirements

S.No.	Description
1.	**Home Page** A clean, visually compelling home page that quickly conveys to the visitor, the BSCL's mission and what BSCL does. It will include (but not limited to) the following information either directly or linked through other pages: ▪ About BSCL; Corporation, Message from the CMD, Board of Directors, Shareholding pattern, Organogram & Key Personnel ▪ City Profile ▪ Master Plan ▪ Investment opportunities ▪ Key statistics ▪ Tourist Locations ▪ GIS map of the City ▪ Photo Gallery ▪ Online Services listing (e-governance services) ▪ Opportunities; Tenders, Careers, Empanelment, Training ▪ Downloads ▪ Links to Face-book, twitter etc. ▪ FAQs ▪ Feedback ▪ Contact Us ▪ Search ▪ News & Updates ▪ Log in ▪ Privacy Policy, Disclaimer, Visitors count, Important links, Site map ▪ Portal must support advanced template and must have an integrated content management system in order to store images, stylesheets and various web artifacts
2.	**Branding:** Clearly communicates a sense of 'identity' at first glance.
3.	**Visual appeal:** The site must have an attractive mix of text, images, audio and video.
4.	**Fast Loading Pages:** Optimization of web pages for a faster browsing experience with compatibility with key industry browsers and platforms.
5.	**Responsive Design:** The site must be mobile-optimized through responsive design methods. Therefore, it should detect that a mobile device is being used and present the user with the mobile version first. The user should be able to switch to the desktop version and adjust resolution and format accordingly.
6.	**Bilingual** The portal shall be available in Hindi & English and Unicode complaint.

S.No.	Description
7.	**Simple and clear navigation:** The site should be easy to navigate. Information should be grouped and presented in a logical manner and require no more than three levels of "drill down" for the user to find the desired information thus creating a clean, clear, easy and satisfying user experience. This should include drop down menus, so that the visitor can easily find what they are looking for with a few clicks of the mouse.
8.	**Search Tools:** Provide search capabilities using key words or phrasing that will provide access to content from throughout the site. Additionally, make it possible to download historical and recent data whereby the user can define his/her preference. Platform should allow users to search content of the portal easily and quickly without the need of high speed bandwidth.
9.	**Important Links:** Links should be placed within the portal to allow individuals to contact institutions affiliated with the BSCL and access to the portal as well the respective departments/agencies/corporations/ministries.
10.	**Easy access to Key performance indicators (Infographics):** Seamless presentation of dashboard data to provide continuously updated graphs and charts.
11.	**News/Update feed:** Constant and dynamic update feed on portal home page. Displays announcements and notifications for new content additions on front page of portal.
12.	**Calendar and bookings:** A dynamic calendar that displays events as well as filters for searching events and booking any available venues/functions.
13.	**Contact Form:** Provides a web-based contact form with anti-spam controls and shall allow stakeholders to track the status of request at any point of time, if any.
14.	**e-Mails**: automatically send follow-up emails to our stakeholders (subscribers) if they visited a specific web page, or completed some specific task (e.g. survey) on the website.
15.	**Social Media Engagement Tools:** New tools to improve interaction with social media. Portal platform must support advanced features for social media integration and analytics.
16.	**Search Engine Optimization (SEO):** Portal availability using common search engines to ensure it is optimized using SEO.
17.	**Search capability:** Portal should provide search engine with advanced full-text search capabilities.
18.	**Compatibility:** Site must be compatible with common operating platforms including Google Chrome, Microsoft® Internet Explorer 8.0 or higher, Microsoft Edge, Mozilla Firefox, and Safari 5.0 or higher.
19.	**Mobile Access**: Portal must be "responsively designed" to accommodate mobile users. This also includes accommodations for slower, cellular internet connections. This includes compatibility with iOS, Android and other industry standard platforms.
20.	**Settings:** Portal must not require plug-ins as a default.
21.	**Performance:** Portal must be able to handle multimedia (video) with high performance.
22.	**HTML Compliance:** Full compliance with HTML 5.0 or higher.
23.	**GIS:** web GIS view of BSCL Smart City depicting information through various layers would be shown to stakeholders; showing occupied and vacant land parcels, access to information on industries, residential properties, education & health facilities, transportation etc.
24.	**Security:** Portal shall be secure against hacking and other vulnerable activities.

S.No.	Description
25.	**Content Management System:** ✓ shall have Content Management System to update the content on the Portal which shall have minimum following capabilities: ▪ Content Authoring ▪ Content Publishing ▪ Content Delivery ▪ Content Storage Management ▪ Content Archival ✓ Separation of content from presentation, which allows authors to focus on content rather than web design. ✓ Content storage management of all types of content; text graphic, audio, video etc.
26.	**Integration with other applications:** Different existing and future applications/modules shall have to be seamlessly integrated with the portal. It is envisaged that GIS and the proposed systems shall work in an integrated manner to allow BSCL to extract maximum benefits from the system.
27.	**Design and Construction** ▪ Work closely with the BSCL at each stage of the design to identify user needs and corresponding user interface requirements, workflows, and functionalities ▪ Ensure integration of all elements including content, information format, compatibility with software platforms used by BSCL and standards for content management ▪ Platform should allow easy integration of multimedia products and user-friendly administrator interface ▪ Create wireframes, storyboards and prototypes to propose options for implementation. Provide five (5) template designs for review to select a concept ▪ Concepts should reflect the BSCL's identity, nature and purpose ▪ Develop corresponding user interface components (web templates, style sheets, scripts, images, dashboards, social media interfaces) as needed ▪ Use simple, cost-effective techniques to test designs with representatives of target audience prior to launch of portal ▪ Submit the final concept to BSCL for review prior to 'going live' ▪ Secure the existing portal prior to transitioning to the new platform ▪ Keep a full backup of the portal through the currency of the Project ▪ Manage all upgrades and updates on the website including content update in an efficient and integrated manner ▪ Portal design shall support easy upgrades and updates on content without the need to redo the base design.

5.7.3 Mobile App

With rapidly increasing levels of mobile penetration and continuous improvement in bandwidth, and requirements of accessibility and citizen convenience, it has been envisaged to offer information dissemination to stakeholders over mobile devices. There shall be a strong interfaces, technologies, applications etc. for mobile devices.
Application architecture must provide for a robust mobile backend layer, providing for listed functionalities like push/pull notifications, storage of images, geolocation, advanced analytics etc. with standard Active-Active clustering on high availability mode. MSI can consider a public cloud based deployment for such mobile backend layer, as per modern architecture standards. In order to maximize citizen convenience and bring about business process improvements, the successful MSI shall continuously innovate, upgrade and incorporate such new technologies that emerge new avenues.

Functional and Technical Requirements :

S.No.	Description
1	Mobile app should mirror the portal and be adapted for optimum viewing on multiple operating systems and device sizes. However the actual application layout design for both mobile and web is the responsibility of MSI.
2	Mobile app must be based on latest HTML 5 and above.
3	Mobile app shall be hybrid on Android, iOS and Windows platform.
4	Mobile app should be in Hindi & English and capable to take the load of all concurrent users at peak time. MSI has to evaluate and make the app's functioning smooth for peak load.
5	Mobile app should be capable of showcasing enriched infographics to its stakeholders.
6	Mobile app shall be designed in such a manner that it shall address the following key issues: ▪ Caching: Caching unnecessary data on a device that has limited resources ▪ Communication: Failing to protect sensitive data over any carrier ▪ Data Access: Failing to implement data-access mechanisms that work with intermittent connectivity
7	Mobile app shall be integrated with main core solution proposed. There shall be facility to PUSH through and PULL through mechanism to get and receive information using SMS service.
8	Mobile app shall provide critical data such as user identification and location information including latitude, longitude and altitude.
9	The mobile app shall have the ability to take and transmit, pictures and videos in real time along with geo-tags from the device.
10	Mobile app should have capability of - ▪ Image compression, B/w conversion from color images ▪ Auto cropping, Auto orientation, perspective correction, geo capture ▪ Image capture setting (camera resolution, image type)
11	Mobile app shall have the ability to post bulletins and resources on another mobile app through API's.

S.No.	Description
12	Platform will provide a report generating tool, which can be used to generate customized reports at any level.
13	Platform should allow for a graphical interface to view the summary data in MIS reports. This would include trend graphs, graphs indicating how much of the target has been met etc.

5.8 Network Backbone and Internet Connectivity

Overview

a) Pan city network backbone and internet connectivity is an important component of the project and needs very careful attention in assessment, planning and implementation. It is important not only to ensure that the required connectivity is reliable, secure and supports the required SLA parameters of Latency, Jitter, Packet Loss and Performance. City wide network is essentially intended to provide high-speed network connectivity for supporting all existing and future smart solutions. The project objectives broadly are as follows:

   i. To provide inexpensive and pervasive connectivity all across the city

   ii. To boost digital inclusion among departments and citizens

   iii. To provide 24*7 uninterrupted connectivity across the city

   iv. To establish a medium for quick data gathering from multiple sources and faster decision making

   v. To act as a channel for integration of all the city services

   vi. To enable the government to have advanced communication products/platforms and better security and surveillance systems

b) The IP High Level Design is recommended to be built on a hierarchical model with a N+1 redundancy. The main design methodology is to focus on essential functional layers where hardware of different traffic handling capacity can be plugged in and out as the city grows. The different design blocks that create the network high level architecture are:

   i. Core
   ii. Distribution/Aggregation
   iii. Access

A typical Network Architecture is shown in **Figure** below:-

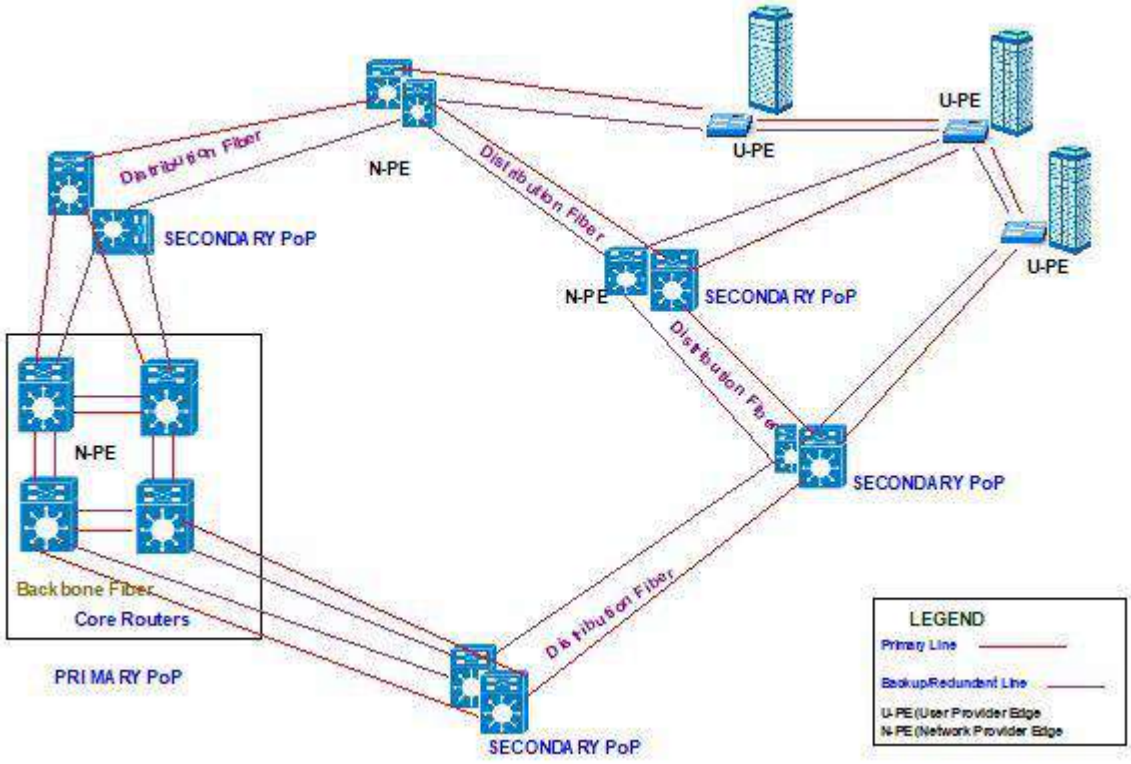


Figure 5: Design of Distribution and Access Network

c) The Access nodes provide different UNI (User-Network Interface) options as well as performing service multiplexing, subscriber security considerations and any or all the other functionality required for triple play service delivery and support. Another important consideration is that for Multi Dwelling Units (MDU) (Either commercial or residential buildings), the Access switch (U-PE) will reside in the Tertiary-PoP. The media choices for Access are either copper access, such as Category 6 unshielded twisted pair, or fiber. A pair of Access U-PEs devices in every PoP shall be used to terminate and support services like Video Surveillance, Traffic Management etc.

d) The Core layer would initially support 100Gbps network to support up to 200 Gbps eventually. For Distribution/Aggregation layer initially it would support 50 Gbps and later 100 Gbps and for the Access layer it would be 10 Gbps initially and 50Gbps at a later stage. The Core backbone, Aggregation zone backbone and the Access layer backbone with Ring topology all would be 96 core OFC. Each Core zone could contain many Distribution sites connected in a full mesh/ring topology. There will be at least one Distribution site per Primary and Secondary PoP. Each Distribution link towards the Core will initially provide 50 Gbps of bandwidth in a redundant manner therefore the whole bandwidth on an Distribution node will be 100 Gbps. Similarly for the whole Distribution site total bandwidth handling capacity will be 200 Gbps i.e. 100 Gbps per Distribution Node. At a Primary-PoP the Distribution site equipment will be co-located with the Core equipment in order to serve the city blocks in the vicinity. Access nodes have high speed fiber point-to-point links towards the Distribution layer supporting bandwidths from 10 Gbps or higher. They have low speed fiber, copper or wireless links towards customer CPEs supporting bandwidths from 1 Gbps to 10 Gbps.

Assumptions

a) Minimum expected bandwidth for Services(single entity) such as Internet BW, IP TV

BW, VAS, Video game etc. would be around 800 Mbps.

b) Each residential or commercial entity shall be connected using a 1 Gigabit physical interface.
c) Each residential unit will have only one Home Access Gateway(HAG).
d) Each commercial, business or utility will be provided with at least one Customer Premises Equipment (CPE). Additional CPE devices can be provided on demand to meet redundancy or high availability requirements
e) The HAG or CPE shall be the demarcation point between the customer and the OAN provider.
f) The Access switches of the OAN provider will be placed in the Main Telecom Rooms of the residential, commercial or utility buildings.
g) Access switches will be also placed in the PoPs to meet the requirements of some of the public services.
h) The Primary PoP will have core equipment. Secondary PoPs will have Aggregation equipment and Tertiary PoPs will have Access equipment to provide connectivity's.

The proposed smart city solution will involve city wide network coverage across various locations in BSCL. BSCL smart city will offer various smart services to its citizens. To provide these services in an uninterrupted and effective manner a robust network is required to be deployed. Network needs to be planned to meet the all the network requirements for currently services envisaged, scalability and future requirement. BSCL intends to provide connectivity at locations like; municipal offices, Bus depots, traffic junctions, parks, fire brigade, police stations, urban health centers, schools etc. MSI would be required to create a single network i.e. city wide network for the smooth functioning of all solutions. Successful bidder is required to integrate city wide network with Data center (DC), Disaster recovery (DR) and Command & Control Center (ICCC).

BSCL intends to procure Leased Circuits & Internet Bandwidth for the city wide network under the BSCL smart city Project. The successful bidder is required to terminate the desired Leased circuits and Internet Bandwidth at the locations to be identified by MSI in consultation with BSCL.

A Service Level Agreement will be signed with the successful bidder. As bidder, will be responsible for smooth functioning of the entire network connectivity, availability of sufficient quantities of all the critical components will be taken care of by the bidder to maintain the guaranteed uptime. Bidders are requested to take into consideration the equipment's required at each location for providing connectivity while quoting for the tender.

Full Duplex Bandwidth as Per Schedule of Requirement has to be provisioned and implemented by the Service Provider. Service Provider has to keep provision of giving burstable Bandwidth & the rates will be as per finalized rates. Service Provider has to arrange fiber & other last mile equipment accordingly including media convertors wherever required.

5.8.1 Scope of work

The detailed scope of work for MSI for providing of pan city network backbone is given below:

a) Bandwidth Provisioning

MSI shall implement the solution in and procure &provision the network bandwidth as per details given below. MSI shall be responsible for upgrading its infrastructure, including the last mile, to meet the requirements of the BSCL, at

no additional cost to the BSCL. The network & bandwidth should meet following requirements:

i. BSCL may order an increase/decrease/termination/withdrawal in bandwidth, which bidder shall take into account.
ii. The network should be capable of providing Bandwidth on Demand for planned as well as for unplanned activities.
iii. MSI should provide the bandwidth for intranet & internet.

b) Internet Bandwidth at ICCC, Data Center and all field locations
   i. BSCL is procuring bulk internet bandwidth for the requirement of various locations throughout the city. MSI is required to terminate these links at the desired locations defined as per the price bid format of this RFP.
   ii. Redundancy
   iii. As a measure of redundancy remote locations, ICCC, DC & between DC & DR site connected through Leased Circuits should have redundancy in place to meet necessary SLA requirements.
   iv. Location-wise Bandwidth requirements should be planned by MSI
   v. Rate Contract
   vi. BSCL is procuring leased circuits to be delivered at various locations spread across the BSCL city.
   vii. Looking at the scalability and future requirement discovery of prices shall be valid for the period of contract duration under the Rate Contract as per price bid.
   viii. It has been observed that there is a considerable price reduction in cost of domestic and Internet bandwidth during last few years. Hence, BSCL will review the prices at end of every year and MSI is required to match the prevailing market prices as per TRAI regulations.
   ix. Adding new location – whenever a new location is decided to be added by the BSCL, an order will be placed with MSI at the contracted price. MSI shall carry out site-survey at new location for feasibility of location over wired connectivity. MSI would be required to implement and commission the location within 2 weeks from the date of work order.

5.8.2 General Specifications

The areas covered under Bidder's scope are as follows:

a) IT Data Center complete in all respect (UTP / STP CAT 6A, 10G and 10G fiber (Single Mode OM3 OM4 fiber))
b) All cabling will be Intelligent Cabling Solution for Facility and for Rack to Rack connectivity MTP 40G Solution.
c) Backbone between Spine and Leaf switches (Single Mode OM3 fiber) and Spine Switches to Leaf Switches in Hub rooms for sitting area (Multi Mode OM3 fiber). The server racks and storages may have any of the three possible interconnects
d) Structured cabling involves supply, installation, testing and commissioning of all Jack panels, Network/Server Racks, Laying of cables (FTP/Fiber), Terminations at both end and other passive components.
e) Cable laying will be through metal raceways, PVC conduits, overhead ladder / tray and

other relevant activities.

f) Laying of FTP Cable in raceways includes proper bunching and tagging for Data/ Voice Cable including color coding.
g) Preliminary continuity Testing & Ferruling at both end for the each cable, unique identity by proper Tagging.
h) Termination, Installation, Fixing of 24 Port Jack Panels including proper Dressing of Cables
i) Fixing & Casio labeling of Jack Panels
j) Installation & proper routing of Patch Cords in Racks, Jack Panels and wire/ cable manager with tagging of Mounting Cords
k) Installation of Network rack with proper cable management, Ladder Fixing, fixing of panels including control panels, fixing of Vertical Wire Manager, Horizontal Wire Manager etc
l) Penta-Scanner Testing of laid FTP Cables for the performance testing of Installed Cabling System with EIA/TIA specified parameters like Resistance, Delay, Attenuation, Wiremap, Return Loss, PSNEXT, PSELFEXT, ACR etc.
m) Documentation of the Installed Network with the as built Diagram and labeling details of the I/O's and Jack Panels and Penta-Scanning Results of Nodes
n) Fiber termination and Management System and Fiber routing also has to be included in the scope.
o) The bidder shall give the break-up prices of each component being used in the scope of structured cabling
p) Though the approximate no. of ports per facility is given below, the bidder may add points they feel necessary for any particular facility after obtaining necessary approval.
q) All horizontal cabling should emanate from Jack panels on the distribution switch and be routed to outlets nominated through ceiling space, risers, skirting duct and workstation partition duct etc.
r) The cables must be laid in an aggregated manner to reduce the cabling space requirement.
s) Cables should be installed in a workman like manner, parallel to walls, floors and ceilings, as applicable.
t) The Manufacturers cable form should be maintained at all times. No distortion due to kinks, sharp bends or excessive hauling tension should be allowed to occur during installation.
u) Care should be taken to prevent other trades damaging the cable by walking or storing heavy objects on them whilst laying out and installation.
v) Cables should be run in a manner eliminating any possibility of strain on the cable itself or on the terminations.
w) Cables entering or exiting trays, conduits, centenary wires and other fixed support should have a small gooseneck or slack provided and should be fixed at both ends to prevent the possibility of cable stress.
x) Cables should be concealed except where nominated otherwise, and should run in neat lines.
y) Cables should have no joints or splices, all foil should necessarily be grounded at all terminations.
z) Cables should be kept at a minimum distance of 150mm from items liable to become hot or cold. The distance should be consistent with the maximum or minimum temperature possible and the cable type. Cables should at no point make direct contact with such items.
aa) Cables should not be directly embedded in plaster, concrete, mortar or other finishes

unless they are in conduit and capable of being fully withdrawn and replaced after the building is finished without damage to finishes.

bb) Bending radius should not be less than the manufacturer's recommendation and in any case should be not less than eight times the overall cable diameter.

cc) Cabling will run in separate shafts and ducts from the electrical ducts so as to avoid any interference.

dd) Cable should either have a nylon sheath or should be enclosed in a conduit if running underground.

ee) Under no circumstance hand labeling of the cables will be accepted. No hand punching shall be allowed without proper tools. Labeling and Punching should be done as per TIA/EIA standards

ff) All copper conductors must be tested for continuity and pair integrity as well as EMI interference.

gg) Any cable that does not meet TIA/EIA specifications should be repaired or replaced at the Vendor's expense.

hh) The termination of connectors should be RJ-45 Single Information Outlets with faceplates, shutter and Surface box

ii) The Fibre Couplers and Connectors generally would be LC type

jj) There should be Professional Cable Management and tools available on site e.g. FTP Cable Termination tools

kk) Each outlet shall be tested for satisfactory operation based on certification parameters valid for the entire warranty period of 20 years or more as applicable. All outlets in the Facility be clearly marked, labeled & documented for future reference.

ll) Maintenance of the LAN Passive components shall be done by the Agency. Provision of additional Passive nodes whenever required shall need to be provided based on requests. The bidder must quote per termination charges in various slabs.

mm) Cable layout plan should be submitted as part of the technical bid.

5.8.3 Technical Specifications

a) Leased circuit:

x. The bandwidth must be provisioned on Optical Fiber Media. No other last mile media type is acceptable.

xi. Latency from point A to point B should not exceed 20 ms.

xii. The bandwidth supplied should be symmetric, dedicated 1:1 with 100% throughput.

xiii. Up time guarantee must be 99.5 %.

xiv. Deliver this bandwidth on a fiber optic cable network at the respective locations.

xv. All costs to connect the links to last mile node of SCADA has to be borne.

xvi. BSCL need not pay or reimburse any last mile of extra work cost.

xvii. To be used the IP addressing schema provided by the SCADA.

b) Internet Bandwidth

xviii. The bandwidth must be provisioned on Optic Fiber media only. No other last mile media type is acceptable.

xix. BSCL is procuring bulk internet bandwidth (as per the Price bid) for the requirement of various locations throughout the city. However, successful MSI is required to terminate these links at the desired locations.

xx. Latency to Google, Yahoo and NIXI peering should not exceed 200 ms.
xxi. The bandwidth should be dedicated 1:1 with 100% throughput.
xxii. Up time guarantee must be 99.7%.
xxiii. Provider must have minimum two sources of Internet Gateway bandwidth input.
xxiv. To deliver this bandwidth on Gigabit Ethernet optically or electrically which will be taken as input.
To deliver the required bandwidth on a fiber optic cable network at the desired locations.
xxv. All costs to connect the link to the last mile node has to be borne by MSI. BSCL will not pay or reimburse any last mile of extra work cost.

5.9 Smart Urban Solution

MSI has to implement below mentioned solutions as per city requirement where provision of various smart solution to be implemented based on various use cases and provide the better response real time bases for effective and efficient public service delivery. The urban smart solutions implemented in city should have friendly features to the extent possible and adhere the guideline issues by Government of India. The solution implemented in the city are as follows as a part of scope of Work:

5.9.1 Edge Analytics and Response Systems

MSI has to work out the quantity and location of these devices during Requirement study of the project based on the Surveillance requirement. Video, Audio Edge sensors and instrument based Analytics with Artificial intelligence and continuous learning are crucial for the safety envisaged, all analytics shall be edge based and will have the capability of continuous machine learning. The advantage of analytics shall be to leverage the current AI technology available and help in incident based surveillance including lower consumption of bandwidth. AI based analytics are preferred to be integrated with Video Management Software to avoid integrational hazards at the time of installation.The minimal expected functionality are mentioned in the below table.
The functionality shall be achieved to meet the requirements of the Detailed use cases, such that the algorithm is implemented at any of the levels in the architecture. The design shall be such that the functionality and use case can be implemented on any Commercial off the shelf device, camera, server, datacenter and cloud. Below use cases should be provided as minimum requirement from the integrated platform proposed by the MSI as a combination of multiple systems like AI platform, VMS, Cameras, ICCC etc. Annexure 1&3 of RFP Volume-2 provides details of locations and quantities to be considered for sizing parameters.

Sr. No	Functionality	Detailed use case
1.	Solid Waste Management	1. Graffiti and Vandalism detection 2. Debris and Garbage detection

Sr. No	Functionality	Detailed use case
		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
2.	Loitering Detection	1.Loitering detection in a given area of interest. 2. Upon verified and confirmed by operator that it is a suspicious person, the system shall be able to track the person across various cameras and to find the origin of such person. The track/trace of the person shall be shown on the map.
3.	Camera Tampering	1. Alert to be generated when camera is tempered by way of change of Field of view of camera, blurring of view, blocking of view by cloth or obstruction, camera disconnection, blinding of camera by laser or flashlights. 2. Once alter is generated, the incident should be flagged, and system should have the capability to trace the person responsible for the sabotage in other cameras and send notification to nearest Police asset on the field about the person of interest. The track/trace of the person shall be shown on the map.
4.	Abandoned object detection	1. System should detect an abandoned object in the configured field of view of

Sr. No	Functionality	Detailed use case
		the camera. 2. System should be able to find in one click when this object of interest entered the scene of interest for the first time. 3. Once verified and confirmed by operator that it is a rouge object, the system shall be able to call it as blacklist and be able to search metadata of the object across the camera recording for timestamp of entry and associated videos. 4. The system shall be able to track the person who left the object across various cameras. The track/trace of the person shall be shown on the map.
5.	Object Classification	1. The system should classify objects into vehicles (color/make/model), Humans(male/Female/Children) 2. The system shall allow different data analytics to be applied on such object classified data. E.g., % of children Vs Adults in an identified camera/area, or ratio of 4 wheelers Vs 2 wheelers in a given segment of time.
6.	Tripwire/intrusion detection	1. detection of intruder entering/exiting a given area of interest. 2. Once verified and confirmed by operator that it is a rouge object, the system shall be able to track the person across various cameras and to find the origin of such person. The track/trace of the person shall be shown on the map.

Sr. No	Functionality	Detailed use case
7.	Person/Face Recognitionusing AI based Facial Recognition System	Detailed description of the system is elaborated in the RFP
8.	Person tracking over network of cameras	1. Tracking of person based on image captured from the proposed cctv footage, e.g. - pause the video and track the person of interest in multiple CCTV cameras and stored video footage of 30 days. 2. tracking of person based on verbal clues given to the central control room e.g., man having beard, dark skin, with white shirt and blue jeans and black jacket. The system shall trigger search and tracking based on attribute-basedsearch. 3. Tracking of people based on Full body photographs received by the police control room. 4. Tracking and detection of people based on Facebook or social media profiles on camera footage as well as recorded video footage.
9.	Gender identification	1. Identification of Male & Female
10.	Hair Identification: Long or Short	1. Identification of long and Short hair.
11.	People counting	1. Counting people in given area of interest or getting % occupancy by people or crowd in given scene of interest. 2. Flagging incident incase crowd level is above defined threshold.
12.	Person collapsing	1. detection of incident and flagging in Control room for medical response if required.
13.	Incident detection: Fight (action)	1. detection of fight in a given area of interest. 2. Once verified and confirmed by operator that

Sr. No	Functionality	Detailed use case
		it is a rouge situation, the system shall be able to track the person across various cameras and to find the origin of such person. The track/trace of the person shall be shown on the map.
14.	Vehicle attributes detection (color/make/model)	1. System should detect, and track Vehicles based on color/make and model.
15.	Automatic Number plate recognition system	Detailed description of the system is elaborated in the RFP
16.	Tracking vehicle across cameras	1. Tagging of vehicles as they pass through ANPR cameras 2. Tracking of blacklisted vehicles across multiple cameras based on attributes like Color/Make/Model. 3. Integrated map for visualization, co-relation and tracing the path of vehicle
17.	Speed of car/vehicle	1. Detection of speed of the vehicle 2. Flagging an incident of speed violation if the speed of vehicle is above a given threshold 3. Provision to e-challan the defaulter once confirmed by the operator 4. Predictive analytics to know the probability of speed violations in a given geography and time, so that speed interceptor vehicles can be directed to the challan the violators.
18.	Helmet detection on two wheelers	1. Detection of violation and flagging it to the Control room. 2. Provision to e-challan the defaulter once confirmed by the operator 3. Predictive analytics to know the probability of violations in a given

Sr. No	Functionality	Detailed use case
		geography and time, so that Traffic police can be directed to challan the violators.
19.	Wrong way driving detection	1. Detection of violation and flagging it to the Control room. 2. Provision to e-challan the defaulter once confirmed by the operator 3. Predictive analytics to know the probability of violations in a given geography and time, so that Traffic police can be directed to challan the violators.
20.	Illegal turn by vehicle	1. Detection of violation and flagging it to the Control room. 2. Provision to e-challan the defaulter once confirmed by the operator 3. Predictive analytics to know the probability of violations in a given geography and time, so that Traffic police can be directed to challan the violators.
21.	Improper/Illegal Parking	1. Detection of violation and flagging it to the Control room. 2. Provision to e-challan the defaulter once confirmed by the operator 3. Once verified and confirmed by operator that it is a rouge object, the system shall be able to call it as blacklist and be able to search metadata of the car/vehicle across the city checkpoints and ANPR camera databases for timestamp of entry and associated videos. 4. The system shall be able to track the person who left

Sr. No	Functionality	Detailed use case
		the object across various cameras and to find the origin of such person. The track/trace of the person shall be shown on the map. 5. Predictive analytics to know the probability of violations in a given geography and time, so that Traffic police can be directed to the challan the violators.
22.	Authorized vehicle entry	1. Whitelisted cars/vehicles to be approved as authorized.
23.	Automatic Anomaly detection	Detecting abnormalities, threshold and KPI violations. Can be done through ICCC/Smart City platform
24.	Threat detection	1. occurrence of detection of more than 1 incident in predefined zone or a pattern of incidents from more than one sensor including camera, panic button sensor, or video analytic alert shall be considered a threat. 2. System shall be able to link the multiple incidents to the same threat automatically using co-relation. 3. Operator shall be able to detach a given incident from a threat level scenario and be able to attach sub-incidents into a given threat level scenario. 4. Based on all the alerts received by the system, the system shall always operate in given threat level, and deploy SOP's which are congruent to the threat level at which the control room is operating. Threat level can be enhanced at times of VIP

Sr. No	Functionality	Detailed use case
		visits where the SOP's will be congruent to the level of threat anticipated by the organization.
25.	Forensic Analytics	Detailed description of the system is elaborated in the RFP

5.9.2 Edge Analytics Specification

w) Deliver 16.2 teraflops of single precision performance or better. Have minimum 100Mb/1GbE management network link
x) Support 1GbE (via RJ45) or 10GbE (SFP+)
y) Support 2 or 4 GPU card device as per below table :

Type	Description	Critical Parameters
Type-1	Edge Analytic Device with 2 x NVIDIA Tesla T4 GPU cardsto handle a minimum 80 Analytic channels	1. For External Use, to be placed in junction box, with continuous operating temperature for 0 to 55 Degrees Celcius. 2. Support for Wifi/Bluetooth/3G/LTE/USB port for monitoring/connectivity.
Type-2	Edge Analytic Device with 4 x NVIDIA Tesla T4 GPU cards to handle a minimum 160 Analytic channels	1. For Internal Use, to be placed at POP, with Temperature tolerance for 0 to 45 Degrees Celcius. 2. Support for 3G/LTE/USB port for monitoring/ connectivity.

5.9.3 Functional & Technical Requirements for IOT

a) Based on requirement of the proposed solutions/integrated solutions, MSI has to provide details of Internet of Things (IoT) sensors in terms of types/categories/location in requirement study. IoT must be configured in such a way, that it provides an end-to-end solution for a comprehensive, scalable, and cost-effective IoT architecture, with following capabilities:

i. Develop and Deploy applications faster, shrinking development costs and time to quickly provide city services by way of integrating IOT sensors from any manufacturer into the IOT application layer proposed for the city. The Application layer should not be from the same manufacturer as the IOT sensors to ensure openness of the RFP.
ii. Manage and Analyse large volumes of sensor and device data throughout the lifecycle, from collection to analysis. The layer should

be able to collect and analyze following unstructured data and structured data and make the control room meet its operational objectives in all 3 dimensions of lifecycle – Before, During and after.

- Unstructured data – video data coming from cameras, image photographs coming from citizens, audio of the DIAL 100 system, audio of the Police radio systems, GIS and map data, screens of operators and unstructured databases like Hadoop, MongoDB etc.

- Structured data - databases, csv, files, protocol standards, SDK/API's of subsystems connected to the control room as part of the current RFP and future.

- The data in the control room shall be used in a complete comprehensive lifecycle of the city
- Before – provide insights before things happen by use of Predictive technologies on the data. Eg, predict traffic jams in city, predict crime types based on historical records etc.

- During - provide insights during things happening by use of automation technologies of workflow management and automating incident and crisis workflows.

- After – provide insights after the things have happened by proving 360 degree capability to reproduce, retool, remodel, recreate the incident from the data in the control room. The entire control room response to the incidents of the city operations shall be recorded 24 x 7 for a period of 30 days, including all the activities being done on the video wall screens, operator screens, ambient sound and video footage of the control room.

iii. Integrate and Automate, using data from connected sensors and devices to make city decisions closer to the network edge. The layer should be able to deploy on edge for data having latency or operational data which needs to have decisions on the edge. The record of such decisions taken on the edge shall be uploaded to the central control room on a continuous basis.

iv. Protect and Comply with security and regulatory requirements with robust, end-to-end data protection

v. Optimize and Innovate, integrating with business and industry applications to reduce costs and accelerate newservice delivery

b) In addition to that cities can unlock new business values, by gaining data-driven insights and drive actions from Internet of Things, helping Smart Cities grow faster and safer. All of this, leads to features like:

i. **Device Virtualization** – Standardize integration of sensors and devices with the city applications and services
ii. **High-Speed Messaging** – Enable reliable, secure, and bi-directional communication between devices in the data centre.
iii. **Endpoint Management** – Manage all city sensor and device endpoint identity, metadata, and lifecycle states
iv. **Stream Processing** – Real-time analysis and incoming data streams with event aggregation, filtering, and correlation
v. **Event Store** – Query and visualize massive amounts of data with integrated BI Service support and enable big data analysis
vi. **Enterprise Connectivity** – Dynamically dispatch critical IoT data and events to city applications and process flows
vii. **REST APIs** – API-based integration with apps and IoT devices
viii. **Mobility** – Send messages to devices from city and mobile apps, independent of device connectivity

c) Key capabilities include:

i. Integrate IoT data with city applications to enhance operations
ii. All-in-one or pre-integrated IoT platform to minimize deployment time and effort. Provide flexibility to fully support any IoT solution requirement.
iii. Support stream analytics, complex event processing-style event pattern matching
iv. A no-coding-required stream-processing engine with robust analytic capabilities
v. Predictive analytics run-time platform built on industry standard algorithms, use cases defined by city authorities and problems identified by city stakeholders..
vi. Gateway software for integration of 3rd party systems, broader analytics features and device virtualization
vii. Out-of-the-box integration with other city services and enterprise applications based on industry standard integration layers or customized integration for systems based on SDK/API integrations.
viii. Administration console for comprehensive provisioning, management and monitoring of devices, message storage and analytics, and enterprise app connections
ix. Robust device virtualization capability that automatically replicates device state and enables IoT to send administrative directives to devices
x. Provide flexibility and scalability for enterprise IoT systems
xi. Ability to define and use custom business objects for managing state and processes for IoT applications
xii. Pre-integrate all essential IoT capabilities and assure the first user experience is quickly gained
xiii. GUI-based administration and configuration

xiv. Enable enterprise application integration without needing separate 3rd party services
xv. Simplify enterprise and IoT data integration and insight
xvi. Provide pre-built/custom built IoT applications for common use cases to minimize delivery time and simplify deployment
xvii. Augment IoT service with big data/ML analytics
xviii. Provide machine learning for predictive maintenance, improve traffic conditions, improve weather forecasts and alerts etc.
xix. Geo-spatial mapping of IoT data for city use cases (e.g., shortest path etc.)Support real-time event streams to support city applications and analytics (e.g. collect and analyze vehicle locations etc.)
xx. Graphical visualization must be intuitive and easy to use when configuring data flows and streams
xxi. Provide various adapters and connectors to simplify integration with devices and enterprise applications
xxii. Include a suite of pre-built IoT applications for asset monitoring, predictive maintenance and logistics – preferably, at no cost

5.9.4 AI with Continuous Learning & Improvement System

a) Deliver processing units performance of 1 petaflop on FP16 or better
b) Have software tools for achieving the following tasks- Resource allocation, queuing of jobs, performance monitoring and creating software containers
c) Support commonly used Deep Learning based AI frameworks.
d) Have minimum 512GB system memory per system or better
e) Have dual 10GbE and 4 IB EDR per system.
f) Min power consumption per system.
g) Have dual 20-core Intel Xeon E5-2698 or better per system.
h) Support parallel computing architecture.
i) Support software libraries for continuous learning and improvement for betterment of intelligent video analytics software installed in edge/field devices using Deep Learning based AI methodologies.

5.9.5 Business Intelligence

a) The Business Intelligence platform should be a proven platform for creating powerful business intelligence applications that enables Smart Cities and city structures to quickly combine data from any source and rapidly create dozens of visualizations, dashboards and advanced calculations in a fast, friendly user interface. It should help cities discover citizen and city insights, and transform raw data to actionable insights. It can be used to predict citizen behaviour's, analyse city data to discover associations, patterns and relationships. Analytics must be instantly available on any device for both city personnel and citizens.
b) The BI platform should provide integrated end user access ranging from interactive dashboards, ad hoc query, pixel-perfect reporting, Office integration, proactive

alerting and mobile access, collaboration Scorecards, and embedded in business applications. Ad-hoc query and analysis environment that works against a logical view of information from multiple data sources in a pure Web environment. BI platform should provide capability combine data from multiple applications or databases in a single calculation. For example, it should be able to combine data from relational databases with non-relational data from Excel spread sheets in a single calculation. Moreover, the platform should offer out-of-box integration with Geo-Spatial analysis and real-time collaboration.

c) BI platform should provide capabilities to create KPIs to measure progress and performance over time and graphically communicate strategy and strategic dynamics using different type of customized views. Intuitive and dense visualizations must be available.
d) Alerting capabilities are required to capture and distribute notifications via multiple channels in response to pre-defined business events and/or data exceptions to speed exception based decision making. The alerting engine should have ability to invoke a workflow, web services, web content, BI content, etc. from the within the BI framework. When a condition is triggered, the user should be presented with a list of possible actions to take.
e) The platform must provide search capabilities for existing content based on full indexing of Dashboards, Analyses, Views, Prompts, KPIs, Scorecards, Formatted Reports, Folders. The metadata should be indexed and searchable. This should go beyond just searching report names and titles, but, instead deeply interrogating every defined analysis to see the contained data elements, prompts and filters.
f) Reporting and Adhoc Query should be available in form Web- based environment that is designed for users who want to create new analyses from scratch or modify and change existing analyses that appear on dashboard pages. BI should also provide feature of self-service where a user can upload his own excel sheet data and combine it with already published BI data and create his own dashboards with no help from IT.
g) Analysis & reporting layer should provide a single user interface for ad-hoc query, reporting & analysis against relational, OLAP and flat file data sources. It should provide complete interactivity with dash board content by selecting prompted values and filtering data; drilling on charts or tables to access detail; changing the sort order or sort direction of columns; maintaining context and moving to a different analysis by automatically passing constraints; or selecting columns to display.
h) City administrators should use a highly customized report format, layout, and output to create pixel-perfect reports and a scalable reporting server that generates and deliver scanned reports from multiple data sources, in multiple document formats, via multiple delivery channels. The Report Builder should generate multiple layouts, including HTML, PDF. It also should provide an interactive, on-line format for delivery over the Web.
i) Breach of KPI benchmarks should have the ability to trigger actions such as Email alerts, ERP workflows, Invoke Web Service, Score cards should provide visualization effective in communicating strategy and causal relationships between, KPIs, corporate objectives and initiatives.

j) Mobile access is another important aspect of the BI platform. Proposed tool should provide complete access to reports, dashboards, notifications through a hybrid mobile application on mobile platforms like Android and Apple. It should support catalog browsing and search over the mobile device. Catalog browsing and search makes it easy for the mobile user to locate and interact with relevant information.

k) In terms of platform availability, the BI platform should support clustering for high availability and scalability. The BI Platform should offer sophisticated Active-Active clustering with automatic failover that enables full utilization of compute resources, easy scale out to address dynamic performance demands, and on-line patching to minimize downtime during upgrade cycles.

l) In terms of security, the platform must be able to maintain user security internally, using standard protocols e.g. LDAP, Active Directory or OID. All data exchange must be SSL enabled.

Capabilities should include and not be limited to:

i. Simplicity, user experience, ease of administration and ease of use by leveraging a common UI and seamless interoperability between Answers and Dashboards.

ii. Single unified platform that integrates business intelligence and enterprise performance management capabilities through a consistent semantic layer. Moreover, it should be able to integrate with event processing applications to support real-time event detection and analysis.

iii. Support for Transactional Business Intelligence and geo-spatial mapping & datatypes

iv. The analytics component should allow users to explore data, upload data, share reports and dashboards, define and configure ad-hoc metrics, create templates, add comments and annotations.

v. User interface should be intuitive and easy to use. It is desired to have a unified administration interface and unified modelling environment. The user interface must be web-based and support various browsers (e.g. Chrome, IE, Firefox etc.) and mobile devices (e.g. Android, iOS).

vi. Caching and in-memory mechanisms must be available to support the creation of dashboards and reports in a timely manner.

vii. Implement an end-to-end analytic process for financial budgeting, planning, consolidation and close processes

viii. Support for multi-structured and big data analytics.

ix. Platform should support scalability, performance and high availability. There should be capabilities to support horizontal scalability, active-active and active-passive clustering, dynamic clusters, and cluster-aware caching. Caching should be supported at the report level and the metadata level.

5.10 Public Address (PA) System

Overview

a) The Public Address System (PA) shall be capable of addressing citizens at specific locations from the ICCC.
b) The proposed system shall contain an IP-based announcing control connected to the ICCC.
c) Public Address system shall be used at intersections, public places, market places or those critical locations as identified by BSCL to make important announcements for the public.
d) The system shall contain an IP based amplifier and uses PoE power which shall drive the speakers. The system shall also contain the control software which shall be used to control/ monitor all the components of the system which include Controller, Calling Station & keypad, Amplifier (Mixing & Booster).
e) It shall be able to broadcast messages across all PA systems or specific announcement could be made to a particular location supporting single zone / multi zone operations.
f) The system shall also deliver pre-recorded messages to the loud speakers attached to them from CD/DVD Players & Pen drives for public announcements.
g) The system shall contain an IP-based amplifier and uses PoE power that could drive the speakers. The system shall also contain the control software that could be used to control/monitor all the components of the system that includes Controller, Calling Station & keypad, Amplifier (Mixing & Booster).
h) PA system's master controller shall have function keys for selecting the single location, group of locations or all locations, simple operation on broadcasting to any terminal or separated zones.
i) PA system's master controller should facilitate multiple MIC inputs and audio inputs.

Scope of Work

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

a) MSI shall install IP based Public Address System as part of the information dissemination system in the city. These systems shall be deployed at identified junction to make public interest announcements.
b) The system deployed shall be IP based and have the capability to be managed and controlled from the ICCC.
c) MSI, in consultation with BSCL can propose alternate locations apart from the locations mentioned in this RFP for installing the PA system where their effectiveness in communicating information about traffic conditions in BSCL will be maximized.
d) BSCL shall review and approve the proposed locations. MSI shall install the PA system on the approved locations.
e) 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.

f) The PAS should also support both, Live and Recorded inputs and have minimum following capability

i. Speaker: To be used for Public Address System
ii. Connectivity: IP Based
iii. Access Control: Access control mechanism would be also required to establish so that the usage is regulated.
iv. Integration : With VMS and Command and Control Centre
v. Construction : Cast Iron Foundation and M.S. Pole, Sturdy Body for equipment
vi. Battery: Internal Battery with different charging options (Solar/Mains)
vii. Power: Automatic on/off operation
viii. CasingIP-55 rated for housing

Minimum Technical Specifications :

S.No.	Item	Minimum Specifications
1	Control Software	1.Using industrial-grade IPC chassis design, chassis with steel, with higher magnetic, dust-proof, anti-shock capability.
		2.17" LED display screen, built-in 5-wire reinforced industrial touch screen, easy to use touch-screen control.
		3.IPC pull-out keyboard design, operation more convenient, support 1 channel HD video output.
		4.Industrial-grade mainboard design, with Intel Haswell chipset, Intel fourth-generation core I3 CPU, memory dual channel 8G DDR3.
		5.Built-in 256G SSD solid state drive, read and write speed up to 600MB/S, without any movable mechanical parts, with superior durability and reliability.
		6.Use embedded industrial-grade server system (Linux systems) as a core operating platform, strong openness,easy extension development, upgrade, superior network support, and open source, high safety, strong compatibility, to protect the system from virus interference and damage.
		7.Support full-duplex audio terminal real-time two-way conversation, support a key for help, a key to broadcast,a key to monitor, session mode , at the same time to call etc. support time policy and forward policy customization, support the functions of calls limit hang up, mute automatically hang up, conference wait customization.
		8.The system supports the maximum 128 multi-parties simultaneous to attend discussion.
		9.Programming timing tasks, support broadcast timing offline files, recording, music files, channel and multiple programming scheme. Support program multiple sets of timing scheme, support the arbitrary optional execution terminal.
		10.Support arbitrarily set the terminal broadcast, intercom, monitoring, fire emergency recording, recording area and recording time, support timing recording and sub-period recording function.

S.No.	Item	Minimum Specifications
		11.Support fire radio, disassembled terminal, terminal line, terminal offline, the sound pressure detection trigger linkage, including the function of short circuit output, send emails, send messages, recording, pop prompt,terminal program broadcasting etc.
		12.Support users customize the audio stream network bandwidth utilization; maximal support 768 KBPS stream in order to meeting the demand of high quality audio playback, minimum support 8Kbps streams to solve the problem of insufficient network resources.
		13.Support VOIP telephone access, maximum 14 channels (optional); Support multiple sound card, multiple channel independent working mode, built-in 2 channel audio collection function;Support digital radio broadcast function
		14.Support audio terminal outside control power management, support timing to open and delay close, time can be set.
		15.Computers, smart phones, tablet and other terminals needn't install any user program, login system through browser, the new human-machine interaction interface, support 3D dynamic drag and drop operation, push real-time data.
		16.Integrated Air Play wireless technology, support all phones, tablets which with Air Play function , all can easy access to use, it has incomparable simple ease operability.
		17.The software supports third-party embedded development and provides standard MFC dynamic link library to realize integrating with other system platform, like Visitor Management System, CCTV, etc. , can provide standard documentation and DEMO programs of HTTP interface, for third party call development.
		18.The backup function ensures the system safety when main serve breaks down.
		19.Standard dual network interface, support exchange expansion mode and redundant backup mode, full speed rate up to 1000M, support cross-network segment and cross-routing mode
		20.Support primary and secondary server mode applications, secondary server hosting applications, support GPS matching NTP (timing) server calibration time.
		21.Support to control broadcast system through mobile APP.
		22.Equipped with standard interface: 1 * PS/2 interface;6 * serial port;1 * VGA;1 * HDMI, 8 * USB interface.
2	Audio source player	1.Standard rack-mounted 1U design, with black Aluminum.
		2.Built-in CD player, MP3, tuner & remote control,USB & SD inputs.
		3.AM/FM tuner each memory of 99 bands.
		4.One CD/MP3 stereo output and one tuner stereo output ;
		5.Remote control over music selection and volume control。
		6.Two florescent screens to display in English CD/MP3 and tuner separated.
		7.Eject, play, stop, play mode, prev, next, USB/SD & mute functional buttons for CD/MP3 player.
		8. AM/FM, ST/MON, MEO, Auto/Manual, Up, down & 1-6 number buttons for tuner.

S.No.	Item	Minimum Specifications
3	Paging mic	1.New desktop appearance design, 7" TFT true color screen, graphical operation interface, capacitive touch screen, easy operation and luxuriant beauty。
		2.Based on Luna cloud server, with very high security and reliability, support 7x24 hours work without interruption.
		3.With terminal management function, it's able to control the terminals which is under the management right, and it's able to check and manage the terminal current task and status.
		4.With two type of call methods: by microphone or headphone; it's suitable for different places.
		5.With multi reminder methods: ring tone, talking caller ID, light and message; support for one key answer, one key monitor, hands-free call and missed call message recording function.
		6.Support for programmable buttons, it can be configured as one key broadcast, one key intercom, one key meeting, one key music playing, one key SOS to satisfy different user demands.
		7.With built-in 2GByte SSD; support remote server management; support for background download under limited bandwidth and auto download when idle to reduce the network burden; media library files has the function of auto play when off line.
		8. Integrated with USB and Micro SD(TF) card interface, max support 4T USB storage device and 128G/SDXC card; Can play the music in USB, TF card and media library files to terminals which are under management right.
		9.Built-in 2W full frequency intercom speaker, with clear and loud sound; the projection microphone ensures the clear sound free from disturbance.
		10.With dual network interface, support exchange and extension mode and redundant backup mode;Full rate connection is up to 1000M; support for cross-segment and cross routing.
		11.2 short-circuit output, 2 short-circuit input, support for flexible user-defined function, to realize shortcircuit collect,alarm triggered, and linkage with the third party system such as fire system and monitor and etc.
		12.Support short-circuit trigger factory reset , convenient for system maintenance and management.
		13.AC power supply and zero switching time 24V DC backup power, to realize 7×24 hour working.
		14.Support background WEB status and information management.
		15.Support protocol：TCP/IP，UDP，IGMP，IETF SIP、Audio：MP3、WMA、WAV.
		16.Support remote firmware upgrade of terminals, no need local upgrade to terminal.
4	Monitor speaker	1.Professional wall mounted IP POE speaker, Based on Luna cloud server, with high safety and stability, support 7x24 uninterrupted operation.
		2.Built in with 2 * 30W amplifier module, to drive the built-in hi-fi speaker，soft and superior sound quality.

S.No.	Item	Minimum Specifications
		3.Built in with 2GByte SSD; support remote server management and downloading in background under limited bandwidth or automatic downloading in idle time, which can lighten the network burden, the files in media library can be played automatically in offline status
		4.With 1 AUX audio input, 1 group MIC input, 1 EMC emergency input; Built-in with digital preamplifier; support user-defined priority.
		5. Built-in 1 Line out independent audio output, to connect with external amplifier ; Support standard headphone interface, to realize audio monitoring, headset microphone amplification and etc.
		6. Support short circuit trigger to restore factory settings, which makes the system maintenance convenient to the greatest extent.
		7. AC power supply and zero switching time 24V DC backup power, to realize 7×24 hour working.
		9. Support protocol：TCP/IP，UDP，IGMP，IETF SIP 10. Support Audio Format：MP3, WMA, WAV
		10. Support background WEB status and information management.
		11.Support remote firmware upgrade of terminals, no need local upgrade to terminal.
5	Fire alarm panel	1. Standard 19" rack-mount design, 2U aluminum industrial panel.
		2. Based on Luna cloud server, with high safety and stability, support 7*24 uninterrupted operations.
		3. 30 fire alarm short-circuit signal input interfaces, it can be expanded input interface without limitation to meet bigger operation system.
		4. 30 fire alarm short-circuit signal output interfaces, it can be real-time connected with other related equipments.
		5.Support one key to restore factory settings, which makes the system maintenance convenient to the greatest extent.
		6. Wide voltage power supply + DC 24V backup power without time interval, to provide 7×24h power.
		7. Support background WEB status and information management.
		8. Support remote firmware upgrade of terminals, no need local upgrade to terminal.
6	Active speakers	1.Professional 15W IP POE column speaker, with integrated structure, good sealing performance of cabinet, full copper nickel plated earthing column with fast conducting,comply with the IP54 protection level certification requirements.
		2.Based on Luna cloud server, with high safety and stability, support 7*24 uninterrupted operations;
		3.Built in with 2GByte SSD; support remote server management and downloading in background under limited bandwidth or automatic downloading in idle time, which can lighten the network burden, the files in media library can be played automatically in offline status;
		4.Various network access methods, including DHCP automatic allocation access, ADSL intelligent dial access, fixed IP address access, etc.
		5.Integrated 24Bit professional sound card, can achieve a audiophile-level play, the highest audio stream is 768kpbs.

S.No.	Item	Minimum Specifications
		6.Built-in a network digital audio decoding module, support IP/TCP, UDP, IGMP (multi cast) and other communication protocols to achieve network transmission of 16 bit CD sound quality。
		7.The terminal is compatible with standard SIP protocol,and can access VOIP phone system (Aserisk and other mainstream IP-PBX) separately.
		8.Support one key to restore factory setting.
		9.Built in digital power amplifier module.
		10.Support remote firmware upgrade of terminals, no need local upgrade to terminal.
		11. DC 24V is optional.
		Specification:
		Network Interface: Standard RJ45 input
		Transmission Rate: 100Mbps
		Protocols: TCP/IP，UDP，IGMP（multicast）IETF SIP
		Audio Format: MP3、WMA、WAV
		Sampling Rate:8K～48KHz
		Frequency Response:130Hz～16KHz +1dB/-3dB
		Rated Power: 15W
		Total Harmonics Distortion:≤1%
		SNR: ≥65dB
		Protection: IP54
		Speaker Unit: 4”×1

5.11 Emergency Call Box (ECB) System

Overview

A high quality digital transceiver, to be placed at strategic locations determined by the BSCL. Key is to make it easily accessible by public. The unit shall have a button which when pressed, shall connect to the ICCC over the existing network infrastructure setup for ITMS project. These are to be placed only at a select locations such as CCTV field of view to avoid misuse and vandalism of the call box.

Scope of Work

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

a) MSI shall also install Emergency Call Box/Panic buttons at various locations (the final No. might vary based on field survey by MSI) in the city. These systems shall be deployed at identified junction for ease of access by citizens of BSCL city.
b) MSI, in consultation with BSCL can propose alternate locations apart from the locations mentioned in this RFP for installing ECB system where their effectiveness in communicating information about traffic conditions in BSCL will be maximized.
c) BSCL shall review and approve the proposed locations. MSI shall install ECB system on the approved locations.
d) ECB should have minimum following capabilities:

i. Construction: Cast Iron/Steel Foundation, Sturdy Body for equipment
ii. Call Button: Watertight Push Button, Visual Feedback for button press
iii. Speaker: To be used for Public Address System
iv. Connectivity: GSM/RF/PSTN/Ethernet as per solution offered
v. Sensors: For tempering/ vandalism
vi. Battery: Internal / External Battery with different charging options (Solar/Mains) with minimum backup of 60 Minutes.
vii. Power: Automatic ON/OFF operation with automatic power ON function after power failure.
viii. Casing: IP-55 rated for housing

5.12 Variable Message Sign boards

Overview

a) Central Control Software shall allow controlling multiple VMSB from one console.
b) Capable of programming to display all types of Message/ advertisement having alphanumeric character in English and Hindi and combination of text with pictograms signs. The system should have feature to manage video / still content for VMSB display.
c) The system shall have capability to divide VMSB screen into multi parts to display diverse form of information like video, text, still images, advertisements, weather info, city info etc.
d) The system shall also provide airtime management and billing system for paid content management
e) Capable of controlling and displaying messages on VMSB boards as individual/ group.
f) Capable of controlling and displaying multiple font types with flexible size and picture sizes suitable as per the size of the VMSB.
g) Capable of controlling brightness & contrast through software.
h) Capable to continuously monitor the operation of the Variable Message sign board, implemented control commands and communicate information to the Traffic Monitoring Centre via communication network.
i) Real time log facility – log file documenting the actual sequence of display to be available at central control system.
j) Multilevel event log with time & date stamp.
k) Access to system only after the authentication and acceptance of authentication based on hardware dongle with its log.
l) Location of each VMSB will be plotted on GIS Map with their functioning status which can be automatically updated.
m) Report generation facility for individual/group/all VMSBs 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.
n) Configurable scheduler on date/day of week basis for transmitting pre-programmed message to any VMSB unit.
o) Various users shall access the system using single sign on and shall be role based. Different roles which could be defined (to be finalized at the stage of SRS) could be Administrator, Supervisor, Officer, Operator, etc.
p) Apart from role based access, the system shall also be able to define access based on location.
q) Rights to different modules / Sub-Modules / Functionalities shall be role based and proper log report should be maintained by the system for such access
r) Components of the architecture must provide redundancy and ensure that there are no single points of failure in the key project components. To take

care of remote failure, the systems need to be configured to mask and recover with minimum outage.

s) The architecture must 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 Antivirus 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.

t) 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.

u) System shall use open standards and protocols to the extent possible

v) Facility to export reports to excel and PDF formats.

w) Remote Monitoring

   i. All VMSB shall be connected/configured to Traffic Monitoring system for remote monitoring through network for two way communication between VMSB and control Room to check system failure, power failure & link breakage.
   ii. Remote Diagnostics to allow identifying reason of failure up to the level of failed individual LED.

Scope of Work

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

a) Variable Message Sign Board (VMSB referred herein) shall be installed at identified strategic locations. The location of VMSB shall be on the key junctions (mostly on the sides without obstructing the traffic) and other strategic locations with large foot fall. The VMSB software application will allow user to publish specific messages for managing traffic and also general informative messages.

b) VMSB shall enable BSCL/Police to communicate effectively with citizens and also improve response while dealing with exigency situations. These shall also be used to regulate the traffic situations across the city by communicating right messages at the right time.

c) These displays can also be used for advertisement purposes. Approximately 20% to 30% of the total running time will be utilized by BSCL in day-to-day scenario (i.e. normal, non-emergency situations) for its own discretion whereas the remaining time can be used for advertisement purpose.

However during emergency or disaster situations, VMBS would be required to play messages issued by ICCC all the time till normal situation is restored.

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 VMSB should display text and graphic messages using Light Emitting Diode (LED) arrays.
d) The System should be 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 VMSB workstation at the ICCC should communicate with the VMS controller through the network. It should send out command data to the variable message sign controller and to confirm normal operation of the signboard. In return, the VMS workstation should receive status data from the VMS controller.
g) VMSB controllers should continuously monitor the operation of the VMS via the provided communication network.
h) Operating status of the variable message sign should be checked periodically from the ICCC.
i) It shall be capable of setting an individual VMSB or group of VMSB'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 VMSB or a group of VMSB'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 VMS or group of VMS's.
l) It shall also store information about the time log of message displayed on each VMS. The information stored shall contain the identification number of the VMS, 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 VMS. Data communication shall be provided with sufficient security check to avoid unauthorized access.

5.13 Variable Message Sign Board application

a) Central Control and Communication Software should allow controlling multiple VMS from one console.
b) Capable of programming to display all types of Message/ advertisement having alphanumeric character in English, Hindi, and combination of text with pictograms signs. The system should have feature to manage video / still content for VMS display.
c) The system should have capability to divide VMS screen into multi-parts to display diverse form of information like video, text, still images, advertisements, weather info, city info etc. The system should also provide airtime management and billing system

for paid content management

d) Capable of controlling and displaying messages on VMS boards as individual/ group.
e) Capable of controlling and displaying multiple font types with flexible size and picture sizes suitable as per the size of the VMS.
f) Capable of controlling brightness & contrast through software.
g) Capable to continuously monitor the operation of the Variable Message sign board, implemented control commands and communicate information to the ICCC via communication network.
h) Real time log facility – log file documenting the actual sequence of display to be available at central control system.
i) Multilevel event log with time & date stamp.
j) Access to system only after the authentication and acceptance of authentication based on hardware dongle with its log.
k) Location of each VMS will be plotted on GIS Map with their functioning status which can be automatically updated.
l) Report generation facility for individual/group/all VMSs 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.
m) Configurable scheduler on date/day of week basis for transmitting pre-programmed message to any VMS unit.
n) 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.
o) Apart from role based access, the system should also be able to define access based on location.
p) Rights to different modules / Sub-Modules / Functionalities should be role based and proper log report should be maintained by the system for such access
q) Components of the architecture must provide redundancy and ensure that there are no single points of failure in the key project components. To take care of remote failure, the systems need to be configured to mask and recover with minimum outage.
r) The architecture must 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 endeavor 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.
s) 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.
t) System shall use open standards and protocols to the extent possible
u) Solution shall be integrated with the environmental monitoring system for automatically displaying information from environmental sensors.
v) Facility to export reports to excel and PDF formats.

5.13.1 Remote Monitoring

All VMSB shall be connected / configured to ICCC for remote monitoring through network for two way communication between VMS and control Room to check system failure, power failure & link breakage.

a) Remote Diagnostics to allow identifying failure up to the level of failed individual LED.
   i. Minimum 3.0m length X 1.5m height X 0.2m depth. (3000mm x 1500mm X 200mm approx.)
   ii. Colour LED: Full Colour, class designation C2 as per IRC/EN 12966 standard
   iii. Luminance Class/Ratio: L3 as per IRC/EN 12966 standards.
   iv. Luminance Control & auto Diming
   v. Should be automatically provide different luminance levels but shall also be controllable from the traffic centre using software.
   vi. Auto dimming capability to adjust to ambient light level (sensor based automatic control)

b) Photoelectric sensor shall be positioned at the sign front or sign rear to measure ambient light. Capable of being continually exposed to direct sunlight without impairment of performance.
   i. Contrast Ratio: R3 as per IRC/EN 12966 standard
   ii. Beam Width: B6+ as per IRC/EN12966 standards.
   iii. Pixel Pitch: 12mm or better

c) Picture Display
   i. At least 300mm as per IRC /EN 12966 standards
   ii. Full Matrix: Number of lines & characters adjustable, active area: 2.88mX1.2m at-least
   iii. Synchronized Dot to Dot display.
   iv. Capable of displaying real time message generated by ICCC.
   v. Special frontal design to avoid reflection.
   vi. Display shall be UV resistant
   vii. Viewing Angle: B6+ as per IRC/EN12966 standard- Viewing angle shall ensure message readability for motorists in all lanes of the approach road
   viii. Viewing Distance: Suitable for readability from 100 Mtrs. or more at the character size of 240mm, from moving vehicles.

d) Self-Test
   i. VMS shall have self-test diagnostic feature to test for correct operation.
   ii. Display driver boards shall test the status of all display cells in the sign even when diodes are not illuminated.
   iii. All periodic self-test results shall be relayed to the ICCC in real time to update the status of the VMS

5.13.2 Alarms

a) Door Open sensor to Inform Control room during unauthorized access
b) LED Pixel failure detection alarm
c) Flicker: Refresh Frequency should not be less 90 Hz. No visible flicker to naked eye.

d) Multiple Data Communication interface/Port: RJ45 Ethernet, RS232, RS 485, FC port and any other suitable
e) Communication (connectivity): Wired & GPRS based wireless technology with 3G upgradable to 4G capability.
f) Ambient Operating Temperature: should be capable of working in ambient temperature of city requirement
g) Humidity (RH): Operating ambient humidity: 10% - 95% Rh or better.
h) Protection against Pollution/dust/water: Complete VMS should be of IP 65 protection level from front and IP54 from side and rear. As per EN60529 or equivalent Standard.

5.13.3 Power

a) Protection for overvoltage/ fluctuation/drop of the nominal voltage (50%) shall be incorporated.
b) The enclosure shall contain at least two 15 Amp VAC (industrial grade) outlet socket for maintenance purpose.
c) Power Back-up & its enclosure: UPS for one hour power back-up with auto switching facility. The enclosure of UPS and battery should be pole mountable with IP 65 protected housing and lockable.
d) Batteries with solar charging options can also be provided as back up
e) Material for VMS frame: at least 2mm aluminium or Non-corrosive, water resistant or better. Frame of the VMS should be black & Powder coated.
f) Mounting, Installation and finishes
g) Mounting structure shall use minimum 6Mtrs. High Cylindrical GI Pole (Class B) or suitable structure with 5.5 mtr. Minimum vertical clearance under the VMS sign from the Road surface.
h) The mounting shall be capable of withstanding road side vibrations at site of installation.
i) It shall be provided with suitable walkway for maintenance access.
j) The side interior and rear of enclosures shall be provided in maintenance free natural aluminium finish. All enclosure shall be flat and wipe clean.
k) Rugged locking mechanism should be provided for the onsite enclosures and cabinets.
l) For Structural safety, the successful bidder has to provide structural safety certificate from qualified structural engineers approved/ certified by Govt. Agency.
m) Wind Load: WL9 as per EN12966 to withstand high wind speeds and its own load.
n) Cabling, connections and Labelling
o) All cable conductors shall be of ISI marked for quality and safety. It shall be of copper insulated, securely fastened, grouped, wherever possible, using tie warps approximately every 10-20 Cms or cable trays.
p) All connections shall be vibration-proof quick release connections except for power cables terminating in terminal blocks, which shall be screwed down.
q) All terminal block shall be made from self- extinguishing materials. Terminations shall be logically grouped by function and terminals carrying power shall be segregated from control signal terminals.
r) All cables shall be clearly labelled with indelible indication that can clearly be identified by maintenance personnel using “As built: drawings”.

s) Lightening arrester shall be installed for safety on each VMS.
t) The successful bidder has to provide safety certificate from qualified Electrical engineers approved/certified by Govt. Agency.
u) Local Storage in VMS: Embedded VMS controller should be capable to store at-least 100 messages and symbols/pictograms to allow display to run in isolated mode on a predefined structure/timings, in case of connectivity failure.

5.14 Smart Parking Management System (SPMS)

Smart Parking solution will involve the use of near-to-real-time data and applications that allow users to monitor available or unavailable parking slots. The goal is to automate and decrease time spent manually searching for the optimal parking area and even slot. Solution will encompass a complete suite of services such as online payments, parking time notifications and even car searching functionalities for very large lots. A parking solution will greatly benefit both the user and the lot owner.

Functional Requirements:

a) The smart parking solution is envisaged for both closed parking lots and open parking lots.
b) Indoor Parking Spaces- Such parking spaces are managed through sub contracted vendors and the parking lots have boundary walls, closed terrace and a defined entry and exit points.
c) Outdoor Parking Spaces- Such locations are managed through sub contracted vendors and have a boundary wall and defined entry and exit points. These kind of parking spaces have specified number of slots available, typically on an open ground or road.
d) On street Parking Spaces- Such locations are managed through sub contracted vendors and do not have a boundary wall and defined entry and exit points. These kind of parking spaces have specified number of slots available, typically on an open ground or road.
e) Solution must geo-reference all the parking lots and shall have the ability to add more locations in future.
f) Solution should be able to tally the entry and exit car counts and calculate the available parking in that parking structure.
g) Solution may use video camera based analytics or other sensor based solutions to determine number of vehicles entering and exiting parking lots. The smart parking solution should do so at each floor, in case of multilevel parking and communicate the data.
h) Solution shall also include provision to capture image of vehicle including license plate number of every vehicle entering and leaving any of the parking spaces and the all the information related to the same shall be stored at a central server.

Bhagalpur City will have two solutions for below mentioned two different scenarios:

a) For Closed Ground or Multilevel Car parking:
   - All parking slots will be earmarked with proper numbering.
   - Boom-barriers at Entry & Exit

- Real-time information of particular parking slot availability through Mobile App.
- Driver can book parking slot through App or at counter.
- App will have online Pre-paid option only.
- App based and Display board based guiding to booked slot.
- Driver has to park vehicle at designated slot only, otherwise penalty.
- ANPR & CCTV based monitoring / surveillance.
- Actual Parking amount or wrong parking penalty will be charged while exit.
- Provision for Monthly/periodic Parking slot booking.

b) For Open On-Street Parking :

- All parking slots will be earmarked with proper numbering.
- Real-time information of number of free parking slots through Mobile App.
- App based and Display board based guiding to Parking area.
- Parking slot will be allotted by attendant while parking, slot will be blocked in App by attendant.
- Driver has to park vehicle at designated slot only, otherwise penalty.
- CCTV based surveillance.
- Actual Parking amount or wrong parking penalty will be charged while exit.
- Once, the slot is vacated, attendant will update in App.

Based on the above solution, MSI shall provide the software solution with below features:

i. Mobile App to help in finding parking space quickly & easily
ii. Finding parking space with clear & simple directions reducing traffic congestion.
iii. Correct detections of violations & suspicious parking/over duration parking
iv. Availability of data & Analysis for growing need for expansion or more parking slots; subsequently required measures to handle problem
v. The application should have citizen module and officer module.
vi. The citizen should be able to see all the parking lots with exact available space in a real time mode.
vii. While locating nearest parking lot, the most updated parking slot availability should be given to the user.
viii. Through the citizen module, the user should be able to locate nearest parking lot and also pre–book based on his geographical coordinates. The same information must be made available on map with routing information.
ix. The administrators/key users should be able to generate MIS report to view occupancy, collection and other usage statistics over a defined time period.
x. Real-time Monitoring and Dynamic MIS Reporting
xi. Reports shall be available in all standard acceptable formats like .csv, .pdf, .txt, etc.
xii. The Citizen App and Web Portal shall have module for Parking Solution. Solution should optimally make parking data available to a smart phone application that citizens might use to get real time parking availability.

xiii. Solution shall have capability to automatically capture details of the license plates of the vehicles at every entry and exit of each parking lot.
xiv. System shall include central reporting system establishing the connection between the devices and sensors, and the ICCC.
xv. Total number of slots and free slots for parking must be displayed on a digital signboard, Mobile App, Web portal etc.
xvi. Solution should report occupancy of parking lots to a central software application deployed at the Integrated Command and Control Center.
xvii. Solution should enable BSCL to obtain real time situational awareness about the occupancy of parking lot through smart dashboard.
xviii. Solution should enable citizens to obtain real time space availability
xix. Solution shall include reporting dashboards with location specific thresholds to be set for generating customized reports
xx. Solution shall be capable of monitoring the number of vehicles that entered or exited the parking premises during any given time
xxi. The smart parking solution should retain videos of car entering /exiting the parking zone as per the security parameters defined by BSCL
xxii. Solution should enable accounting and mapping of individual parking spots. There should be a provision to increase or decrease the number of parking spaces that can be reserved online through web client or mobile App, and same must reflect on web clients or mobile apps.

Smart Parking Solution - Key Components

a) Web Portal and Mobile App for Public

i. Connected to central web-server
ii. Receive parking slot information from central web-server
iii. Display the real-time monitoring of parking slots state in the nearest parking zone

b) Control and command center

i. Integration with ICCC system
ii. Data management, analytics and Business Intelligence on real time basis
iii. Monitoring of real time transactions, parking availability
iv. Management of Equipment status and alarms on real time basis
v. Dash boards and reports

c) Central Web-Server

i. Receive parking slot information on real time updates
ii. Display the parking slots state of parking zone in real-time
iii. Send information to mobile phone application
iv. Save information in database
v. Reporting & analytics

d) Digital Display Unit

i. Shall receive information from the Parking Information System and operate accordingly

5.15 Environmental Management System

Functional Requirement of EMS

S.No.	Description
1.	Shall be ruggedized enough to be deployed in open air areas on streets and park
2.	Environmental Sensor station shall be housed in a compact environmentally rated outdoor enclosure. It shall be an integrated module which shall monitor overall ambient air, noise quality, weather etc.
3.	Mounting of the environmental sensor module shall be co-located on streetlight pole or shall be installed on a tripod/standalone pole.
4.	Environmental sensor station shall monitor following parameters and include the following integrated sensors inside one station: ▪ Carbon Monoxide (CO) sensor ▪ Ozone (O3) sensor ▪ Nitrogen Dioxide (NO2) sensor ▪ Sulphur Dioxide (SO2) sensor ▪ Carbon Dioxide (CO2) sensor ▪ Particulate/SPM Profile (PM10, PM2.5, and TSP) sensor ▪ Temperature sensor ▪ Relative Humidity sensor ▪ Wind Speed sensor (Can be in same or separate enclosure) ▪ Wind Direction sensor (Can be in same or separate enclosure) ▪ Rainfall sensor (Can be in same or separate enclosure) ▪ Barometric Pressure sensor; and ▪ Noise sensor.
5.	Solution shall display trends of environmental parameters based on user specific time periods.
6.	Data shall be collected in a software platform that allows third party software applications to read that data.
7.	Solution shall display real time and historical data in chart and table views for dashboard view of the Client.
8.	Alarms shall be generated for events where the environmental parameters breaches the safe or normal levels.
9.	The sensor management platform shall allow the configuration of the sensor to the network and also location details etc.
10	▪ It shall comprise of an Industrial PC running latest version OS and compatible software. ▪ Data logging with central Monitoring System will be through GPRS/TCP-IP from all the AAQMS and MMS system and shall have an ability to program and log channels at different intervals and shall have a capability of averaging and displaying real time data and averaged data over a period of 1 min, 10 min, 30 min, 1 hr, 4 hr, 8, hr, 24 hr and so on. ▪ Real time or averaged data can be viewed quickly and easily through a remote interface on the central computer. ▪ System shall be able to perform nested calculations vector averaging and rolling averages.

S.No.	Description
	▪ It shall have a feature for viewing instantaneous and historical data in the form of tables and graphs either locally or from a remote client. ▪ Data retrieval from CMS via USB and DVD shall be possible. ▪ Generation of reports for pollution load, wind rose etc. ▪ Alarm annunciation of analyzer/sensor in abnormal conditions.
11	▪ The environment sensors shall be integrated with the command control system to capture and display/ provide feed. The data it collects is location-marked. ▪ Various environment sensors shall sense the prevailing environment conditions and send the data to the integrated control system where real time data resides and the same shall be made available to various other departments and applications for decision making. ▪ Information shall be relayed to signage – large, clear, digital-display screens which let citizens know regarding the prevalent environmental conditions. ▪ Further environmental sensors recorded data shall be used by Mobile application to enable user for alarm management and notification of environmental details on real time basis.

Technical Requirement of Environment Management Sensors

S.No.	Description
1.	**Carbon Monoxide (CO) Sensor** ▪ CO sensor shall measure the carbon monoxide in ambient air ▪ Range of CO sensor shall be between 0 to 31 ppm ▪ Resolution of CO sensor shall be 100ppb or better ▪ Lower detectable limit of CO sensor shall be 0.040 PPM or better ▪ Precision of CO sensor shall be less than 3% of reading or better ▪ Linearity of CO sensor shall be less than 1% of full scale or better ▪ Response time of CO sensor shall be less than 60 seconds ▪ Operating temperature of CO sensor shall be 0°C to 60°C ▪ Operating pressure of CO sensor shall be ±10%.
2.	**Ozone (O3) Sensor** ▪ O3 Sensor shall measure the ozone in ambient air ▪ O3 Sensor shall have a range of at least 0-400 PPB ▪ Resolution of O3 sensor shall be 10ppb or better ▪ Lower detectable limit of O3 sensor shall be 0.001 PPM or better ▪ Precision of O3 sensor shall be less than 2% of reading or better ▪ Linearity of O3 sensor shall be less than 1% of full scale ▪ Response time of O3 sensor shall be less than 60 seconds ▪ Operating temperature of O3 sensor shall be 0°C to 60°C ▪ Operating pressure of O3 sensor shall be ±10%
3.	**Nitrogen Dioxide (NO2) Sensor** ▪ NO2 Sensor shall measure the Nitrogen dioxide in ambient air ▪ NO2 Sensor shall have a range of at least 0-300ppb ▪ Resolution of NO2 sensor shall be 10ppb or better ▪ Lower detectable limit of NO2 sensor shall be 0.001 PPM or better ▪ Precision of NO2 sensor shall be less than 3% of reading or better ▪ Linearity of NO2 sensor shall be less than 1% of full scale ▪ Response time of NO2 sensor shall be less than 60 seconds ▪ Operating temperature of NO2 sensor shall be 0°C to 60°C

S.No.	Description
	▪ Operating pressure of NO2 sensor shall be ±10%
4.	**Sulfur Dioxide (SO2) Sensor** ▪ SO2 Sensor shall measure the Sulfur dioxide in ambient air ▪ SO2 Sensor shall have a range of at least 0-700ppb ▪ Resolution of SO2 sensor shall be 10ppb or better ▪ Lower detectable limit of SO2 sensor shall be 0.009 PPM or better ▪ Precision of SO2 sensor shall be less than 3% of reading or better ▪ Linearity of SO2 sensor shall be less than 1% of full scale ▪ Response time of SO2 sensor shall be less than 60 seconds ▪ Operating temperature of SO2 sensor shall be 0°C to 60°C ▪ Operating pressure of SO2 sensor shall be ±10%
5.	**Carbon Dioxide (CO2) Sensor** ▪ CO2 Sensor shall measure the carbon dioxide in ambient air ▪ CO2 Sensor shall have a range of at least 0-5000 PPM ▪ Resolution of CO2 sensor shall be 1 PPM or better ▪ Lower detectable limit of CO2 sensor shall be 10 PPM or better ▪ Precision of CO2 sensor shall be less than 3% of reading or better ▪ Linearity of CO2 sensor shall be less than 2% of full scale ▪ Response time of CO2 sensor shall be less than 60 seconds ▪ Operating temperature of CO2sensor shall be 0°C to 60°C ▪ Operating pressure of CO2 sensor shall be ±10%
6.	**Particulate Profile Sensor** ▪ Particulate profile sensor shall provide simultaneous and continuous measurement of PM10, PM2.5, SPM and TSP (measurement of nuisance dust) in ambient air ▪ Range of PM2.5 shall be 0 to 230 micro gms / cu.m or better ▪ Range of PM10 shall be 0 to 450 micro gms / cu.m or better ▪ Lower detectable limit of particulate profile sensor shall be less than 1 µg/m3 ▪ Accuracy of particulate profile sensor shall be <± (5 µg/m3 + 15% of reading) ▪ Flow rate shall be 1.0 LPM or better ▪ Operating temperature of the sensor shall be 0°C to 60°C ▪ Operating pressure of the sensor shall be ±10%
7.	**Temperature Sensor** ▪ Temperature sensor shall have the capability to display temperature in °Celsius ▪ Temperature range shall be -10° to +50°C ▪ Sensor accuracy shall be ±0.3°C (±0.5°F) or better ▪ Update interval shall be 1 Minute
8.	**Relative Humidity Sensor** ▪ Range of relative humidity sensor shall be 1 to 100% RH ▪ Resolution and units of relative humidity sensor shall be 1% or better ▪ Accuracy of the sensor shall be ±2% or better ▪ Update interval shall be less than 60 seconds ▪ Drift shall be less than 0.25% per year
9.	**Wind Speed Sensor** ▪ Wind speed sensor shall have the capability of displaying wind speed in km/h or knots ▪ Range of sensor shall be 0-60 m/s ▪ Accuracy of wind speed sensor shall be ±5% or better ▪ Update interval shall be less than 60 seconds

S.No.	Description
10.	**Wind Direction Sensor** ▪ Range of the wind direction sensor shall be 0° to 360° ▪ Display resolution shall be 16 points (22.5°) on compass rose, 1° in numeric display ▪ Accuracy shall be ±3% or better ▪ TR 6.70 Update interval shall be 2.5 to 3 seconds
11.	**Rainfall Sensor** ▪ Rainfall sensor shall the capability of displaying level of rainfall in inches and millimeter ▪ Daily Rainfall range shall be 0 to 99.99" (0 to 999.8 mm) ▪ Monthly/yearly/total rainfall range shall be 0 to 199" (0 to 6553 mm) ▪ Accuracy for rain rates shall be up to 4"/hr (100 mm/hr) or ±4% of total ▪ Update interval shall be 15 Min or less. ▪ 0.02" or (0.5mm) of rainfall shall be considered as a storm event with 24 hours without further accumulation shall end the storm event
12.	**Barometric Pressure Sensor** ▪ Barometric pressure sensor shall have the capability of displaying barometric pressure in Hg, mm Hg and hPa or mb ▪ Range of barometric pressure sensor shall be 540 hPa or mb to 1100 hPa or mb ▪ Elevation range of the barometric pressure sensor shall be -600 m to 4570 m ▪ Uncorrected reading accuracy shall be ±1.0 hPa or mb at room temperature or better ▪ Equation source of the sensor shall be Smithsonian Meteorological tables ▪ Equation accuracy shall be ±0.01" Hg (±0.3 mm Hg, ±0.3 hPa or mb) or better ▪ Elevation accuracy shall be ±10' (3m) to meet equation accuracy specification or better. ▪ Overall accuracy shall be ±0.03" Hg (±0.8 mm Hg, ±1.0 hPa or mb) or better. ▪ TR 6.85 Update interval shall be less than 60 seconds
13.	**Noise Sensors** ▪ Noise sensor shall detect the intensity of the ambient sound in a particular area ▪ Noise Sensors shall be installed for the outdoor applications ▪ Noise sensor shall be able to identify the areas of high sound intensity ranging from 30 dBA to 120 dBA ▪ Noise sensor shall have resolution of 0.1 dBA
14.	Integration with ICCC solution, VMSB, Portal and Mobile applications
15.	Conditions-Ruggedized enough to be deployed in open air areas on streets and park

5.16 Trenching using HDD/ Optical Fibre Cable

5.16.1 Specification of Permanently Lubricated HDPE Pipe

HDPE pipe shall be suitable for underground fibre optic cable installation by blowing as well as conventional pulling and should be free from the risk/damage caused by Rodents.
Construction(Two layer)

The HDPE pipe shall have two concentric layers viz. outer layer and inner layer. The outer layer shall be made of HDPE material and the inner layer of solid permanent lubricant. These concentric layers shall be co-extruded and distinctively visible in cross-section under normal lighting conditions and generally conform to IS-9938. The color of HDPE pipe shall be uniform

throughout. In the finished HDPE pipe, the co-extruded inner layer of solid permanent lubricant shall be continuous and integral part with HDPE outer layer and preferably be white in color. The inner layer of solid permanent lubricant shall not come out during storage, usage and throughout the life of the pipe. The pipe shall be supplied in a continuous length of 1000 meter in coil form, suitable for transportation, installation and handling purposes.

Standards

The HDPE pipe shall conform to the following standard and the technical specifications described as under:-

A. IS: 4984 - Specification for HDPE pipe.

B. IS: 2530 - Method for tests for polyethylene moulding materials and compounds.

C. IS: 9938 -Recommended colours for PVC insulation for LF wires and cables.

D. TEC-spec no -HDPE pipe for use as duct for G/CDS-08/01 optical fibre cable.

E. IS: 7328 - HDPE material for moulding and extrusion.

F. ASTM D 1693 - Test method for environmental stress cracking of ethylene plastics.

G. ASTMD 1505 - Test method for density.

H. ASTMD 3895 - Method for Oxidation Induction test.

Material

The raw material used for the HDPE pipe shall meet the following requirements:-

(i) the anti-oxidant establishers, colour master batch and other additive used shall be physiologically harmless and shall be used only to minimum extent necessary to meet the specification.

(ii) Usage of any additives used separately or together should not impair the long-term physical and chemical properties of the HDPE pipe.

(iii)Suitable Ultra-Violent stabilizers may be used for manufacture of the HDPE pipe to protect against UV degradation when stored in open for a minimum period of 8 months.

(iv)The base HDPE resin used for manufacturing outer layer of pipe shall conform to any grade of IS-7328 or to any equivalent standard meeting the following requirement when tested as per standards referred in Clause 1.3.1 below.

Density 940 to 958 kg/m3 at 27o C

Melt Flow Rate 0.12 - 1.1g/10 minutes at 190oC & 5kg load

(v) In case of HDPE pipe of two concentric layer construction, the friction reducing, polymeric material to be used as the inner layer lubrication material shall be integral with HDPE layer. The lubricant materials shall have no toxic or dramatic hazards for safe handling.

Tests on Material of HDPE pipe

(i) Melt Flow Index and Density: The base HDPE resin material shall be tested for its melt flow index as per IS:2530 and density as per standard ASTM D 1505.

(ii) Oxidant Induction Test: The oxidation induction test on base HDPE resin shall be conducted as per ASTM D 3895 and the oxidation induction time shall be >/= 30 minutes.

Dimensions of HDPE Pipe with co-extruded copper wire shall be as under:

a) Outside diameter	:	50 mm +0.4 mm - 0.0 mm
b) Wall thickness	:	3.5 mm + 0.2 mm
c) Standard length	:	1000 + 100 metres
d) Copper Wire Diameter	:	1.22 mm +/- 0.02
e) Copper Wire Resistance	:	< 15.0 Ohms/Km. at 27 deg. C.
f) Web Strength	:	> 300 Kgs/10 cm
g) Web Thickness	:	> 1.5 mm
h) Thickness of Permanent Lubricant Layer	:	> 0.4 mm

Permanent Lubricated (Per Lub) HDPE Pipes should be sourced from the manufacturer with ISO 9000 accredited manufacturing facility. Per Lub HDPE Pipes should be should be sourced from the manufacturer having valid Type Approval Certificate from DOT as per the latest TEC Specs and its amendments thereof.

Accessories

The following accessories are required for jointing the pipe and shall be supplied along with the pipe. The manufactures shall provide complete design details, procedure for method of installation and type of the material used for the accessories.

(i) Plastic coupler: The coupler shall be used to join two HDPE pipes. The coupling shall be able to provide a durable water tight joint between two pipes without deteriorating the strength of the pipes. The strength of coupler shall match the primary strength of the HDPE pipe. It should be push fit type. Threaded coupler is not acceptable. The jointing shall meet the air pressure test of 15 kg/cm2 for a minimum period of 2 hours without any leakage.

(ii) End plug: This shall be used for sealing the ends of empty pipe, prior to installation of FO cable and shall be fitted immediately after laying of the HDPE pipe, to prevent entry of any unwanted elements such as dirt, water, moisture, insects/rodents etc.

(iii) Cable sealing plug: This is used to hold the cable and prevent entry of any unwanted elements, as specified above.

(iv) End cap: This cap is made of hard rubber, shall be fitted with both ends of HDPE pipe to prevent the entry of any unwanted elements such as dirt, water, moisture, insects/rodents during transportation and storage.

OSP Fiber Optic Cable

The optical fiber proposed is an all Dielectric Gel-Free lightweight Single Mode as well as Multi-mode Fiber Optic cables designed for duct installation for backbone and access respectively. FOC shall provide full-spectrum availability for optical transmission systems operating over the entire wavelength range from 1260 nm to 1625 nm.

5.16.2 Technical Specifications of Single Mode Optical Fibre Cable

Cable Construction

Strength Member

The duct placement cables shall have a non-metallic central strength member covered by a suitable coating. The cable shall be designed with sufficient strength members to meet installation and service conditions so that the fibres are not subject to excessive strain.

Colour Coding

Loose tubes shall be individually coloured for ease of identification. Individual fibres shall also be colour coded. Fibre colours shall be as follows:-

Blue, orange, green, brown, grey, white, red, black, yellow, violet, pink, turquoise.

The tube colouring shall follow the same colour code. Fillers shall be of natural colour to fill up the cable core.

Cable Sheath Layers

The cable core shall be covered with a seamless black sheath mask of U.V. stabilised weather resistant polyethylene incorporating a moisture barrier (swellable components). The outer sheath excluding moisture barrier shall have a minimum thickness of 0.5 mm. The cable sheath shall be printed in yellow with a suitable legend to be agreed between the Contractor and the SALCAB Project Manager. The sheathing method including control measurements shall be fully described. In particular the cable diameter measurement, high voltage testing, printing and take-up on drum shall be described.

Table 6: Fiber Mechanical Characteristics

Fibre count	48	96	144
Fibre count in tube	4	12	12
Min. bending radius during installation (mm) －installed (mm) Tensile load －Short term(N) －Long term(N) Crush load(N/10cm) Applicable Temp. range －Operation －Installation	240 120 3000 1500 1000 -40~+70 -20~+60	240 120 3000 1500 1000 -40~+70 -20~+60	240 120 3000 1500 1000 -40~+70 -20~+60

Table 7: Fiber Parameters and Values

Parameters		**Values**
Mode Field Diameter	- range	9.2 +/- 0.4 um
	- deviation	+/- 10%
Attenuation	1285-1330nm1550nm	< / = 0.34 dB/km < /=0.20 dB/km
Attenuation Uniformity	Point or Step Defect Extended variations	< 0.1dB < 0.1dB
Temperature variation of attenuation from 0 Degree Celsius to 65 Degree Celsius	1300nm 1550 nm	< 0.05dB/km < 0.05dB/km
Dispersion	1285-1330 nm 1270-1340 nm 1550 nm	< 3.5 ps/nm.km < 6.0 ps/nm.km < 18 ps/nm.km
Mode cut off wavelength (of a primary coated fibre as Rec. G.652)		< /=1260 nm
Reference surface diameter		125 +/- 0.7um
Core / Cladding concentricity		< 0.6 um
Class non circularity (%)	Core Reference surface	<6 <2
Coating diameter		242 +/- 5um
Proof test (%)		>1.0
Macro bend test (dB) 60mm diameter mandrel, 100 turns, loss increase at 1550nm		< 0.2

Splice Loss

The maximum acceptable splice loss is 0.15dB at 1500nm. The average splice loss taken in one direction on each route shall not exceed 0.1 dB at 1500nm.

Splice/Joint closures and Manholes

Fiber joint closures or Splice closures are required to join sequential cable and fiber lengths together, or provide a function for distribution of smaller drop cables. The splice closures would be located based on the length of the fiber being supplied and the No. of cuts being envisaged during the span of next 20 yrs. Manholes provide accessible space in an outside plant pathway system for the pulling, placing, and splicing (Mid Span) of cables. Manholes are also used to segment the pathway system into lengths compatible with standard reel lengths for outside plant cable and to conform to maximum pathway lengths as defined in the TIA/EIA standards. Manholes would be placed at every 1000 m distance.

Manholes should be constructed in such a way that they are capable of supporting the heaviest anticipated street traffic weight, even though all manholes should be located under the pavement. Include reasonable measures such as cable glands, rodent protection foams etc. for the purpose of water proofing and protection from pests. Provide sufficient cable supports or cable racks to be able to manage the maximum designed capacity of OFC.

Typical Manhole dimensions 1600(L)x1250(W)x1000(D) (+/-10% variation is allowed for Length &Width only)

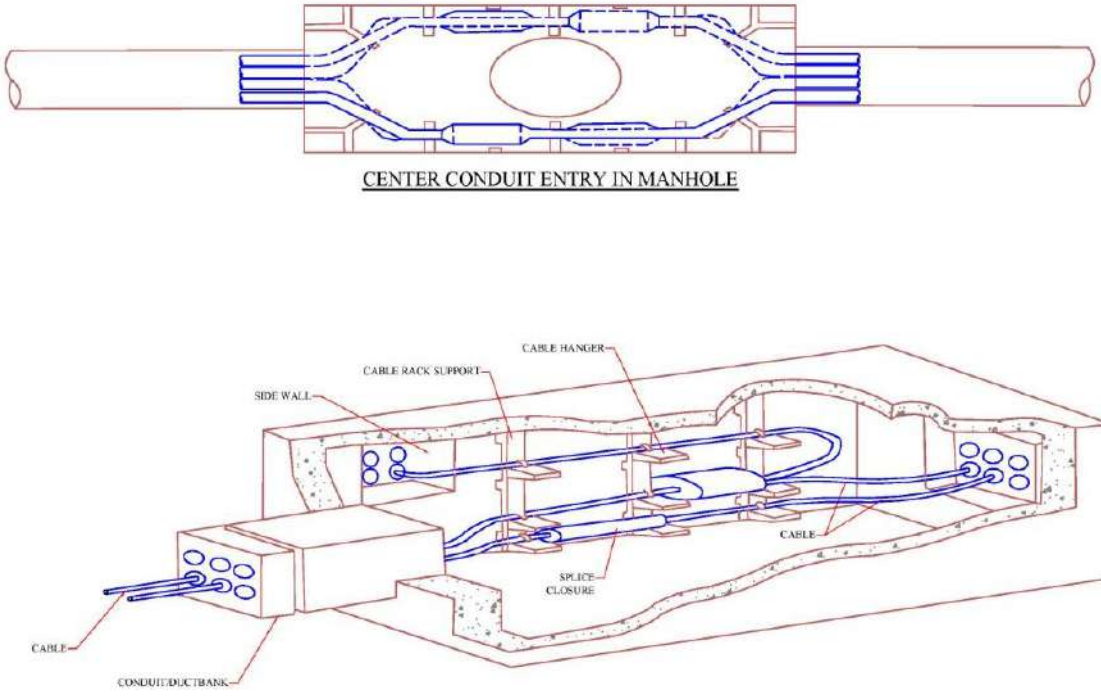


Figure 6: Typical Manhole Dimensions

5.17 Scope of Integration

MSI has to integrate all the existing and upcoming solutions available in city with respect to use cases through API and other method for seamless integration and the effective decision management perspective as mentioned below but not limited to:

a) Smart Lighting
b) ICT Enabled Solid Waste Management
c) Intelligent Transportation System
d) E-Challan System
e) Public Bike Sharing
f) Smart Water Supply System
g) Smart Education
h) Smart Health Management System
i) e-Municipality
j) SCADA
k) Smart Road Network
l) eBuses Live Tracking and Monitoring System
m) eToilet Monitoring System
n) ICT component of eLibrary System
o) ICT component of Smart Bus Stop System
p) Any other upcoming solutions

District level ICCCs will be integrated with Patna ICCC for sharing the City Dashboard and major analytics. The Software for Integration would be centrally provided at Patna and the same software would be utilized by the District level ICCCs. The MSIs of the District level ICCCs would coordinate with the MSI for Patna Smart City for proper utilization and implementation of the Software at their locations and also for seamless integration of all the ICCCs.

6 SOW For Integrated Traffic Management System (ITMS)

6.1 Overview

6.1.1 Key Components of Adaptive Traffic Control System (ATCS)

a) **Traffic Signal Controller**

i. The Traffic Signal Controller equipment is a 32 bit or 64 bit microcontroller with solid state traffic signal lamp switching module with the ability to program any combination of traffic signal stages, phases and junction groups. The controller will ideally have a conflict monitoring facility to ensure that conflicting, dangerous are pre-flagged at the programming stage and these are disallowed even during manual override phase.

ii. The Traffic Signal Controller will be adaptive so that it can be controlled through the central traffic control Centre as an individual junction or as part of group of traffic junctions along a corridor or a region. The signal controller design must be flexible for the junction could be easily configured to be part of any corridor or group definition and could be changed through central command controller easily

iii. Site specific configuration data shall be stored in a non-volatile memory device (FLASH memory) easily programmable at the site through keypad or laptop. A minimum of 512KB flash memory and 128KB RAM shall be provided. Volatile memory shall not be used for storing the junction specific plans or signal timings.

iv. All timings generated within a traffic signal controller shall be digitally derived from a crystal clock which shall be accurate to plus or minus 100 milliseconds.

v. The controller shall provide a real time clock (RTC) with battery backup that set and update the time, date and day of the week from the GPS. The RTC shall have minimum of 7days battery backup with maximum time tolerance of +/- 2 sec per day.

vi. The controller shall have the facility to update the RTC time from ATCS serveror GPS receiver and through manual entry.

vii. The traffic signal system including controller shall have provision audio output tones and should be disabled friendly for.

viii. The controller shall be capable of communicating with the ATCS server through Ethernet on a managed leased line network or any other appropriate stable communication network.

- **Traffic Signal Controller Operating Parameters**

i. Phases- The controller shall have facility to configure 32 Phases either for vehicular movement, filter green, indicative green, pedestrian movement or a combination thereof.

ii. It shall be possible to operate the filter green (turning right signal) along with a vehicular phase. The filter green signal shall flash for a time period equal to the clearance amber period at timeout when operated with a vehicular phase.

iii. The pedestrian phase signal shall be configured for flashing red or flashing green aspect during pedestrian clearance.

iv. It shall be possible to configure any phase to the given lamp numbers at the site.
v. Stages – The controller shall have facility to configure 32 Stages.
vi. Cycle Plans – The controller shall have facility to configure 24 Cycle Plans and the Amber Flashing / Red Flashing plan. It shall be possible to define different stage switching sequences in different cycle plans. The controller shall have the capability for a minimum of 32 cycle-switching per day in fixed mode of operation.
vii. Day Plans – The controller in coordination with ATCS server shall have facility to configure each day of the week with different day plans. It shall also be possible to set any of the day plans to any day of the week. The controller shall have the capability to configure 20 day plans.
viii. Special Day Plans – The controller shall have facility to configure a minimum of 20 days as special days in a calendar year.
ix. Starting Amber – During power up the controller shall initially execute the Flashing Amber / Flashing Red plan for a time period of 3 Seconds to 10 Seconds. The default value of this Starting Amber is 5 Seconds. Facility shall be available to configure the time period of Starting Amber within the given limits at the site.
x. Inter-green – Normally the inter-green period formed by the clearance Amber and Red extension period will be common for all stages. However, the controller shall have a facility to program individual inter-green period from 3 Seconds to 10 Seconds.
xi. Minimum Green – The controller shall allow programming the Minimum Green period from 5 Seconds to 10 Seconds without violating the safety clearances. It should not be possible to pre-empt the Minimum Green once the stage start commencing execution.
xii. All Red – Immediately after the Starting Amber all the approaches should be given red signal for a few seconds before allowing any right of way, as a safety measure. The controller shall have programmability of 3 Seconds to 10 Seconds for All Red signal.
xiii. Signal lamps monitoring – The controller shall have inbuilt circuitry to monitor the lamp status
xiv. Green – Green Conflict Monitoring – The controller shall have a facility to list all conflicting phases at an intersection. The controller should not allow programming of these conflicting phases in a Stage. A hardware failure leading to a conflict condition (due to faulty devices or short circuit in the output) shall force the signal into Flashing Amber / Flashing Red.
xv. Cable less Synchronization – It shall be possible to synchronize the traffic signal controllers installed in a corridor in the following modes of operation, without physically linking them and without communication network. GPS enabled RTC shall be the reference for the cable less synchronization.
xvi. Fixed Time mode with fixed offsets
xvii. Vehicle Actuated mode with fixed offsets

- **Input and Output facilities**

i. Lamp Switching: The controller shall have maximum 64 individual output for signal lamp switching, configurable from 16 to 32 lamps. The signal lamps shall be operating on appropriate DC/AC voltage of applicable rating.
ii. Detector Interface: A minimum of 16 vehicle detector inputs shall be available in the controller. All detector inputs shall be optically isolated and provided with LED indication for detection of vehicle.
iii. Communication Interface: The traffic signal controller shall support Ethernet interface to communicate with the ATCS server
iv. Power Saving: The traffic signal controller shall have a facility to regulate the intensity of signal lamps during different ambient light conditions thereby saving energy.
v. Real-time Clock (RTC): The GPS receiver for updating time, date and day of the week information of the traffic signal controller should be an integral part of the traffic signal controller.
vi. The traffic signal controller shall update the date, time and day of the week automatically from GPS during power ON and at scheduled intervals.
vii. Manual entry for date, time and day of week shall be provisioned for setting the traffic signal controller RTC (Real Time Clock).
viii. It shall be possible to set the RTC from the Central Server when networked
ix. Keypad (optional): The traffic signal controller shall have a custom made keypad or should have provision for plan upload and download using PC/laptop/Central Server
x. Operator Display (optional): The traffic signal controller shall optionally have a LED backlit Liquid Crystal Display (LCD) as the operator interface.

b) **Countdown Timer:**
It shall be installed at each traffic junction under ITMS & City Surveillance System Project.

i. Count Down Timer to be configured in Vehicular Mode.
ii. The Vehicular countdown timer should be dual
iii. Color,; Red for Stop or STP and Green color for Go
iv. There should be alternate Red and Balance phase time for STOP or STP in Flashing
v. Alternate Green and Balance Phase Time for Go in Flashing

6.1.1.1 Technical Requirements of Countdown Timer

S.No.	Description
1	CPU: Micro Controller
2	Mechanical Specifications
3	Structural Material Polycarbonate strengthened against UV rays
4	Body Color: Light Grey/Black
5	Dimensions:360mm x 370mm x 220mm
6	Display Specification:
7	Lamp Diameter : 300mm
8	Digit Height:150 -165mm
9	Display Type Dual Coloured (Red & Green)
10	No. of Digit : 3

11	LED Specifications
12	LED Diameter : 5mm LED Viewing Angle 30° LED Wave Length 630-640nm (Red), 505nm - 520nm (Blue-Green) LED Dice Material AlInGaP (Red), InGaN (Blue-Green) LED Warranty period 5 years
13	Poles for Traffic Signals : Material: GI Class 'B' pipe
14	Paint: Pole painted with two coats of zinc chromate primer and two coats of golden yellow Asian apostolate paint or otherwise as required by architect and in addition bituminous painting for the bottom 1.5 m portion of pole.
15	No's of cores: 7 and 14 core 1.5 sq. mm.; 3 Core 2.5 sq. mm.
16	Materials: PVC insulated and PVC sheathed armoured cable with copper conductor of suitable size.
17	Certification: ISI Marked Standards: Indian Electricity Act and Rules IS:1554 - PVC insulated electric cables (heavy duty)

c) **Communication Network :**

i. Function of the Communication network is for remote monitoring of the intersection and its management. Real time data (like RTC time, stage timing, mode, events, etc.) from the traffic signal controller is required to be sent to the Central Computer in ICCC. Central Computer running the ATCS application shall calculate and send optimum signal timings to all intersections in the corridor. MSI shall clearly specify the bandwidth requirements and the type of network recommended for the ATCS.

ii. The contractor shall specify the networking hardware requirements at the ICCC and remote intersections for establishing the communication network.

6.1.1.2 Technical Requirements of Field Junction Box

S.No.	Parameter	Minimum Specifications
1.	Size	Suitable size as per site requirements to house the field equipment
2.	Cabinet Material	Powder coated CRCA sheet/ Stainless steel
3.	Material Thickness	Min 1.2mm
4.	Number of Locks	Two
5.	Protection	IP66 / NEMA 4X
6.	Mounting	On Camera Pole / Ground mounted on concrete base
7.	Form Factor	Rack Mount/DIN Rail
8.	Other Features	Rain Canopy, Cable entry with glands and Fans/any other accessories as required for operation of equipment's within junction box.

iii. Junction Boxes

The junction box shall be fitted in secure locations (not easily accessible to the general public) and shall be fitted with a standard cabinet lock. Roadside cabinets shall be secured with anti-tamper fixings in addition to the standard cabinet lock.

- Each Junction box shall be fitted with sufficient screw type terminals to terminate all pairs used and unused. The terminal blocks shall be certified for use with the box.
- Each box shall be equipped with certified cable glands/plug and with earthing bar.

Cable continuity shall be through junction box dedicated terminals

d) **ATCS Software Application**

i. Objective of the ATCS is to minimize the stops and delays in a road network to decrease the travel time with the help of state-of-the-art technology. The adaptive traffic control system shall operate in real time with the capacity to calculate the optimal cycle times, effective green time ratios, and change intervals for all system traffic signal controllers connected to it. These calculations will be based up on assessments carried out by the ATCS application software running on a Central Computer based on the data and information gathered by vehicle detectors at strategic locations at the intersections controlled by the system.

6.1.1.3 ATCS Application Software Requirement

S.No.	Description
1.	Identify the critical junction of a corridor or a region based on maximum traffic demand and saturation.
2.	The critical junction cycle time shall be used as the group cycle time i.e. cycle time common to all intersection in that corridor or region.
3.	Stage optimization to the best level of service shall be carried out based on the traffic demand.
4.	Cycle optimization shall be carried out by increasing or decreasing the common corridor cycle time based on the traffic demand within the constraints of Minimum and Maximum designed value of cycle time.
5.	Offset correction shall be carried out to minimize number of stops and delays along the corridor for the priority route. Offset deviation measured using distance and speed between successive intersections shall be corrected within 5 cycles at a tolerance of +/- 5 seconds maximum.
6.	The system shall have provision to configure priority for upstream signals as default. The ATCS software shall continuously check the traffic demand for upstream and downstream traffic and automatically assign the priority route to the higher demand direction.
7.	Develop appropriate stage timing plans for each approach of every intersection under the ATCS, based on real time demand
8.	Propose timing plans to every intersection under the ATCS in every Cycle
9.	Verify the effectiveness of the proposed timing plans in every cycle
10.	Identify Priority routes
11.	Synchronize traffic in the Priority routes
12.	Manage and maintain communication with traffic signal controllers under ATCS

13.	Maintain database for time plan execution and system performance
14.	Maintain error logs and system logs
15.	Generate Reports on request
16.	Graphically present signal plan execution and traffic flow at the intersection on desktop
17.	Graphically present time-space diagram for selected corridors on desktop
18.	Graphically present network status on desktop
19.	Make available the network status and report viewing on Web
20.	The ATCS shall generate standard and customer ports for planning and analysis
21.	It shall be possible to interface the ATCS with popular microscopic traffic flow simulation software for pre and post implementation analysis and study of the proposed ATCS control strategy
22.	Shall have the ability to predict, forecast and smartly manage the traffic pattern across the signals over the next few minutes, hours or 3-5 days and just in the current real time.
23.	Shall provide a decision support tool for assessing strategies to minimize congestion, delays and emergency response time to events via simulation and planning tools liked with real time traffic data fusion and control of traffic signaling infrastructure on ground.
24.	Shall collect continuously information about current observed traffic conditions from a variety of data sources and of different kind (traffic states, signal states, vehicle trajectories, incidents, road works, etc.).
25.	Shall infer a coherent and comprehensive observed traffic state (speeds, vehicular densities, and presence of queues) on all network elements, from abovementioned observations, including vehicle trajectories, through a number of map matching, data validation, harmonization and fusion processes).
26.	Shall extend the measurements made on only a number of elements both on the rest of the unmonitored network, and over time, thus obtaining an estimation of the traffic state of the complete network and the evolution of this traffic state in the future.
27.	Shall forecast the traffic state with respect to current incidents and traffic management strategies (e.g. traffic signal control or variable message signs), improving the decision making capabilities of the operators even before problems occur.
28.	Shall calculate customizable Key Performance Indicators (KPI) to quickly assess the results
29.	Shall provide calculated traffic flows estimation and forecast, queues and delays to Urban Control and Adaptive Signal Control Systems, allowing for proactive Traffic Management and Control
30.	Shall generate alerts to the operator that trigger on customizable conditions in the network (starting with simple drops in flow, up to total queue lengths along emission sensitive roads surpassing a definable threshold)
31.	Shall distribute both collected and calculated traffic information via a variety of communication protocols and channels, ensuring high interoperability degree and thus acting as a "traffic data and information hub"
32.	Shall create a traffic data warehouse for all historic traffic information gathered from the hardware installed on the road network.
33.	Shall operate in real time that is continuously updating the estimates on the state of the network and the travel times on the basis of data collected continuously over time.

34.	Shall operate the traffic lights with the adaptive traffic controls, based on the current and forecasted traffic demand and the current incidents, thus optimizing the green waves continuously throughout the network
35.	Enable a smart public transport priority respecting the delays for all road users at once with the adaptive signal controller
36.	Reports: a. Intersection based reports i. Stage Timing report – The report shall give details of time at which every stage change has taken place. The report shall show the stage sequence, stage timings and stage saturation of all stages of all cycles for a day. The saturation is defined as the ratio between the available stage timings to the actual stage timing executed by the traffic signal controller for the stage (stage preemption time). ii. Cycle Timing report – The report shall give details of time at which every cycle has taken place. The report shall show the cycle sequence and cycle timings for all the cycles in a day. iii. Stage switching report – The report shall give details of time at which a stage switching has taken place. The report shall show the stage sequence, stage timings and stage saturation for a day. iv. Cycle Time switching report – The report shall give details of time at which a cycle switching has taken place. The report shall show the cycle sequence and cycle timings for the cycle in a day. v. Mode switching report – The report shall give details of the mode switching taken place on a day. vi. Event Report - The report shall show events generated by the controller with date and time of event. vii. Power on & down: The report shall show time when the master is switched on, and last working time of the master controller. viii. Intensity Change – The report shall show the brightness of the signal lamp is changed according to the light intensity either manually through keypad or automatically by LDR with time stamp. ix. Plan Change – The report shall show the time of change of plan either through keypad or remotely through a PC or Server. x. RTC Failure – The report shall show the time when RTC battery level goes below the threshold value. xi. Time Update – The report shall show the time when the Master controller updated its time either manually through keypad, automatically by GPS or through remote server. xii. Mode Change – The report shall show the time when Master controller's operating mode is changed either manually through keypad or a remote server. The typical modes are FIXED, FULL VA SPLIT, FULL VA CYCLE, FLASH, LAMP OFF and HURRY CALL. xiii. Lamp Status Report – The report shall show lamp failure report with date and time of failure, color of the lamp and associated phase. xiv. Loop Failure Report – The report shall show the date and time of detector failure with detector number and associated phase. xv. Conflict – The report shall show the conflict between lamps (RED, AMBER, GREEN) in the same phase or conflict between lamps with other phase.

	b. Corridor Performance Report – The report shall show the saturation of all the intersections in a corridor for every cycle executed for the corridor and the average corridor saturation for a day c. Corridor Cycle Time Report – The report shall show the Corridor cycle time, Intersection cycle time, Mode of operation and degree of saturation of all the intersections in a corridor for every cycle for a day.
37.	Graphical User Interface - The application software shall have the following Graphical User Interface (GUI) for user friendliness. i. User login – Operator authentication shall be verified at this screen with login name and password ii. Network Status Display – This online display shall indicate with appropriate color coding on site map whether an intersection under the ATCS is online or off. On double clicking the intersection a link shall be activated for the traffic flow display for the intersection. iii. Traffic Flow Display – This online display shall indicate the current traffic flow with animated arrows, mode of operation, stage number being executed and elapsed stage time. iv. Saturation Snapshot – This display shall show the current saturation levels of all intersections in a corridor. v. Reports Printing / Viewing – This link shall allow selection, viewing and printing of vi. different reports available under ATCS vii. Time-Space Diagram – The time-space diagram shall display the current stages being executed at every intersection in a corridor with immediate previous history. viii. Junctions shall be plotted proportional to their distance on Y-axis and time elapsed for the stage in seconds on X-axis. ix. Junction names shall be identified with each plot. x. Facility shall be available to plot the time-space diagram from history. xi. Currently running stage and completed stages shall be identified with different colors. xii. Stages identified for synchronization shall be shown in a different color. xiii. Speed lines shall be plotter for stages identified for synchronization to the nearest intersection in both directions. xiv. It should be possible to freeze and resume online plotting of Time-Space diagram. xv. The system shall have other graphical interfaces for configuring the ATCS, as appropriate.

6.1.1.4 Detailed Specifications for Vehicle Detector Sensor

Sr. No	Description
1.	The vehicle detector should Forward firing technology multilane radar/video based technology with 4D object tracking with HD resolution. The sensor should be capable of working in fog, rain and without any requirement of cleaning and can provide precise information on counting , classification queue length for at least 175 meters for all stopped and moving vehicles..
2.	The sensor should have a detection range of 3m to 175 meters.
3.	The vehicle detector should have had a wide field of view of 40 degrees, and at the same time a range of up to 180m
4.	Vehicle detector should be multilane and should Detect up to 126 individual objects, and measure their position and speed
5.	The sensor should have radar/video based 4D object tracking and should measure (X, Y, Z) Cartesian coordinates or polar coordinates range, azimuth and elevation angle, as well as the speed vector simultaneously for up to 126 objects
6.	The radar/video based 4D with HD technology used should provide high-resolution capability in scenarios where many vehicles are closely spaced, i.e. in many lanes, dense traffic, traffic jams, stop and-go situations.
7.	One single sensor should allow up to 16 virtual loops and should have very high detection performance compared to video detectors.
8.	Vehicle detector should detect moving and stopped traffic i.e. Should detect vehicles, no matter if stopped or moving. Up to 150km/h: no matter what traffic direction.
9.	Vehicle detector should not be affected by dirt, smog, sunlight, wind or sandstorms.
10.	IP67, from 0 °C to + 60 °C.
11.	The Vehicle detector should maintain high accuracy by means of built-in self-calibration functions throughout the entire design life.
12.	It should have flexibility of installation on the roadside, at the corner of an intersection, at the median of a highway or on a gantry, with best results, not like side-firing technology, needing set-back from the road and having high occlusion risk
13.	It should have flexibility of installation on the roadside, at the corner of an intersection, at the median of a highway or on a gantry, with best results, not like side-firing technology, needing set-back from the road and having high occlusion risk
14.	The sensor should have wide field of view -20° to+20° Azimuth and the long range (175m) to allow the user to define at least 16, up So that vehicles are tracked over a longer period when they drive in the field of view to avoid occlusion.

6.2 Scope of Work

6.2.1 Automatic Number Plate Recognition (ANPR) System

Overview

ANPR System shall enable monitoring of vehicle flow at strategic locations. The system shall support real-time detection of vehicles at the deployed locations, recording each vehicle, reading its number plate, database look up from central server and triggering of alarms/alerts based on the vehicle status and category as specified by the database. The ANPR software preferred to be integral part of Video Management and Intelligent Traffic Management software for no integrational hazards at the time of installation.The system usage shall be privilege driven using password authentication. System should have following functional requirements:

Scope of Work

a) System should have following components and capable of doing following:

i. Ability to have IR illuminators to provide illumination for night-time scenario.
ii. Ability to provide the live feed of the camera at the integrated command control center or as per user requirement.
iii. Ability to provide video clips of the transaction from the ANPR lane cameras as evidence.
iv. Ability to detect the color of all vehicles in the camera view during daytime. The system can store the color information of each vehicle along with the license plate information for each transaction in the database.
v. Ability to search historical records for post event analysis by the vehicle color or the vehicle color with license plate and date time combinations.
vi. Ability to input certain license plates according to the hot listed categories like “Wanted”, “Suspicious”, “Stolen”, etc. by authorized personnel.
vii. Ability to generate automatic alarms to alert the control room personnel for further action, in the event of detection of any vehicle falling in the hot listed categories.
viii. Ability to generate automatic alarm to alert the control room on successful recognition of the number plate based on pre-defined rules.
ix. Ability to easy and quick retrieval of snapshots, video and other data for post incident analysis and investigations.
x. Ability to generate MIS reports to concerned authorities and facilitate optimum utilization of resources. These reports shall include but not limited to:

- Report of vehicle flow at each of the installed locations for Last Day, Last Week and Last Month.
- Report of vehicles in the detected categories at each of the installed locations for Last Day, Last Week and Last Month.
- Report of Vehicle Status change in different Vehicle Categories.

xi. Ability to search the information based on parameters defined.
xii. Ability to auto generate reports and send to stakeholders.
xiii. Ability to define system access based on rule.

xiv. Local Server at Intersection: The Local processing unit should be industrial grade and must avoid single point of failure. The system must run on a Commercial Off the Shelf Server (COTS). Outdoor IP 66 Quad core processor based server should be able to cover at least 8 lanes. Temperature rating of the server should be at least 60 degree.

xv. Operating system: The system must be based on open platform and should run on LINUX/Windows Operating system.

xvi. ANPR system should work in integration with RLVD system and enable the RLVD system for generating the evidence of violation.

xvii. The system should perform ANPR on all the vehicles passing the site and send alert to the Command and Control Centre on detection of any Hot-listed.The VMS software must have tight integration with command and control software so that the event snap and event video as well as user can have the access of archived video of that particular camera.

xviii. With the detected number plate text, picture should also be sent of hot listed vehicle. It is highly likely to misread similar alphabets like 7/1/L or 8/B.

xix. The system should have ANPR/ OCR to address the Alpha numerical character of irregular font sizeswith a very good accuracy.

xx. Minimum 2(two) USB Port to support the latest external mass storage devices and Ethernet (10/100) Port for possible networking. However all logs of data transfer through the ports shall be maintained by the system.

xxi. System should be capable of working in ambient temperature range of 0 Degree Celsius to 60 Degree Celsius.

xxii. Lightening arrester shall be installed for safety of system (As per BIS standard IS 2309 of 1989).

xxiii. The housing(s) should be capable of withstanding vandalism and harsh weather conditions and should meet IP66, IK10 standards (certified).

xxiv. Encrypted data, images and video pertaining to Violations at the Onsite processing station should be transmitted to the ICCC electronically.

xxv. Advanced Encryption Standard (AES) shall be followed for data encryption on site and ICCC, and its access will protected by a password.

xxvi. Ability to video recording in base station for 7 days. Automatically overwrite the data after 7 days.

xxvii. Direct extraction through any physical device like USB flash drive, Portable Hard disk etc. shall be possible.

xxviii. Network Connectivity: Wired/GPRS based wireless technology with 4G and upgradable or batter to be provided.

xxix. Vehicle number detection is to be made possible on the ANPR cameras.

xxx. ANPR cameras should also have capability to detect Red Light Violation together with evidence camera (RLVD).

xxxi. The complete tracking of the vehicle is to be made possible on the GIS map to locate any suspicious / identified vehicle.

xxxii. The identified or suspicious vehicle may be flagged by any police personnel or sensed by ANPR or through other analytics like vehicle tracking based on color& shape of the vehicle.The ANPR software shall have the facility to search only the number plates of any given time.

6.2.2 Red Light Violation Detection (RLVD) System

Overview

a) System should have the facility to provide the live feed of the camera at the central command centre. System should generate Alarms at control room software if any signal is found not turning RED within a specific duration of time. The following Traffic violations to be automatically detected by the system by using appropriate technology. The RLVD software must be innate of ITMS and VMS software for easy to use.The Evidence camera should also be used for evidence snap generation minimum for Red Light Violation, Stop Line Violation, Wrong left turn violation, Wrong direction driving violation.
b) The system should be capable of capturing multiple infracting vehicles simultaneously in Different lanes on each arm at any point of time with relevant infraction data like Type of Violation, Date, time, Site Name and Location of the Infraction, Registration Number of the vehicle through ANPR Camera system for each vehicle identified for infraction.
c) The system should be equipped with a camera system to record a digitized image and video of the violation, covering the violating vehicle with its surrounding and current state of signal (Red/Green/Amber) by which the system should clearly show nature of violation and proof thereof : When it violates the stop line and When it violates the red signal.
d) The system must have in-built tool to facilitate the user to compose detail evidence by stitching video clips from any IP camera in the junction (including but not limited to the red light violation detection camera, evidence camera), and any other surveillance cameras in the vicinity of the spot of incidence. The entire evidence should be encrypted. The system should interface with the traffic controller to validate the colour of the traffic signal reported at the time of Infraction so as to give correct inputs of the signal cycle.
e) The system shall be equipped with IR Illuminator to ensure clear images including illumination of the Number Plate and capture the violation image under low light conditions and night time.

Scope of Work

Over all solution should be able to provide features and capable to fulfil the following requirements:

a) Speed Violations :

i. The nonintrusive system shall be capable of measuring speed of vehicles and capture over-speed vehicles The Speed measurement should support multiple methods for calculation of speed – either Average or Instantaneous Speed Measurement methods. All ANPR Camera must provide average speed of all crossing vehicles along with OCR.The system shall have the provision of setting different speed thresholds for different class of vehicles for any particular Lane.
ii. The speed violations system should be installed on mid-blocks or designated areas as identified during design stage.

b) Wrong Direction Vehicle Movement

The non-intrusive system should be installed at critical junctions to capture the wrong direction vehicle movement. The system should identify and capture multiple IVD. The e-Challan standard procedure should be triggered.

c) Recording & display information

The recording and display of information should be detailed on the snapshot of the infracting vehicle as follows:

i. Computer generated unique ID of each violation
ii. Date (DD/MM/YYYY)
iii. Time (HH:MM:SS)
iv. Equipment ID
v. Location ID
vi. Carriageway or direction of violating vehicle
vii. Type of Violation (Signal/Stop Line)
viii. Lane Number of violating vehicle
ix. Time into Red/Green/Amber
x. Registration Number of violating vehicle

- The system should start automatically after power failure. The system should have secure access mechanism for validation of authorised personnel.
- A log of all user activities should be maintained in the system.
- Roles and Rights of users should be defined in the system as per the requirements of the client
- In the event that the connectivity to the ICCC is not established due to network/connectivity failures, then all data pertaining to the infraction shall be stored on site and will be transferred once the connectivity is re- established automatically. Ability of physical transfer of data on portable device whenever required. There should be a provision to store minimum one week of data at each site on a 24x7 basis. System should be mounted as per appropriate deign by MSI.

RLVD Application

a) It should be capable of importing violation data for storage in database server which should also be available to the Operator for viewing and retrieving the violation images and data for further processing. The programme should allow for viewing, sorting, transfer & printing of violation data.
b) It should generate the photograph of violations captured by the outstation system which include a wider view covering the violating vehicle with its surrounding and a closer view indicating readable registration number plate patch of the violating vehicle or its web link on notices for court evidence.
c) All outstation units should be configurable using the software at the Central Location.
d) Violation retrieval could be sorted by date, time, location and vehicle registration number and the data structure should be compatible with BSCL Police database structure. It should also be possible to carry out recursive search and wild card search.

e) The operator at the back office should be able to get an alarm of all fault(s) occurring at the camera site (e.g. sensor failure, camera failure, failure of linkage with traffic signal, connectivity failure, Camera tampering, sensor tampering).
f) The application software should be integrated with the e-Challan/Vahan software for tracing the ownership details of the violating vehicle and issuing/printing notices. Any updates of the software (OS, Application Software including any proprietary software), shall be updated free of cost during the contract period by MSI.
g) Image zoom function for number plate and images should be provided. In case the number plate of the infracting vehicle is readable only through the magnifier then in such cases the printing should be possible along with the magnified image.
h) Components of the architecture must provide redundancy and ensure that there are no single points of failure in the key project components. To take care of remote failure, the systems need to be configured to mask and recover with minimum outage.
i) The evidence of Infraction should be encrypted and protected so that any tampering can be detected.
j) The user interface should be user friendly and provide facility to user for viewing, sorting and printing violations. The software should also be capable of generating query based statistical reports as per requirement.

i. The system should be capable of generating a video & minimum 5 snapshot/images in any of the standard industry formats (MJPEG, JPG, avi, mp4, mov, etc.) with at least 10 frames per second. The video shall be from t-5 to t+5 sec of the violation and should also be recorded (being the instant at which the infraction occurred).
ii. Digital Network Camera: As per specified in Surveillance Camera Section.
iii. On site-out station processing unit communication & Electrical Interface (Junction Box).
iv. The system should be equipped with appropriate storage capacity for 7days 24X7 recording, with over writing capability. The images should be stored in tamper proof format only.
v. Wired/GPRS based wireless technology with 4G and upgradable.
vi. Minimum 2(two) USB Port to support the latest external mass storage devices and Ethernet (10/100) Port for possible networking.
vii. System should be capable of working in ambient temperature range of 0 degrees C to 60 degrees C.
viii. Lightening arrester shall be installed for safety of system (As per BIS standard IS 2309 of 1989).
ix. The housing(s) should be capable of withstanding vandalism and harsh weather conditions and should meet IP66, IK10 standards (certified).
x. Encrypted data, images and video pertaining to Violations at the Onsite processing station should be transmitted to the ICCC.
xi. Advanced Encryption Standard (AES) shall be followed for data encryption on site and ICCC, and its access will protected by a password.
xii. Ability of continuous video recording in base station for 7 days. The system shall automatically overwrite the data after 7 days. It should be noted that at any point

of time the local storage at the base station should have the data of previous 7 days.

xiii. Direct extraction through any physical device like USB flash drive , Portable Hard disk etc. shall be possible

6.2.3 Automated e- Challan System

a) Modules for e-Challan Software

i. Photo Collection
ii. Violation booking
iii. e-challan Generation
iv. Postal dispatches
v. Postal Statement
vi. Postal returns and return info feeding
vii. Data entry in vehicle Registration. remarks database
viii. Provision to enter comment Sold out vehicles/Fake vehicles /Fake addressed
ix. Vehicles/Theft Vehicles/Authorized complaints/Multiple owners)
x. Identification of Police Stations, Junctions, Courts, Police Staff for the Traffic dept
xi. MV Act cases
xii. ID ,Address& contact details fields addition
xiii. Action dropouts as per Court decisions
xiv. Report Generation
xv. Online Pending Challan Verification
xvi. Online Violation photo view facilities
xvii. Upgrading the E-challan Software
xviii. Online Uploading photos by the Police in Control room
xix. Online handheld machine tracking System
xx. Server database and crash recovery of data
xxi. Regular Backup System
xxii. Performance tuning of the Application, Database tuning, Network tuning, Web Service tuning
xxiii. Traffic violators History (for suspension of driving license)
xxiv. APIs for sharing e-Challan information for online payment and up-dation of payment status in e-Challan application server
xxv. Generating hash value for each challan
xxvi. Digital signing of – challan

6.2.4 Speed Violation Detection (SVD) System

Overview

a) The Speed Violations should be automatically detected by the system by using appropriate user certified technology.The Speed detection solution shall be a part of ITMS and integrated with VMS for easy to operate. 24x7 recording of all Speed Camera need to be kept and possible to mark as do not delete to use as evidence in the court of law as and when required.
b) The system should be capable of capturing multiple infracting vehicles simultaneously in defined lanes at any point of time simultaneously with relevant infraction data like:

i. Type of Violation
ii. Speed of violating vehicle
iii. Notified speed limit
iv. Date, time, Site Name and Location of the Infraction
v. Registration Number of the vehicle through ANPR Camera system for each vehicle identified for infraction.

c) The system should be equipped with a camera system to record a digitized image or video frames of the violation, covering the violating vehicle with its surrounding.
d) The system shall provide the No. of vehicles infracting simultaneously in each lane. The vehicles will be clearly identifiable and demarcated in the image produced by the camera system.
e) The system shall be equipped with IR Illuminator to ensure clear images including illumination of the number plate and capture the violation image under low light conditions and night time.
f) Speed measurement may be made by using non-intrusive technology such as Image based or any other appropriate certified technology.. The system must have installed in Indian roads and the OEM must produce satisfaction certificate from any traffic police department minimum IPS level.
g) The system should automatically reset in the event of a program hang up and restart after power failure.
h) Ability to define role based access.
i) The data shall be transferred to the ICCC in real time for verification of the infraction and processing of challan.
j) In the event that the connectivity to the ICCC is not established then all data pertaining to the infraction shall be stored on site and will be transferred once the connectivity is re-established automatically.

Speed Violation Application

The speed detection shall have the highest accuracy and capture rate of 99%. The system shall have the ability to track multiple vehicles in single lane. It shall have an accurate measurement of the speed and location of the vehicle within the measuring area. It shall also support wireless handheld device configuration, visual configuration interface in a highly user-friendly and efficient interface. The system shall also be be able to detect vehicles go into the wrong. The system must be capable to detect speed of Two -wheeler, Three- wheeler, Four-wheeler and Heavy vehicles.

a) It should be capable of importing violation data for the Operator for viewing and retrieving the violation images and data for further processing. The programme should provide for sort, transfer & print command.
b) It should generate the photograph of violations captured by the outstation system which include a wider view covering the violating vehicle with its surrounding and a closer view indicating readable registration number plate patch of the violating vehicle or its web link on notices for court evidence.
c) All outstation units should be configurable using the software at the Central Location.
d) Violation retrieval could be sorted by date, time, location and vehicle registration number and data structure should be compatible with BSCL Traffic Police database and BSCL Transport department database structure.
e) The operator at the back office should be able to get an alarm of any possible fault(s) at the camera site (outstand) (e.g. sensor failure, camera failure, failure of linkage with traffic signal, connectivity failure, Camera tampering , sensor tampering).
f) The automatic number plate recognition Software may be part of the supplied system, or can be provided separately as add on module to be integrated with violation detection. a.) Success rate of ANPR will be taken as 80% or better during the day time and 60% or better during the night time on standard number plates.
g) Image zoom function for number plate and images should be provided. Any updates of the software available, shall be updated free of cost during the contract period by the vendor and will integrate the same with existing application and database of BSCL Traffic Police and BSCL Transport department.
h) The application software should be integrated with the notice branch software for tracing the ownership details of the violating vehicle and issuing/printing notices.
i) Various users should be access the system using single sign on and should be role based. Different roles which could be defined (to be finalized at the stage if SRS) could be Administrator, Supervisor, Officer, Operator, etc.
j) Apart from role based access, the system should also be able to define access based on location.
k) Rights to different modules / Sub-Modules / Functionalities should be role based and proper log report should be maintained by the system for such access.
l) Important technical components of the architecture must support scalability to provide continuous growth to meet the growing demand of BSCL Police. The system shall support vertical 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. Main technological components requiring scalability are Storage, Bandwidth, Computing Performance (IT Infrastructure), Software / Application performance and advancement in proposed system features.
m) The system shall also support horizontal scalability so that depending on changing requirements from time to time, the system may be scaled horizontally.
n) Components of the architecture must provide redundancy and ensure that are no single point of failures in the key project components. Considering the high sensitivity of the system, design shall be in such a way as to be resilient to technological sabotage. To take care of remote failure, the systems need to be configured to mask and recover with minimum outage.

o) The architecture must 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. Preferred to use LINUX OS in the servers to defend the virus attacks and windows in client workstations/client for easy operation. 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.

p) Ease of configuration, ongoing health monitoring, and failure detection are vital to the goals of scalability, availability, and security and must be able to match the growth of the environment.

q) Systemshalluseopenstandards and protocols to the extent possible.

r) The user interface should be user friendly and provide facility to user for viewing, sorting and printing violations. The software should also be capable of generating query based statistical reports on the violation data.

s) The data provided for authentication of violations should be in an easy to use format as per the requirements of user unit.

t) User should be provided with means of listing the invalid violations along with the reason(s) of invalidation without deleting the record(s).

u) Basic image manipulation tools (zoom etc.) should be provided for the displayed image but the actual recorded image should never change.

v) Log of user actions be maintained in read only mode. User should be provided with the password and ID to access the system along with user type (admin, user).

w) Image should have a header and footer depicting the information about the site IP and violation details like viz. date, time, equipment ID, location ID, Unique ID of each violation, lane number, Registration Number of violating vehicle and actual violation of violating vehicle etc. so that the complete lane wise junction behaviour is recorded viz. (Speed of violating vehicle, notified speed limit, Speed Violation with Registration Number Plate Recognition facility. Number plate of cars, buses/HTVs should be readable automatically by the software/interface. There should be user interface for simultaneous manual authentication / correction and saving as well.

x) Interface for taking prints of the violations (including image and above details).

Scope of Work

a) Traffic violations of over speeding vehicles in fixed locations as well as predefined stretch of road shall be automatically detected by satisfactorily certified by any traffic police department from India.

b) All over speeding vehicles not following traffic rules and driving unsafe with risk to themselves and others will be fines. Vehicles crossing any dangerous spot will be booked with SPOT SPEED ENFORCEMENT SYSTEMS. At the same time Point to point speed will also be installed in some strategic arterial (urban/highway

road to prosecute commuters who try to slow down just in front of the spot speed systems and then over speed. Vehicles passing through the control section at a Speed greater than a determined speed limit (values to be made configurable via software) shall be detected as violation and System shall produce a sequence of relative images (or a movie) with value of speed detected and executing ANPR process to automatically extract number plate of vehicle in infraction.It should be possible to set speed limit for different types of vehicles (different speeds for two-wheeler, three-wheeler, four-wheeler and heavy vehicles).

c) The photograph generated by the system at both locations shall be stitched together and ANPR shall be performed.
d) Specifications for Instant Speed System.

S.No.	Specifications
1	Traffic violations should be automatically detected by the system. The System should provide image of over speeding vehicle with proper proof of speed violation in terms of Video and photographs of vehicle with required data printed on it.
2	Following data for each infraction should be provided: date, time, location, speed, number plate with the help of automatic number plate detection mechanism(using ANPR camera or similar means).
3	System should generate automatically color image (day time) of the number plate of the Vehicle. In case of traffic violations, the system shall generate challan as per pre-defined formats with relevant images of violation. The system should provide control image to verify speed.
4	The Speed system should use a speed sensor which has means to cross confirmation through simulators. The speed sensor should have possibility of proper working without actual vehicle transit.
5	System should be in the form of a composite unit with all components inside the IP65 box or comprised of camera or other units mounted on poles or gantries with controller and processors at side poles to make sure all lanes of the road are covered. Preferred systems should be installed at a minimum height of 3 meters or above.
6	System should work in day and night condition and in bad weather conditions
7	i. Speed should be measured using advanced Image based technology. ii. System shall provide Range, speed, lane, class of each vehicle. iii. The system shall be able to track at least 64 objects iv. Lane separation shall be available to at least 100m distance from the sensor v. Typical speed measurement accuracy shall be within < ±1 km/h or ±1% (bigger of) vi. Extreme value should not increase 3% error vii. Detectable Speed shall be in the range of 320 km/h viii. Range measurement accuracy shall typically be within 2.5% or 0.25m (bigger of) ix. Classification shall be between Truck and Car x. The sensor shall be able to detect oncoming and outgoing traffic simultaneously on up to 4 lanes xi. The System should work with an object tracking principle xii. The system shall be able to separate lanes and to output lane specific information at least every 50ms for each vehicle inside its field of view(i.e. speed, position, classification and ID)

S.No.	Specifications
8	Camera Unit: Cameras must be Day night and must have CMOS with 1/2.8" sensor (or greater), shutter speed 1/1000 sec or better, resolution 2Megapixel or better, temp range -5 to +55°C, Megapixel auto iris lens.
9	Integrated external Infrared capable to take images in night time and detect automatically number plate for minimum 25 meters.
10	Control: speed setup Km/hr, up to 150km/h ± 3%
11	Working temperature 0°C to +60°C 80% and above humidity.
12	Processor: Industrial processor for local site with minimum 7 days recording. LPU/system should send data automatically to the CCR and should be able to auto start in case of power failure.
13	BACK office: the system should provide data decryption and storage, Issuing of automatic challan with automatic number plate detection with multiple images. No deletion or addition of data without proper authorization & proper password protection
14	Possibility to import data files and infractions should be provided as per city police requirement. Violation retrieval should be available for selected location, time and number series (DL 07,UP 07...etc.). (one-time configuration of software as per Traffic police requirement should be considered)
15	System should be able to recognize automatically the number plate of cars in involved in violation. The accuracy should be more than 80% in day and 60 % night condition. ANPR system should be capable to work with Indian number plates and should preferably have been used for Indian plates for a considerable period of time.
16	Communication: -The system should have proper communication with control room and should be able to provide online infraction reports and live infraction. Automatic number plate detection should be part of the system
17	Back office: Server Intel Xeon (8M Cache, 2.30 GHz or better) with 16GB (2 X 8GB) RAM and 6TB SATA Hard Disk Server based back office will be preferred to single pc software
18	Stability of product and after sale services: MSI should have local support for technical assistance and system should be repairable or replaceable. MSI should show spares availability for minimum 2 such systems.
19	Third party (authorized company to do so) speed test reports can be submitted to client. On field detailed speed test reports for more than 120-200 km/hr with various speed limits. Alternatively, the system should be approved and homologated by some traffic or infrastructure department who directly over sees fine generation post implementation but before FAT.
20	Test reports for IP 66 for cameras should be provided. This is to support harsh rainy season and dusty environment.

e) Specification for Average Speed System

S.No.	Specification	Minimum User Requirement
1	General	Technology to be used is non-intrusive.
		The measure of vehicle speed shall be the Average Speed in a control section.
		The system may also be used for measuring Instant Speed at any point
		All vehicles passing through the control section at a Speed greater than a determined speed limit (values to be made configurable via software) shall be detected as violation and System shall produce a sequence of relative images (or a movie) with value of speed detected and executing ANPR process to automatically extract number plate of vehicle in infraction. The system should not be solely ANPR depended for speed ticket generation. System shall have provision for setting different speed thresholds for minimum of two vehicles categories (light, commercial).
		System shall work in day and night conditions and should be
		The system should have option to add instant speed in case if client decided to add instant speed in future.
2	Data capture	Cameras fitted in the equipment shall record a digitized image or video frames of the violation covering defined lanes on each approach arm at any point of time simultaneously with relevant data about the offence, i.e. date, time, fixed location and speed etc.
		The photograph generated by the system at both locations shall be stitched together and ANPR be performed.
		The results are independent of number plate recognition at individual points.
3	Camera Unit	Make: Certified Camera for the Purpose as per certificate Resolution: 2 Megapixels or better(see camera details in Camera part)
4	IR Module:	External IR (no flash)
		Distance: 25 meters with 20 degrees beam
5	Housing	The mounting(s) shall house all the required connections including the electricity and network connectivity. It also houses the microprocessor unit and electronic interface with the sensors, camera(s) etc. and an UPS
		The housing(s) confirms to IP 66
6	Safety	Speed shall be measured using eye safe laser-class 1

S.No.	Specification	Minimum User Requirement
		(security class LASER (IEC/EN 60825) /Image based System in cases were instant speed is installed with average speed
7	Speed measurement	Speed limits to be measured 150km/hr.
		Maximum error permissible ±3 %
		Speed measurement to be made by non-invasive
		system through approved technologies and for systems already in use used by authorities worldwide.
		System should provide specific lane of the vehicle when speeding
		System should provide clear megapixel image with automatic ANPR data with speed in image
8	Calibration	The vendor shall calibrate the cameras from time to time and ensure that the calibration certificates are provided to the client to ensure accuracy of system.
9	Accuracy	Accuracy should be higher than 97 percentage on free flow traffic for test and for all vehicles passed
10	Violation Retrieval	Violations should be available for selection from a displayed list corresponding to each location separately. The retrieval could be sorted by date, time, location and by vehicle registration number.
11	Statistical Analysis	Various automated reports should be available for hourly data, infraction per hour/day week etc.
12	User Interface	The user interface broadly falls into the categories of viewing, sorting and printing violations and system configuration/housekeeping.
		The violation viewer shall be provided with a means of listing the invalid violations along with the reason(s) of invalidation without deleting the original record(s).
		Complete database management and E fine issuance
		Software shall provide interface for taking printouts of violations .
		There shall be a password access system along with user type (admin, user). It permits role based permission system for accessing the data base and printouts.
13	Communication	The system shall have appropriate means of communication viz. 3G/leased lines or any other better means of network with the Control Room.

S.No.	Specification	Minimum User Requirement
14	Local Processing	The industrial processor used should be provided with each camera. Should be minimum multiple core , RAM 2 GB, with SD storage and USB storage options, temp -40 to 60 degrees and should be part of system.
	Unit	(LPU specifications are minimum and OEM should provide industrial LPU as required for applications supplied)
15	Integration with Third Part VMS	The system should be integrated with the proposed Video Management System.

f) Violation Transmission and Security

i. Encrypted data, images and video pertaining to Violations at the Onsite processing station should be transmitted to the ICCC electronically through GPRS based wireless technology with 3G upgradable to 4G or wired connectivity, in JPEG format.
ii. Advanced Encryption Standard (AES) shall be followed for data encryption on site and ICCC, and its access will protected by a password.
iii. The vendor shall ensure that the data from the onsite processing unit shall be transferred to ICCC within one day. The Speed detection system of ITMS and VMS should be deeply integrated with command and control software.

g) Video Recording

i. The system should be capable of continuous video recording in base station for 7 days. The system shall automatically overwrite the data after 7 days. It should be noted that at any point of time the local storage at the base station should have the data of previous 7 days.
ii. Direct extraction through any physical device like USB, Hard disk shall be possible.

6.2.4.1 Traffic Accident Reporting System (TARS)

a) TARS solution should provide:

i. Accident reporting system
ii. Accident recording system
iii. Analysis of accidents
iv. Dissemination of data

b) Solution shall provide accident database that will support collecting high quality information on all aspects of road traffic collisions and incorporate best practices of Road Accident Investigation.
c) Solution shall support authorities in quickly and accurately reconstructing collisions and analysing the data to develop standards to prevent future collisions or mitigate injuries.

d) Solution shall support information gathering and dissemination as per various stakeholder requirements for accident data, namely, BSCL, police, decision makers etc.
e) Information to be captured shall include, but not limited to:

i. how the accident happened,
ii. detailed information about the vehicle(s) involved
iii. type and extent of human impact
iv. human factors involved (inebriation, etc.)
v. nature of any injuries,
vi. type and extent of property damage,
vii. socio-economic data of the people involved,
viii. primary & secondary causes of the accident
ix. incident photos
x. drawing of accident analysis
xi. information on analysing agency and personnel

6.2.4.2 Traffic Sensors Lights and Signals

a) Appropriate camera based traffic sensors may be chosen to provide the operational levels and accuracy as required for successful function of the ATCS system as per the SLAs defined.
b) Appropriate controller technology may be chosen to provide the operational levels and accuracy as required for successful function of the ATCS system as per the SLAs defined. The proposed traffic controller shall be disabled friendly and shall also provide audio tones output
c) Traffic Lights: Key Features:

i. lowest power consumption for all colors
ii. Meets or exceeds intensity, color and uniformity specifications
iii. Temperature compensated power supplies for longer LED life
iv. Uniform appearance light diffusing
v. Should be Intertek/ETL/EN certified
vi. LED shall be single source narrow beam type with clear lens & Luminance uniformity of 1:15
vii. Pedestrian traffic lights should be
viii. provided with clearly audible signals for the benefit of pedestrians with visual impairments
ix. Phantom Class 5 or equivalent. IP Rating: IP65
x. LED aspects:
xi. Red, Amber, Green-Full (300 mm diameter) : Hi Flux
xii. Green-arrow (300 mm diameter): Hi flux
xiii. Animated Pedestrian-Red and Green Animated c/w countdown (300 mm) Hi Brite with diffusions
xiv. LED Retrofit Specifications:
xv. Power supply: Redundant
xvi. Standards: EN 12368 certified
xvii. Convex Tinted Lens: Available

xviii. Fuse and Transients: Available

xix. Operating Temperature Range: 0 degree Celsius to 55 degree Celsius Turn Off/Turn On Time: 75 milliseconds max

xx. Total Harmonic Distortion: <20%

xxi. Electromagnetic interference: Meets FCC Title 47,Subpart B, Section 15 Regulation or equivalent EN/IRC standard

xxii. Blowing Rain/Dust Spec: MIL 810F or Equivalent EN/IRC standard complaint

xxiii. Minimum Luminous Intensity (measured at intensity point)(cd):

- Red 400
- Amber 400
- Green 400
- Dominant Wavelength (nm):
  - ✓ Red 630
  - ✓ Amber 590
  - ✓ Green 505 - 520

d) Lamp conflict compatibility system: Compatible with lamp failure and conflict detection

7 CCTV Surveillance System

MSI has to supply, install, commission and maintain the required number of camera in the location as mentioned in Annexure. MSI has to provision for poles, switch, UPS and other equipment for installing the camera. The MSI should do necessary cabling for electrical supply and connectivity required for the field devices. MSI will also implement the following software to enable monitoring through the surveillance cameras. To facilitate the VMS system architecture, the BIDDER shall ensure that sufficient capacity is designed into the data communications & telecommunications infrastructure to deliver the required functionality, along with the ability to allocate and reserve resources (including bandwidth).Video Management System (VMS) and Video Analytics System.

General specifications of all type of cameras are as below:

a) All the network cameras supplied must be certified for: FCC ,CE and UL (Certificates to be enclosed)

b) All cameras should have feature for Bandwidth Compensation & Optimization, it should also support 3rd Party Edge Analytics, with continuous Learning

c) Ability to support use of HTTPS and SSL/TLS, providing the ability to upload signed certificates to encrypt and secure authentication and communication of both administration data and video streams.

d) The Camera shall support IEEE 802.1X authentication, Password protection, IP address filtering, HTTPS encryption, Digest authentication, User access log, Centralized certificate management

e) Ability to support open and published API

f) Programmers Interface shall provide necessary information for integration of functionality into third party applications. It should have standard components and proven technology using open and published protocols and adopt to industry established standards.

g) The implemented API shall be standardized and supported by all network video products offered by the various manufacturers.

h) Ability to provide 24/7/365 availability and use.

i) All the major components of the CCTV systems shall be latest but field-proven and shall not be End-of-Life / Outdated; the same shall have to be supported by concerned OEM for at-least 5 years' period from the date of supply.

j) All the cameras shall have 5 Years OEM warranty and the same shall be submitted on OEM letter head.

k) OEM of CCTV should be registered in India for last 5 years directly and not through distributor or Joint Venture. Proof of the same should be attached with the Technical bid.

l) OEM of CCTV shall have local support centre.

m) All the cameras shall have ability to change the GOP/ GOV or HOP/iframe for Bit rate optimization

n) VMS should have ability to select user defined shape for motion detection to include or exclude area to reduce false alarms, bandwidth and storage.

o) All cameras shall have ability to send and receive triggers to perform any action without intervention of VMS.

7.1 Overview

City Safety and Security solution helps protect cities against crime, terrorism, and civil unrest, planning events, monitoring of infrastructure, encroachments etc. It helps law enforcement monitor public areas, analyze patterns, and track incidents and suspects enabling quicker response. Keeping the above perspective, BSCL for this purpose is intending to implement the high definition IP based surveillance cameras across various locations within BSCL. The exact location will be finalized after detailed survey, post award of the contract. The cameras should be housed on the intelligent/street poles. It shall also be possible to adjust the camera focus from a remote location.

Following is an indicative scope of work;

a) Installation and commissioning work includes installation of all required, cameras, monitors, networking, cables laid in PVC conduit etc., commissioning all the systems at the pre-defined locations in the project area
b) The MSI shall prepare the final camera distribution plan at all the camera locations in discussion with BSCL
c) Actual location for placement of pole & number of cameras at each location, type of cameras, fixation of height & angle for the cameras would be done carefully to ensure optimum coverage
d) Bidder should use the industry best practices while positioning and mounting the cameras. Some of the check-points which need to be adhered by the Bidder while installing / commissioning cameras are as follows:
    i. Ensure Project objectives are met while positioning the cameras, creating the required field of view
    ii. Ensure appropriate housing is provided to protect camera from the on field challenges
    iii. Carry out proper adjustments to have the best possible image
    iv. Ensure that the pole /tower/ mast implementation is vibration resistant
e) MSI shall undertake detail assessment for integration of the Surveillance System with the Geographical Information System (GIS) so that physical location of cameras are brought out on the GIS map. Bidder is required to carry out the seamless integration to ensure ease of use of GIS in the Surveillance System Applications/ Dashboards in Command Control Centres. GIS Base Map shall be supplied and integrated by the MSI at 1:1000 scale or better with all surveillance cameras located on the map apart from the updated map of all buildings, utilities and roads. Field survey needs to be done by the MSI. Bidder is required to update GIS maps from time to time. GIS data need to be created that supports rule based model on industry standard such as Topology, Spatial connectivity rules, relationship, GIS layer domains and subtypes, GIS Geometric network, industry specific editing rules and future scalability. MSI is suggested to visit government departments for review and better understanding of available data with them.
f) MSI shall carry out SMS Gateway Integration with the Surveillance System and develop necessary applications to send mass SMS to groups/individuals, which can be either manual or system generated. Any external/third party SMS gateway can be used, but this needs to be specified in the Technical Bid.

g) MSI will have to identify and obtain necessary legal / statutory clearances for erecting the poles and installing cameras, for provisioning of the required power, etc. the same will be facilitated by BSCL. It is important to mention that a timely communication and required follow-up will be required by the MSI for the clearances.
h) During implementation period, in case the pole is damaged by a vehicular accident (or due to any other reason outside the control of MSI) and needs repair, then the MSI will need to repair / have the new pole within 15 days of the incident. Damages are to be borne by MSIs in such cases through proper insurance.
i) For the successful commissioning &operation of the edge devices and to provide the video feeds to Command Control Centre, the MSI will be required to provide electricity to the edge devices through the aggregation points. MSI has to plan the power backup based upon the power situation across the city. MSI may propose solar based powering systems however field devices shall be operational 24x7 and power needs to be calculated accordingly.
j) MSI will be responsible for the solution deployment / customization for implementing end-to-end Surveillance System including its integration with other components as required.
k) MSI will ensure that the best practices for software development and customization are used during the software development/customization and implementation exercise.

7.1.1 Functional & Technical Requirements for VMS

1. Ability to use centralized management system of all field devices, servers and client installed at BSCL and run on any PC and Operating system.. Preferred to use Linux OS in servers to prevent virus attacks and client may be of any OS (windows/Linux/MAC) irrespective of any OS in servers.
2. Ability to integrate with ICCC platform and non-proprietary with perpetual license using open standards
3. Ability to view live video stream by user authorization.
4. Ability to support a distributed architecture with no single point of failure
5. Dockable windows shall include:

   • Site Explorer
   • Alarms/Events window
   • PTZ and advanced telemetry functions
   • Monitors window
   • Maps window
6. Ability to stream direct from camera to client; streaming via a proxy, or intermediate server.
7. Ability to handshake between client and camera shall be done directly.
8. Ability to provide flexible rule-based system driven by schedules, events and workflows.
9. Ability to support IP cameras, Virtualization, Video analytics and storage technologies from major vendors for integration.
10. Ability to support LDAP (Lightweight Directory Access Protocol)l integration
11. Ability to deploy in High availability environment
12. Ability to overlaid cameras in graphical map in the VMS Graphical User Interface (GUI).

13. The cameras selection for viewing shall be possible via clicking in the camera location on the graphical map.

Detailed Specifications

S. No.	Features	Specifications
1	Supported Operating Systems	Linux/Microsoft Windows: 7/8, Microsoft Server 2008 R2/2012, Microsoft Windows Embedded 8 Standard. Support for 32-bit (x86)/64-bit (x64) versions
2	ONVIF Support	ONVIF, ONVIF Profile S Supported Cameras
3	Video Stream Formats	MJPEG, MPEG-4, H.265,H.264 or better
4	Audio Support	YES
5	Resolution	Limited only by the camera
6	Frame Rate	Limited only by the camera
7	Number of servers in the system	Unlimited
8	Number of remote workstations	Unlimited
9	Interface Language	English
10	Archive Materials Storage Format	In the format received from the IP camera
11	Archive Size	Should be able to create different archive sizes per any camera or any group of cameras.
12	File Playback Speed	From single-frame playback up to 32x speed up or better
13	Auto Zoom	Displaying the separate enlarged area with moving objects
14	PTZ cameras	Control of PTZ cameras using the client interface: camera rotation, zoom in/out (optical zoom), focus
15	Panoramic camera support	Support of various modes used in panoramic cameras with just a single VMS license.
16	Cameras auto search	The ability to automatically search for cameras that support ONVIF or UPnP detection protocol in a local network
17	Server backup	Hot backup: in case of server failure, recording is redirected to a backup server
18	Integration with 3rd Party Video Analytics Server	Should support and accept notifications from 3rd Party analytics server.
19	User Interface	Timeline based UI which allows one-click based access to past recordings.
		Timeline should always accessible. No separate interface for viewing recordings.
		The timeline can be hidden so that the camera windows can be shown on the whole screen.

		VMS should support Calendar search and specific time search
		The size and layout of camera windows should be able to be freely adjusted
		Window layouts should be saved per user as per required.
		Automatic arrangement of camera windows should be possible
		Video Wall support and camera window arrangement functionality
		Pre-programmable notifications
		Creation and naming of bookmarks of video.
20	Camera Window Tools	Full screen Mode: Should be able to the selected camera in full screen mode
		Should be able to export the video in the secured Export Format with authentication.
		Should only show the recordings for this camera on the timeline. The playback can be manually jumped to points of motion detection. The motion detection points should be highlighted on the timeline for quick jump to next item..
		The events/motion detections will be shown on the timeline. It should be possible to play pre-alarm /event/motion detections or move to next event.
		Should allow simultaneous viewing of the present time and recordings from the same camera .
		Detach from the main timeline: Should open a separate timeline as a window. The other camera windows should follow the main timeline.
		It should be possible to customize control gates or other external devices with rule-customized buttons or control buttons on maps.
		Screenshot: Saves the visible image as an image file (JPG, PNG or PDF). Resolution can be selected.
21	Remote Use	Compatible with Windows/ Linux / OS X client machines
		Should use TCP/IP connection that can be encrypted.
		Can be connected to multiple network video servers simultaneously.
		Recordings from multiple servers can be synchronized.
		Real-time image and recording transfer online, either full quality or compressed quality can be selected.
		Notification events and alarms are forwarded directly from the server to the user.
		It should be possible to customize recording and saving events/alarms from connected external devices/systems.
22	Notifications	Real-time notification window
		Notifications include a screenshot and a description of the event contents
		Notification colors should be adjustable
		Clicking the notification should open an image recording of the event from the connected camera.
		Bookmarks should be able to be saved directly from notifications

		Should have the capability to have the notification
		Rules should be able to be used to set specific conditions for notifications.
23	Multiple Network Video Recorders Synchronization	Should support viewing synchronized real-time and recorded image feed from multiple servers
		Should support saving views comprised of camera feed from multiple recorders
		Area search for a combination of cameras from different recorders to be able to find a specific individual over a specified time and cameras
		Notifications and alarms from multiple recorders simultaneously
		Saving video clips
24	Bookmarks	Support saving bookmarks in the timeline
		Support naming, editing and removing bookmarks
		Bookmarks should be saved in the bookmark list and should also be visible on the timeline.
		Bookmarks are saved locally.
		Bookmarks can be browsed on the timeline
25	Editable Camera Views	Camera windows can be arranged as wanted
		Camera window layouts can be saved and named
		Frequently used views can be saved as shortcut buttons
		Camera views can contain cameras from multiple recorders
26	Video Clips	Time frame and selected cameras: Saves a grid comprising of selected cameras into a single page or view.
		Events/ Quick search/ area search can be easily exported to video clips for post-event analysis.
		Save as an AVI/MP4.
27	Backup Copies	Saving of full-quality backup copies /video clips
		The start and end points of the backup file/video clip can be freely determined.
		Events/Quick search/area search can be used to detect unwanted movement.
		Backup copies can be viewed using the remote software.
		While opening Events/Quick/area searches it should be possible to create backup file/video clips for a specific time range.
		Screenshots can be saved from the backup file/video clips.
28	Rules& Workflows	Rules can be used to control recorder functionality and external devices as well as to send information on different events
		One or more conditions are set for the rules.
		Conditions can include for example: Schedule, I/O-feed, motion detection, alarm lines, connection loss etc.
		User should have ability to define an adpative workflow procedure containing a list of tasks actions to be taken when an alarm occurs.

		Rules are set actions to be performed when rule conditions are met. Actions can include: Digital output control, notification event/alarm, selecting a PTZ preset, saving a bookmark, sending an email message etc.
		Automatic actions could be executed as automatic tasks in a workflow procedure shall support creating, closing and changing incidents.
29	User Management	Username and password protection, Selecting functions and software areas, Camera access based on user permissions, Remote access selection for users, Camera control selection for users
30	Archival Storage Modes	Storage space is shown as a percentage of total available space.
		Recording time can be specified to a date or a weekly recording schedule may be configured
		User Interface should be able to show the date of the oldest recording
31	Access Groups and Users	The VMS should have the capability to create at least 4 access groups.
		Administrator should have the right to assign the camera to at least one group.
		Different level of access to the camera shall be configurable in the VMS
32	Tours	Tour switching time should be configurable for allowing all the cameras to appear on screen tab wise , tab switch time should be common to all the tabs
33	Software Motion Detection	Smart Motion detection should function with all types of ONVIF conformant cameras regardless of manufacturer.
		Sensitivity and noise reduction should be adjustable.
		VMS Should index the images by time stamp and their unique identifiers.
		Separate motion detection areas with different sensitivity can be set for an image.
		Areas of the image that should not be recorded can be covered via motion detection.
34	Map View	Cameras can be placed in map views and opened directly from the map
		There can be multiple maps e.g. for different floors.
		Maps can include links to other maps.
		Maps are placed in separate movable windows, and several windows can be viewed simultaneously
		Maps can be zoomed and moved by using your mouse inside the window.
		Camera locations can be edited
		Map modification can be turned off
35	Virtual Matrix	Command and Control room interface for real-time surveillance
		Virtual matrix can include one or more screens and should support Video Walls.
		Includes monitor windows and regular camera windows that can be used to record several views

		Image source selection for monitor windows can be automated e.g. based on alarms.
		Cameras selected for monitor windows can be controlled with one or more joysticks.
		Controlled camera can be selected with joystick buttons or mouse.
		Notification events are shown instantaneously from e.g. alarm information or motion detection.
36	Shortcut keys	VMS should have the option of customizing the shortcut keys.
37	Diagnostics	Notification events can be set in the system in different ways, such as rules, motion detection from image, external I/O data, or internal software command.
		Notifications can contain a free text field, event colours are customisable, and a preview image is attached to the notification.
		Status information and preset alarms are saved in the alarm log in chronological order
		The alarm log contains an acknowledgement functionality.
		User can access a recording attached to a notification by one click
38	Person Tracking (City Specific Use case)	Track a specific person identified by the facial recognition system, visual description or general monitoring based on events/alerts etc. across several surveillance cameras. The FRS or other edge devices must be able to provide the full frame of the person for enhanced tracking. The application shall allow access to all relevant associated VMS recordings with following Attribute Based Search Initiators: i. Recorded Video; ii. Photographic images i.e. image as received from the Facial Recognition System or other edge devices; iii. Artificial sketch builder allowing selection of various attributes i.e. body color, male/female/child, Hair styles, Texture and color of cloths, various accessories i.e. Spectacles, Shoes, bag/ suitcase, Tie etc. a. When initiating a query on recorded content, the operator shall initiate the query for a specific VMS video channel and time range in order to precisely get results of individual's signature as indexed in the image database that was generated in real- time by the analytics application. b. The application shall support a list of atleast 20 different textures types. c. The application shall support map images and GIS maps and the movement of the individual should be tracked on the map.

7.1.2 Functional & Technical Requirements for Facial Recognition System

Face recognition system matches faces captured from Face Recognition Cameras against the database of face images and shows the details of the face stored in the database.

The solution has two applications:

A. **Real Time Face Detection & Recognition Solution:** This application detects and analyses the faces captured in real time from any full HD camera. The application does real time video screening and shows the matching results instantly. The application also gives anonymous people analytics.
B. **Offline Search of Facial Images in Database:** This application allows you to compare facial images from different sources to those stored in image database.

There are multiple use cases where these two applications can be implemented:

A. Real Time Face Detection & Recognition Solution
    a. Tracking criminals and persons in the watch list in public areas such as
        i. Airports
        ii. Railway stations
        iii. Bus stands
        iv. Places of religious importance
        v. Public gatherings
        vi. High security areas.
    b. Tracking VIPs for un-obtrusive access control in areas such as
        i. Legislative assemblies
        ii. High security areas
        iii. Airports
B. Offline Search of Facial Images in Database
    a. Recognize people from database in videos collected from different sources
    b. Law enforcement
        i. Identify suspects
        ii. Create match lists
        iii. Search for missing persons
    c. Criminal investigation
        i. Photograph enhancement tools
        ii. Detailed inspection of facial data
        iii. Investigation management – create investigation cases and add probe images
    d. Identity fraud prevention and detection in multiple identities such as passport, Aadhaar, visa, driving license, voter registration

Functional Requirements :

1. Face Recognition System (FRS) shall be designed for identifying or verifying a person from various kinds of photo inputs from digital image file to video source. The system shall offer logical algorithms and user-friendly, simple graphical user interface making it easy to perform the facial matching.
2. The system shall be able to broadly match a suspect/criminal photograph with database created using photograph images available with Passport, CCTNS, and Prisons, State or National Automated Fingerprint Identification System or any other image database available with police/other entity. The system shall be able to:

a. Capture face images from CCTV feed and generate alerts if a blacklist match is found.
b. Search photographs from the database matching suspect features.
c. Match suspected criminal face from pre-recorded video feeds obtained from CCTVs deployed in various critical identified locations, or with the video feeds received from private or other public organization's video feeds.
d. Add photographs obtained from newspapers, raids, sent by people, sketches etc. to the criminal's repository tagged for sex, age, scars, tattoos, etc. for future searches.
e. Investigate to check the identity of individuals upon receiving such requests from Police Stations.
f. Enable Handheld mobile with app to capture a face on the field and get the matching result from the backend server.

3. The facial recognition system shall be enabled at cameras identified by the purchaser.
4. The facial recognition system shall be operated with any Full HD IP camera using standard video stream.
5. The facial recognition system in offline mode shall be provided by the MSI in line with the requirement specified in the RFP.
6. The facial recognition system should be able to integrate with IP Video Cameras as required in the solution and shall be able to identify multiple persons of interest in real-time, through leading-edge face recognition technology. The system shall be able to recognize subjects appearing simultaneously in multiple live video streams retrieved from IP surveillance cameras. The Facial recognition system should seamlessly be integrated to the network video recorders and the video management system.
7. The facial recognition system shall detect and recognize faces with size of 45x45 pixels.
8. The facial recognition system should be able to work on the server/ desktop OS as recommended by OEM and provided by the System Integrator.
9. The user interface of the facial recognition system should have a report management tool on the Web client without installation of any additional client software. It should be able to generate real time report such as Audit log report, Hit List Report, Daily Statistics Report, and Distribution Report.
10. The facial recognition system should be accessible from 5 different desktop/laptops at any given time. When choosing a distributed architecture, the system shall be able to completely centralize the events and galleries from each local station into a unique central station, devoted to management and supervision.
11. The system should have ability to handle initial real-time watch list of 1,000,000 Faces (should be scalable to at least 100 Million faces) and 50 Camera Feeds simultaneously per server and generate face matching alerts.
12. The algorithm for facial recognition or the forensic tool should be able to recognize partial faces with varying angles.
13. The system should be able to detect multiple faces from live single video feed and if possible the appearance of the person.
14. The system should present the full face as well as zoom out of the person body
15. The system should have short processing time (approx 0.2 sec for 1,000,000 DB) and high recognition rate
16. The system should be able to recognize faces regardless of vantage point and any facial accessories/ hair (glasses, beard, expressions)
17. Face detection algorithms, modes and search depths should be suitable for different environments such as fast detection, high accuracy etc. The FRS system shall use GPU

technology instead of Traditional CPUs, to greatly improve the computational performance in crowded environments.

18. The system should be able to identify and authenticate based on individual facial features
19. The system should be compatible with the video management system being proposed by the system integrator
20. The system should have capability for 1:1 verification and 1: N identification matching
21. The system should be able to integrate with other systems in the future such as 'Automatic fingerprint identification system (AFIS)' etc.
22. The system should be able to support diverse industry standard graphic and video formats as well as live cameras
23. The system should be able to match faces from recorded media.
24. The system should be able to detect a face from a group photo
25. The system should be able to detect a face from stored videos of any standard format
26. The system should have bulk process of adding faces in the system
27. The system should be an independent system, with capability to integrate with industry standard Video Management Systems (VMS) for alert viewing.
28. The system should allow users to search or browse captured faces (based on date or time range), export any captured image for external use with a capability to support a Handheld mobile with app for Windows OS or Android OS to capture a face on the field and get the matching result from the backend server.
29. The proposed solution should provide the ability to assign different security levels to people and places. It should alert security staff when someone is spotted in an area where they're not permitted, whilst allowing them free access to non-restricted/public areas.
30. The system should have the facility to categorize the images like "Remember this person" or "hit-list" or "wanted".
31. It should be able to provide information such as Gender & Age Group along with facial detection/match data.

Hardware Specification:

Bidder to specify and provide minimum specification of hardware with license as required for implementation of above FRS and integration with VMS to meet the specification of the facial recognition system. A suggested server specifications are provided in the below table :

Sr. No.	Server Type
1	FRS-– Master Server (Database) – 1000,000 Live Templates
2	FRS — Stream Processing Servers (50 Cameras)
3	FRS — Social Media/Offline Database Matching
4	Viewing Workstations

7.1.3 CCTV Camera:

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

a) Information to be Captured by Edge Devises

i. Cameras need to work on 24 X 7 basis and transmit quality video feeds to the centralized Data Center
ii. Capture the video feeds at 25 FPS for majority of the time and at 8 FPS for the lean period
iii. Video feeds may be stored at higher FPS (i.e.25), for recorded evidence for future investigation, even for lean time
iv. The complete tracking of the vehicle is to be made possible on the GIS map to locate any suspicious / identified vehicle

b) Information to be analyzed at the ICCC

i. The Video Management System should provide a complete end-to-end solution for security surveillance application
ii. The control center shall allow an operator to view live / recorded video from any camera on the IP network
iii. The combination of control center and the IP network would create a virtual matrix, which would allow switching of video streams around the system
iv. Not all the cameras would be simultaneously viewed at ICCC
v. This shall from time to time help take decisions on utilization of Alerts / Exceptions / Triggers generated by cameras, and specify the client machines where these would get populated automatically

c) Role Based Access to the Entire System

i. Various users should have access to the system using single sign on and should be role based
ii. Different roles which could be defined could be Administrator, Supervisor, Officer, Operator, etc.
iii. Apart from role based access, the system should also be able to define access based on location
iv. The CCTV Surveillance System shall have the standard authentication mechanism to ensure only authorized users have access to the system.
v. The management module should be able to capture basic details (including mobile number & email id, Police Personnel & other personnel requiring Viewing / Administration rights to the system
vi. There should be interface to change these details, after proper authentication
vii. Rights to different modules / sub-modules / functionalities should be role based and proper log report should be maintained by the system for such access

viii. Authorization coupled with login name & password should be enabled to ensure that only the concerned personnel are able to login into the system

ix. Surveillance System should have capability to map the cameras to the police personnel from different Police Stations. There should be interface to change these mappings too

x. For PTZ cameras, there should be provision to specify hierarchy of operators / officers for control of the cameras from various locations

xi. Windows Active Directory/LDAP or any such system can be used to design role based access

d) Information to be made available to different Police Stations

i. The Video Management System shall provide a complete end-to-end solution for security surveillance application

ii. The ICCC shall allow an operator of any Police Station to view live / recorded video from any camera on the IP network

iii. The combination of control center and the IP network would create a virtual matrix, which would allow switching of video streams around the system.

iv. Authority personnel shall have following access to the video feeds of the cameras of their jurisdiction:

- Viewing rights to all the live Camera Feeds
- Viewing rights to the stored feeds, stored on Primary / Secondary Storage
- Ability to view stored feeds from collaborative public CCTV surveillance system
- Access to view Alerts / Exceptions / Triggers raised
- Trail Report on specific person / object / vehicle for a specific period / location
- Personalized Dashboard (depending upon grade of police officer, detailed requirement finalization will be done during Pre-Implementation stage)
- Accessibility to advanced analytics on recorded footages
- Provide search of recorded video
- Advanced search should be possible based on various filters like alarm / event, area, camera, etc.

e) Storage/Recording Requirements

It is proposed that the storage solution is modular enough to ensure compliance to the changes in storage / recording policy, to be evolved upon initial deployment of the system. Following storage requirements are proposed for the project:

i. 30 days of storage for all camera feeds

ii. Archival/Backup to be done on NAS / Scale-out NAS / SAN / Unified or equivalent storage solution

iii. Data on storage would be over-written automatically by newer data after the stipulated time period
iv. If some data is flagged by police personnel (or by designated personnel) as important data / evidence data due to some reporting of crime 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
v. Police Department would analyze such flagged data every 3 months to take such decisions for preservation of the flagged data beyond 90 days
vi. Full audit trail of reports to be maintained for 90 days
vii. Retrieval time for any data stored on secondary storage should be max. 4 hours for critical data & 8 hours for other data
viii. The recording servers / system, once configured, to run independently of the Video Management system and continue to operate in the event that the Management system is off-line
ix. The system to 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
x. The system to support H.265, H.264 or better, MPEG-4 and MJPEG compression formats for all analog cameras connected to encoders and all IP cameras connected to the system
xi. The system to record the native frame rate and resolution supplied by the camera or as configured by the operator from the system administration server
xii. The system should not limit amount of storage to be allocated for each connected device
xiii. The system to allow for the frame rate, bit rate and resolution of each camera to be configured independently for recording
xiv. The system to 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
xv. The system to 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
xvi. Archiving to allow the duration of the camera's recordings to exceed the camera's default database capacity
xvii. Archives to be located on either the recording server or on a connected network drive
xviii. If the storage area on a network drive becomes unavailable for recording, then system/EMS should have the ability to trigger actions such as the automatic sending of email alerts and sound alerts to necessary personnel.

Image and Video Enhancement:-

Sr. No	Feature	Functionality
1	Image Format	Should take input from any standard image format (i.e. jpeg, tiff, png, bmp, targa, etc.…).
2	Video Format	Should take input from any standard video format (avi, flv, 3gpp, wmv, mov), also without the need of the codec installed on the system. Expandable by system codecs.
3	Capture Playback	Should have screen capture utility to capture playback from DVR console display or proprietary player to avoid conversion and downscale issues
4	Proprietary File Conversion	Should Convert proprietary surveillance video files to a standard AVI format like H264
5	Print Image	Should allow Print generated images.
6	Report Generation	Should allow automatic generation of a report containing all the scientific methodology and details of the processing steps, settings, and the bibliographic references to the algorithms in HTML format.
7	Track Targets or Areas of Interest	Should allow to track areas, people, objects through static, dynamic, and custom tracking.
8	File Verification	Should Verify alteration of image and video files in saved projects using hash function.
9	File information	Should display information about the file formats.
10	Exif data	Should display Exif data contained in digital images.
11	Hash Code	Should display Hash Code specific to saved files
12	Image information	Should display current image morphological and statistical features.
13	Video playback	Should have advanced video playback with frame by frame navigation, adjustable frame rate and jog controls.
14	Visualization	Should have custom zoom on an area of the image and color space selection.
15	Processing Workflow	Should allow display of Instant results like: add, configure, move, and modify an unlimited number of filters, in real time even while playing video. User can apply real-time, non-destructive image adjustments that don't require re-rendering as changes are applied.
16	Samples and tutorial	Should have a rich collection of examples and video lessons to start from basics and face the most common cases.
17	Supported Platform	Should support Microsoft Windows
Should Support Following Dynamic Filters		
Sr. No	Filter	Functional Description
1	LOAD	Loads image and video files
2	Image Loader	Loads an image from file
3	Sequence Loader	Loads a list of images as video
4	Video Loader	Loads a video from file
5	Image Paster	Pastes the image in the clipboard for further processing.

Sr. No	Feature	Functionality
6	Video Input	Live feed from DirectShow video sources.
7	LINK	Connects and mixes different source filters.
8	Video Mixer	Overlays or put side by side two different chains
9	WRITE	Writes image and video files
10	Image Writer	Writes the current image to a file
11	Sequence Writer	Writes all frames as image files
12	Video Writer	Writes the current video to a file.
13	SELECT FRAMES	Selects video frames
14	Single Selector	Selects a single frame of the video
15	Range Selector	Selects frames of the video within an interval with an optional step
16	Sparse Selector	Selects a list of frames in random positions
17	Remove Duplicates	Removes duplicated frames
18	Auto Selector	Automatically selects similar frames (for discarding bad frames)
19	IFrames Selector	Select only I frames
20	Demultiplexer	Separates different scenes multiplexed in the same video
21	Motion Detection	Fast seek of events in a video
22	Reverse	Plays back the video in the reverse direction.
23	EDIT	Edits image geometric features.
24	Crop	Crops a region of interest of the image
25	Flip	Mirrors the image
26	Rotate	Rotates the image
27	Resize	Resizes the image (zoom)
28	Smart Resize	Resizes the image with a smart zoom algorithm
29	Correct Perspective	Removes the perspective effect on a plane of interest in the image
30	Deinterlace	Converts interlaced videos into progressive ones
31	Field Shift	Aligns the two fields of an interlaced frame
32	Undistort	Corrects the geometric distortion, caused by capturing devices' optics.
33	Correct Aspect Ratio	Correct the aspect ratio of field based video.
34	Interleave	Converts a video with juxtaposed fields into an ordinary interlaced video.
35	Correct Fisheye	Compensate the distortion of common fisheye lenses.
36	Unroll	Converts an omnidirectional image to a panoramic one.
37	CHANNELS	Color conversion and extraction functions
38	Grayscale Conversion	Converts the image into grayscale
39	Color Conversion	Converts the image from grayscale to RGB
40	Color Switch	Exchanges R and B color channels in the image
41	Extract Channel	Extracts a single channel from the image
42	Enable Channels	Displays only selected color channels
43	ADJUST	Adjusts image values
44	Contrast/Brightness	Adjusts the contrast and brightness values
45	Exposure	Adjusts the image exposure to correct improper camera settings

Sr. No	Feature	Functionality
46	Hue/Saturation/Value	Adjusts the hue, the saturation and the color value of the image
47	Curves	Adjusts the tone values according to the desired curve
48	Levels	Adjusts intensity and color levels
49	Histogram Equalization	Improves the image contrast by equalizing the histogram of its values
50	CLAHE	Applies a contrast limited histogram equalization.
51	Contrast Stretch	Improves the image contrast by expanding the range of intensity values
52	EXTRACT	Extracts and analyzes image features.
53	Negative	Negative of the image
54	Threshold	Cuts image values to the desired threshold(s)
55	Adaptive Threshold	Extracts edges with adaptive threshold algorithm.
56	Laplace	Extracts the edges with a Laplacian filter
57	Sobel	Extracts the edges with a Sobel filter
58	Scharr	Extracts the edges with a Scharr filter
59	Canny	Extracts the edges with a Canny filter
60	Linear Filter	Filters the image with a user-defined kernel.
61	Bilinear Filter	Filters the image with two user-defined kernels and combines the results.
62	Channel Mixer	Mixes the ratio of color in every channel
63	Color Deconvolution	Maximizes the differences between specific colors in the image.
64	Component Separation	Separates different informative components in an image
65	Fourier	Removes periodic noise, backgrounds and interferences in the Fourier domain
66	VERIFY FILE	Verifies digital image and video files
67	File Info (EXIF Data)	Saves file information and EXIF metadata from the original media in the report
68	Hash Code	Calculates input file hash code and check integrity loading the project
69	MEASURE	Extracts real-world measurements from the image
70	Measure 1d	Takes a measure on the planar image in 1 dimension
71	Measure 2d	Takes a measure on planar image after perspective correction in 2 dimensions
72	Measure 3d	Takes a measure on the image with a 3d reconstruction model of the perspective
73	SHARPEN	Enhances image details.
74	Laplacian Sharpening	Sharpens the image using a Laplacian filter.
75	Unsharp Masking	Sharpens the image using unsharp masking filter.
76	DENOISE	Reduces the image noise.
77	Averaging Filter	Smooths the image with an averaging filter.
78	Gaussian Filter	Smooths the image with a Gaussian filter.
79	Bilateral Filter	Smooths the image with a bilateral Gaussian filter.
80	Median Filter	Reduces the impulsive noise with a median filter.
81	Wiener Filter	Smooths the image with a Wiener filter
82	Deblocking	Reduces block artifacts from lossy compression.

Sr. No	Feature	Functionality
83	DEBLURRING	Reduces image blurring
84	Motion Deblurring	Corrects the blur of moving objects
85	Optical Deblurring	Corrects the blur of objects which are out of focus (big blur)
86	Nonlinear Deblurring	Corrects the blur caused by nonlinear motion
87	Blind Deconvolution	Corrects the blur of objects out of focus with blind deconvolution (little blur)
88	Turbulence Deblurring	Corrects the blur caused by air turbulence at long distances
89	STABILIZATION	Stabilizes video frames
90	Local Stabilization	Stabilizes a shaking video keeping steady the current selection
91	Global Stabilization	Stabilizes the overall scene of a shaking video
92	Perspective Registration	Aligns the perspective of different images of the same object, taken from different points of view.
93	INTEGRATE	Enhances image by multiple frames
94	Temporal Smoothing	Reduces the noise integrating current and previous frames
95	Motion Smoothing	Reduces the noise integrating current and previous frames and avoiding halos on moving objects
96	Frame Averaging	Reduces the noise by creating an image which is the average of all the frames
97	Super Resolution	Merges all frames to improve the resolution of the image
98	PRESENTATION	Prepares a video or image for presentation
99	Add Timestamp	Indicate date and time for the current frame
100	Add Text	Insert text on the image.
101	Add Shape	Select and draw shape on current frame
102	Hide Selection	Pixelizes, darkens or blurs an area of interest in a video (witness protection)
103	Change Frame Rate	Change the frame rate of the video
104	Spotlight	Adds a spotlight effect to a selection
105	Compare Original	Juxtaposes or overlays original and enhanced image for comparison
106	Load Timestamp	Displays subtitles on the video frame
107	Load Subtitles	Displays content from embedded subtitle files on the video frame

Advanced image authentication Tool:-

Sr. No	Feature	Functionality
1	Supported Formats	The system shall support for any standard image format (jpeg, tiff, bmp, png...) and raw format from digital cameras.
2	Available filters	The system shall have more than 20 different analysis filters, with user customizable configuration and optional post processing parameters (levels, scale to enhance the displayed image).
3	Image Display	The system shall have embedded viewer with multiple image comparison and synchronization.
4	Comparison Support	The system shall have filters to allow comparison of the results between two images.
5	Output Image Export Options	The system shall support for any standard image format (jpeg, tiff, bmp, png...).
6	Output Data Export Options	The system shall have Export analysis output as plain text, HTML, or TSV.
7	Cached Processing	The system shall have filter results saved in a cache folder for speedy subsequent analysis.
8	Batch Processing	The system shall automatically apply all filters to all images in a folder.
9	Batch File Format Analysis	The system shall have Quick automatic analysis of the format of all images in a folder to find suspicious files (triage).
10	Batch File Format Comparison	The system shall have Quick automatic comparison of the format of all files in a folder with the analyzed image.
11	Batch JPEG Comparison	The system shall have Quick automatic comparison of the quantization tables of all files in a folder with the analyzed image.
12	Excel Integration	The system shall support Export of multiple file analysis table directly to spreadsheets for further processing.
13	Google Maps Integration	The system shall support display image location in Google Maps.
14	Google Images Integration	The system shall support search for similar images and images from a certain specific camera on Google Images. Supports advanced image features filtering.
15	Flickr Integration	The system shall support search for images from a certain camera on Flickr. Supports advanced image features filtering.
16	Reverse Image search engine Integration	The system shall support search for similar images on TinEye like reverse image search engine to make use of image identification technology rather than keywords, metadata or watermarks.
17	Extraction Of Embedded JPEGs	The system shall support to Extract JPEG images embedded in any file type (PDF, PPT, DOC, disk image...) for questioned document authentication support.
18	Supported Platforms	Windows XP, Vista, 7, 8. 32 bit and 64 bit version in a single installer.

7.1.3.1 Functional & Technical Requirements for Outdoor Fixed Cameras(HD)

S.No	Features	Specifications
1.	Form Factor	Box Type / Bullet Camera
2.	Image Sensor	1/2.8" Progressive CMOS
3.	Day/ Night Operation	ICR with IR range of 100m or better
4.	Minimum Illumination	Color 0.005 lux , B/W 0.0005 lux
5.	Lens	External Lens (5 mm to 50 mm)
6.	Electronic Shutter	1 ~ 1/10000 sec.
7.	Image Resolution	1920X1080 @ 30 fps (2MP)or better
8.	Compression	MJPEG, H.265,H.264 or better
9.	Frame Rate and Resolution	Full HD (2MP 1920x1080 or better) @ 25/30 FPS
10.	Simultaneous Stream	Minimum 3 streams should be configurable at 1920 X 1080 @ 25 fps simultaneously
11.	White Balance	Auto / Manual / ATW / One Push
12.	Noise Reduction	3DNR / 2DNR / Color NR
13.	Zoom	Digital Zoom
14.	Video Streams	Three Stream supportable , All stream should be H.265
15.	Image Setting	Saturation, Brightness, Contrast, Sharpness, Hue adjustable
16.	Two way audio	Line in / Line out
17.	Audio Compression	G.711 / G.726 / AAC / LPCM
18.	Iris	P – Iris /Auto-Iris
19.	Wide Dynamic Range	120 dB
20.	Alarm	1 x Input / 1 x output
21.	Edge Video Content Analytics	Camera should have in-built Edge Based Analytics, Abandoned Object, Intrusion Detection, Tampering, Line Crossing, Loitering Detection, Object Removal
22.	Network Interface	1 x RJ45
23.	Storage backup on network failure	Camera should support network failure detection , Camera should have the capability to start the recording automatically on SD card(32 GB min at all locations) in case of connectivity between camera and NVR/Storage device goes down
24.	Protocols	ARP, IPv4/v6, TCP/IP, UDP, RTP, RTSP, HTTP, HTTPS, ICMP, FTP, SMTP, DHCP, PPPoE, UPnP, IGMP, SNMP, QoS, ONVIF
25.	Text Overlay	Date & time, and a customer-specific text etc.
26.	Security	HTTPS / IP Filter / IEEE 802.1X
27.	Firmware Upgrade	The firmware upgrade shall be done though web interface, the firmware shall be available free of cost
28.	Power	PoE / DC 12V / AC 24V

S.No	Features	Specifications
29.	Operating Temperature	0°C ~ 60°C
30.	Operating Humidity	,10% ~ 90%, No Condensation
31.	Certification	UL , CE , FCC
32.	ONVIF	ONVIF profile S & G
33.	User accounts	10
34.	Supported Web Browser	Internet Explorer (7.0+) / Firefox / Safari

7.1.3.2 Functional & Technical Requirements of Dome Cameras

S.No	Features	Specifications
1.	Form Factor	Dome
2.	Image Sensor	1/2.8" CMOS or better
3.	Day/ Night Operation	Yes with IR Cut Filter
4.	Minimum Illumination	Color 0.04 lux ,B/W 0.002 lux
5.	Lens	2.8 - 12 mm, Auto-Iris / P-Iris, motorized, Megapixel Lens with remote zoom and focus
6.	Electronic Shutter	1 ~ 1/10,000 s
7.	Image Resolution	Full HD (2MP or better)
8.	Compression	MJPEG, H.265,H.264 or better
9.	Frame Rate and Resolution	H.264, 2 MP (1920 X 1080) @ 25/30 FPS
10.	Simultaneous Stream	Minimum 3 streams should be configurable at 1920 X 1080 @ 25 fps simultaneously
11.	White Balance	Auto / Manual / ATW / One Push
12.	Noise Reduction	Digital Noise Reduction 2D / 3D DNR
13.	Zoom	3x optical Zoom , 10x Digital Zoom
14.	Digital PTZ	Camera should support digital PTZ
15.	Video Streams	Three Stream supportable , All stream should be H.265
16.	Video quality view	Video compression type (H.264/H.265/MJPEG) and bit rate of each stream should be viewable on home screen
17.	Image Setting	Saturation, Brightness, Contrast, Sharpness, Hue adjustable
18.	Two way audio	Line in / Line Out
19.	Audio Compression	G.711 / G.726 / AAC / LPCM
20.	Iris	P-Iris / Auto-Iris

S.No	Features	Specifications
21.	Wide Dynamic Range	120 dB or better
22.	IR	At least 20 mtr IR distance
23.	Alarm	1 x Input / 1 x output
24.	Edge Video Content Analytics	Camera should have in-built Edge Based Analytics, Abandoned Object, Intrusion Detection, Tampering, Line Crossing, Loitering Detection, Object Removal
25.	Storage backup on network failure	Camera should support network failure detection , Camera should have the capability to start the recording automatically on SD card (min 32GB for all locations) in case of connectivity between camera and NVR/Storage device goes down
26.	Network Interface	RJ-45, 10/100Mbps Ethernet
27.	Edge Storage	Built in SD card slot with support up to 128 GB SD card
28.	Protocols	IPv4/v6, TCP/IP, UDP, RTP, RTSP, HTTP, HTTPS, ICMP, FTP, SMTP, DHCP, PPPoE, UPnP, IGMP, SNMP, QoS, ONVIF
29.	Text Overlay	Date & time, and a customer-specific text etc.
30.	Security	HTTPS / IP Filter / IEEE 802.1X
31.	Firmware Upgrade	The firmware upgrade shall be done though web interface,
32.	Enclosure	IP 66 weather proof ,
33.	Vandal Resistant	IK 10
34.	Power	POE / 12 V DC /24 V AC
35.	Operating Temperature	As per City requirement
36.	Operating Humidity	Humidity 10%–90% No Condensation
37.	Certification	UL, CE, FCC, RoHS
38.	ONVIF	ONVIF Profile S & G
39.	User accounts	10
40.	Supported Web Browser	Internet Explorer (7.0+) / Firefox / Safari

7.1.3.3 Functional & Technical Requirements of PAN, Tilt & Zoom(PTZ) Camera

S. No.	Parameters	Specifications
1.	Certifications	UL ,CE,FCC
2.	Compatibility	ONVIF profile S , G and Q
3.	Sensor	1/2.8" Progressive scan CMOS
4.	Resolution	Min 2 MP (1920X1080)
5.	Multiple Stream	Triple Stream
6.	Frame Rate	upto 25 fps @ 2 MP
7.	Focal Length	4-6mm to 120-180mm
8.	Field Of view	61.2° - 2.32 ° or better
9.	Optical Zoom	30X
10.	Digital Zoom	16X
11.	Focus	Auto / Manual
12.	WDR	120 dB
13.	Noise Reduction	2D / 3D
14.	Shutter Speed	1/1 ~ 1/10000 sec.
15.	IR	Inbuilt IR , IR distance up to 150 mtr
16.	Day & Night	IR Cut filter
17.	Min Illumination	0.05 @ F1.6 (Color), 0 (B/W) @ F1.6
18.	Iris	Auto-Iris / P-iris
19.	Edge Video Content Analytics	Camera should have in-built Edge Based Analytics, Abandoned Object, Intrusion Detection, Tampering, Line Crossing , Loitering Detection, Object Removal
20.	Storage backup on network failure	Camera should support network failure detection , Camera should have the capability to start the recording automatically on SD card in case of connectivity between camera and NVR/Storage device goes down
21.	Edge Storage	Built in SD card slot with 128 GB SD card with class 10 speed.
22.	Video Compression	H.265,H.264 or better
23.	Privacy Mask	Min8 privacy zones
24.	Audio	2 Way audio
25.	Audio Compression	G.711 / G.726 / AAC
26.	PAN	360 ° endless , Manual speed 0.1° ~ 90°/s , preset speed 9° ~ 240°/s
27.	Tilt	-15 ° ~ 90° , Manual speed 0.1° ~ 60°/s , Preset speed 7° ~ 240°/s , Auto flip
28.	Presets	256
29.	PTZ Operation	8 sequence , 8 cruise
30.	Speed by zoom	On / Off (Pan and tilt speed proportional to zoom ratio)
31.	Home Function	Preset / Sequence / Auto pan / Cruise
32.	Calibration	Auto(On/Off)
33.	Resume after power loss	Supported zero downtime power switching
34.	Protocols	IPv4/v6, TCP/IP, UDP, RTP, RTSP, HTTP, HTTPS, ICMP, FTP, SMTP, DHCP, PPPoE, UPnP, IGMP, SNMP,

		QoS, ONVIF
35.	Security	HTTPS / IP Filter / IEEE 802.1x
36.	Alarm	2 Input / 1 Output
37.	Alarm response	Preset / Sequence / Auto Pan / Cruise
38.	Ethernet Interface	1 X RJ 45
39.	Supported Web browser	Internet Explore (10.0+) / Firefox / Safari
40.	Weather Proof	IP 66 / NEMA-4X-rated casing
41.	Operating Temperature	As per city Requirements
42.	Power Supply	802.3at (PoE+) 4-Pair 60W / AC 24V ± 20% / DC 12V
43.	Power Consumption	45W or less (with IR & Heater on)

7.1.3.4 Functional & Technical Requirements of Outdoor Dome Camera

S.No	Features	Specifications
1.	Form Factor	Dome
2.	Image Sensor	1/2.8" CMOS or better
3.	Day/ Night Operation	Yes with IR Cut Filter
4.	Minimum Illumination	Color 0.04 lux ,B/W 0.002 lux
5.	Lens	2.8 - 12 mm, Auto-Iris / P-Iris, Motorized, Megapixel Lens with remote zoom and focus
6.	Electronic Shutter	1 ~ 1/10,000 s
7.	Image Resolution	2MP or better
8.	Compression	MJPEG, H.265,H.264 or better
9.	Frame Rate and Resolution	2 MP (1920 X 1080) @ 25/30 FPS
10.	Simultaneous Stream	Minimum 3 streams should be configurable at 1920 X 1080 @ 25 fps simultaneously
11.	White Balance	Auto / Manual / ATW / One Push
12.	Noise Reduction	Digital Noise Reduction 2D / 3D DNR
13.	Zoom	3x optical Zoom , 10x Digital Zoom
14.	Digital PTZ	Camera should support digital PTZ
15.	Video Streams	Triple Stream supportable , All stream should be MJPEG, H.265,H.264 or better
16.	Video quality view	Video compression type (H.264/H.265/MJPEG) and bit rate of each stream should be viewable on home screen
17.	Image Setting	Saturation, Brightness, Contrast, Sharpness, Hue adjustable
18.	Two way audio	Line in / Line Out
19.	Audio Compression	G.711 / G.726 / AAC / LPCM
20.	Iris	Auto-Iris / P-iris
21.	Wide Dynamic Range	120 dB or better
22.	IR	Min 20 mtr IR distance
23.	Alarm	1 x Input / 1 x output

24.	Edge Video Content Analytics	Camera should have in-built Edge Bases Analytics, Abandoned Object, Intrusion Detection, Tampering, Line Crossing, Loitering Detection, Object Removal
25.	Storage backup on network failure	Camera should support network failure detection , Camera should have the capability to start the recording automatically on SD card in case of connectivity between camera and NVR/Storage device goes down
26.	Network Interface	RJ-45, 10/100Mbps Ethernet
27.	Edge Storage	Built in SD card slot with 128 GB SD card with Class 10
28.	Protocols	IPv4/v6, TCP/IP, UDP, RTP, RTSP, HTTP, HTTPS, ICMP, FTP, SMTP, DHCP, PPPoE, UPnP, IGMP, SNMP, QoS, ONVIF
29.	Text Overlay	Date & time, and a customer-specific text etc.
30.	Security	HTTPS / IP Filter / IEEE 802.1X
31.	Firmware Upgrade	The firmware upgrade shall be done though web interface,
32.	Enclosure	IP 66 weather proof ,
33.	Vandal Resistant	IK 10
34.	Power	POE / 12 V DC /24 V AC
35.	Operating Temperature	0 °C to 60 °C
36.	Operating Humidity	Humidity 10%–90% No Condensation
37.	Certification	UL, CE, FCC, RoHS
38.	ONVIF	ONVIF Profile S & G
39.	User accounts	10
40.	Supported Web Browser	Internet Explorer (7.0+) / Firefox / Safari

7.1.3.5 Functional & Technical Requirements of ANPR Camera

S.No.	Features	Specifications
1	General	The entire ANPR process shall be performed at the lane location in real-time. The information captured of the plate alphanumeric, date-time, and any other information required shall be completed in approximately a few milliseconds. This information shall be transmitted to the Control Room for further processing if necessary, and/or stored at the lane for later retrieval.
2	Lane Coverage	Each camera system covers at least 1 lane having width of 3.5 meter or more.
3	Detection Zone	5 m to 6 m for ANPR data
4	Maximum Vehicle Speed	System captures clear images of all vehicles moving at a speed up to 200 km/hr.
5	Vehicle Detection and Video Capture Module	The System shall automatically detect the license plate of all vehicles in the camera view in real time using video detection and activates license plate recognition software.

S.No.	Features	Specifications
6	Optical Character Recognition	The system shall perform OCR (optical character recognition) of the license plate characters in real time. (English alpha-numeric characters in standard fonts). OCR accuracy shall be at least 90% during day time and 85% during night time for standard number plate . System is able to detect and recognize the English alphanumeric License plate in standard fonts and formats of all vehicles including cars, HCV, LCV and two wheelers. The system is robust to variation in License Plates in terms of font, size, contrast and colour.
7	Network	Connectivity from site to control room shall be through reliable networks and proper encryption tools should be available.
8	Data capture and transfer	The OCR data of all vehicles along with the JPEG image of the vehicle etc. shall be automatically transferred immediately to the nominated server in the Control Room.
		Each vehicle record shall be a single file and shall contain, as a minimum, an ASCII header that
		contains the following:
		a) vehicle registration number
		b) date and time that the vehicle is identified
		c) OCR confidence level
		d) ANPR site location, and
		It shall be possible to include one or more of the following in the same single vehicle record:
		a) image of the number plate
		b) image of the front of the vehicle from the ANPR IR camera, and/or
		c) wide angle vehicle / lane image (with additional scene camera).
		A detailed description of the file format can be finalized by the user to further develop post processing software.
9	OCR Data edit	To ensure 100% accuracy of data in the database, the system shall have provision to edit the incorrect OCR data. This shall be done by viewing of the plate image transferred along with the plate OCR data. An audit trail shall be maintained to record such editing activities.
10	Hot List creation	The system shall have option to input certain license plates according to hot listed categories like “Wanted”, “Suspicious”, “Stolen” etc. The system can generate automatic alarms to alert the control room personnel for further action, in the event of detection of any vehicle falling in the Hot listed categories.
11	Alert Generation	On successful recognition of the number plate, system shall be able to generate automatic alarm to alert the control room for vehicles which have been marked as "Wanted", "Suspicious", "Stolen", etc.
12	Data Storage	The System shall store JPEG image of vehicle and license plate into a database management system like MySql, PostgreSQL etc. along with date timestamp and site location details.
13	Data Retrieval and Reports	The system shall enable easy and quick retrieval of snapshots, video and other data for post incident analysis and investigations. Database search could be using criteria like date, time, location and

S.No.	Features	Specifications
		vehicle number. The system shall be able to generate suitable MIS reports as desired by the user. The system shall also provide advanced and smart searching facility of License plates from the database.
14	Context camera	System should have possibility to add context camera
15	Vehicle Counting and Classification	The system shall automatically count and classify vehicles with additional Sensors
16	Integration with Third Part VMS	The system should be integrated with the proposed Video Management System.
17	Centralization	The solution proposed should have proper centralization of ANPR data which can provide back up, update of data base, black list of vehicles and clear visualizations of systems in the MAP.
18	Testing	Testing will be conducted in presence of authorized Traffic police officer to determine the accuracy percentage in the following manner: i. Detection accuracy: No. of Undamaged Standard Plates detected / No. of Undamaged Standard plates passed. ii. OCR accuracy: No. of Undamaged Standard plates with correct OCR / No. of Undamaged Standard plates detected.

User Minimum Requirement:

S.No.	Features	Specifications
1	Camera	2 Megapixel IP camera Make: Certified Camera for the Purpose as per certificate
		Shutter Speed 1/1000th sec or better.
		5 – 50mm varifocal lens, IR corrected or as per site requirement to meet the desired functional and technical specifications.
		(see details specifications in Camera sheet)
2	Illuminator	Integrated external Infrared capable to take images in night time and detect automatically number plate at distance of minimum 25 meters.
3	Processing unit	The industrial processor used should be able to work with 2 cameras. Should be minimum multicore , RAM 2 GB, with SD storage and USB storage options, temp -5 to 65 degrees and should consume max. 25 W. The specification for LPU are minimum and OEM should provide industrial LPU as required for his application
4	Outdoor equipment housing	IP66 of better standards capable of withstanding vandalism and harsh weather conditions.(certification to be produced)
5	Data Storage at site	The output of the OCR process and all captured images shall be stored on an industrial processing unit (with internal solid-state memory storage device and can work up to 70 degrees) housed in the ANPR field cabinet. When the data storage reaches capacity, the image processor shall automatically over-write the oldest data. The

		system should push data automatically to data centre in central site and raise alarms if any

7.1.3.6 Functional and Technical Requirements of RLVD:

S.No.	Features	Specifications
1	General	System should be totally digital
2	Vehicle violation criterion at Intersection	The system shall detect and capture vehicle details when:
		(a) It violates the stop line/zebra crossing
		(b) It violates the red light signal
		Option for Spot Speed
		(c) It violates the speed limit in any phase (red or green or even when the signal is not working) in places where instant speed system is installed along with RLVD system.
3	Red Light detection	System shall be Non-Intrusive. It shall not be connected with traffic light and red light status is detected without any physical connection to traffic light.
4	Fair System	Red light system shall be completely fair system with all evidences captured before and after the red light jumping infraction has happened.
5	Lane Coverage	Each camera system shall cover at least 1 lane having width of 3.5 meter or more.
6	Detecting Vehicle Presence	Red light system should detect vehicle presence without intrusive sensors like magnetic loops. This is to avoid street working during installation and to reduce maintenance cost
7	System Mounting	System can be composite unit with all components inside the IP65 box OR comprised of camera or other units mounted on poles or gantries with controller and processors at side poles to make sure all lanes of the road are covered.
8	Number Plate Capture	System should be able to recognize automatically the number plate of cars in violation.
		The system shall perform OCR (optical character recognition) of the license plate characters (English alpha-numeric characters in standard fonts). ANPR system works with Indian number plates
9	Accuracy of Number Plate capture (ANPR)	OCR accuracy shall be at least 90% during day time and 85% during night time.

S.No.	Features	Specifications
10	Infraction data to be provided by system	Date, time, location of incident image of vehicle, speed, Image of the number plate, text conversion of number plate after OCR
		At least one image for over-speeding violation and at least six images for pre and six images for post infraction for red light over jumping
11	Context Image	System shall provide Context image (always color to have proof of signal light) of the signal and shall show wide angled context of the offence as well as details of the offending vehicle.
		Multiple stitched images of the same is possible.
		The system shall produce, store and transmit a sequence of at least 6 image relatives to red light violation, or a movie in standard format like avi, mp4, mov, vfwetc
12	Data Retrieval and Reports	Database search could be using criteria like date, time, location and vehicle number. The system is able to generate suitable MIS reports as desired by the user.
13	IP camera for License Plate Capture	The system shall support all standard brands. One camera shall cover at least 3.5 meter width of lane, and capture the license plates of vehicles which violates the traffic signal and moving at a speed of 0 to 200 km/hr
14	IR Illuminator	Integrated external Infrared shall be capable to take images in night time and detect automatically number plate at distance of minimum 20 meters.
15	Working temperature	0 to +60 deg.C
16	Security	Standard Digital signature on each violation to assure data integrity. Strong encryption on data during local storage and data transfer to back office
17	Local Storage	Minimum local storage 64 GB
18	Communication	Connectivity from site to control room shall be through fibre optic/leased lines or better with minimum uptime of 99.5%
19	Alert Generation	On successful recognition of the number plate, system shall generate automatic alarm to alert the control room for vehicles which have been marked as "Wanted", "Suspicious", "Stolen", "Expired".
20		CE and RoHS compliant certificate

S.No.	Features	Specifications
	Compliance Certificate	
21	Test reports	Third party (authorized company to do so) speed test reports can be submitted to client. On field detailed speed test reports for more than 120-200 km/hr with various speed limits. Alternatively, the system should be approved and homologated by some traffic or infrastructure department who directly over sees fine generation. or A certificate/test report from reputed research institutes accredited and recognized by Govt of India is acceptable. Certificate on the accuracy from any IPS officer for ±2 kmph and running satisfactorily in Indian city for at least an year is a must.
22	BACK office software	The system should provide facility to privileged users to manually check the entry in database using standard Web browsers and edit the numbers which may be wrongly OCR-read, before the numbers are fed to the Challan generating sub-system. An audit trail should be maintained to record such editing activities.
		No deletion or addition of data without validation , proper password protection
		The system should provide facility to search for the cases of violations occurred during any specific span of time, and provide a statistical analysis of the number of such incidences occurring during various days of the month
23	Challan	System can be integrated with E-challan generating systems with fine generated for each infraction with multiple images clearly showing color of red light signal and violation (i.e. color image of context camera), date, time, vehicle registration number, classification of offence, speed of violating vehicle, notified speed, etc..
	Integration	Integration with RTO database in future should be possible and should also be integrated with the proposed Video Management System.
24	Certifications:	In case of Spot system with RLVD , Systems should be certified as per requirement of Speed Systems (as per Speed systems technical requirement)
25	End-User Certificate	Product should already in use with enforcement authorities and is used for generating fines. End user certificates for proper working shall be submitted.

7.1.3.7 Functional & Technical Requirements of Infrared Illuminators

The infrared illuminators can also be used in conjunction with the Fixed Box cameras specified above to enhance the night vision, in case, MSI wants for his proposed solution.

S.No.	Description	Required Parameters
1	Power	Auto on off, POE+ , AC24V
2	IR Control	Power level, Photocell sensitivity, Timer
3	Type	850 nm semi-covert
4	Distance & Angle of Beam -.	Minimum : 10° x 10°: 120 m (394 ft) or better as may be required for the application
5	Casing	Aluminium and Polycarbonate
6	LED Indicators	Required
7	Environmental Protection	IP66, IK09 Rated
8	Mount Options	Wall, Ceiling, Camera Housing Mount
9	Operating Temperature	0 °C to 55 °C or better
10	Standards/Certification	UL,CE,FCC
11	Approved Makes	Same as Camera OEM

8. Project Governance and Change Management

8.1. Project Management and Governance

8.1.1. 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 BSCL and other officials/representatives by invitation. The operational aspects of the PMO need to be handled by MSI including maintaining weekly statuses, 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:

a) Project Progress
b) Delays, if any – Reasons thereof and ways to make-up lost time
c) Issues and concerns
d) Performance and SLA compliance reports
e) Unresolved and escalated issues
f) Project risks and their proposed mitigation plan
g) Discussion on submitted deliverable
h) Timelines and anticipated delay in deliverable if any
i) 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:

a) Module development status
b) Testing results
c) IT infrastructure procurement and deployment status
d) Status of setting up/procuring of Helpdesk, DC hosting
e) 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.

8.1.2. Helpdesk and Facilities Management Services

a) MSI shall be required to establish the helpdesk and provide facilities management services to support the BSCL and stakeholder department officials in performing their day- to-day functions related to this system.
b) MSI shall setup a central helpdesk dedicated (i.e. on premise) for the Project. 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.
c) 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 MSI is required to maintain for provisioning of the FMS services are described in the Service Level Agreement of this Tender.

d) Helpdesk System should be part of Workflow management system as mentioned section 5.6.2 with facilities like Auto-Routing, Auto-Escalation, User Management, Password Management, In-Built Form Builder & Process Designer etc.

8.1.3. Steering Committee

a) The Steering Committee will consist of senior stakeholders from BSCL, its nominated agencies and MSI. MSI will nominate its Smart City vertical head to be a part of the Project Steering Committee.
b) 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.
c) 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.
d) 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.
e) Other than the planned meetings, in exceptional cases, BSCL may call for a Steering Committee meeting with prior notice to MSI.

8.1.4. Project Monitoring and Reporting

a) MSI shall circulate written progress reports at agreed intervals to BSCL 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.
b) Other than the planned meetings, in exceptional cases, project status meeting may be called with prior notice to the Bidder. BSCL reserves the right to ask the bidder for the project review reports other than the standard weekly review reports.

8.1.5. Risk and Issue management

a) MSI shall develop a Risk Management Plan and shall identify, analyze and evaluate the project risks, and shall develop cost effective strategies and action plans to mitigate those risks.
b) MSI shall carry out a Risk Assessment and document the Risk profile of BSCL based on the risk appetite and shall prepare and share the BSCL Enterprise Risk Register. 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 BSCL.

c) MSI shall monitor, report, and update the project risk profile. The risks should be discussed with BSCL 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.

8.2. Governance procedures

MSI shall document the agreed structures in a procedures manual.

8.2.1. Planning and Scheduling

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. MSI has to get the plan approved from BSCL 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:

a) The project break up into logical phases and sub-phases;
b) Activities making up the sub-phases and phases;
c) Components in each phase with milestones;
d) The milestone dates are decided by BSCL 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.
e) Key milestones and deliverables along with their dates including those related to delivery and installation of hardware and software;
f) Start date and end date for each activity;
g) The dependencies among activities;
h) Resources to be assigned to each activity;
i) Dependency on BSCL

8.2.2. License Metering / Management

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, and DC. This may be carried out through the use of standard license metering tools.

8.3. Manpower Deployment

MSI shall deploy below Manpower during implementation and O&M phases. The deployed resource shall report to BSCL 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 to meet the Go-Live milestone and to meet the defined SLAs in this RFP:

Table 8: Manpower Deployment

Sl. No. #	Type of Resource	Quantity	Minimum Deployment during Implementation phase	Minimum Deployment during Operation and Maintenance phase
1	Project Director	1	At least 25%	Onsite Support to Project team on need basis
2	Project Manager	1	At least 80%	100%
3	Solution Architect	1	At least 80%	Onsite Support to Project team on need basis
4	Intelligent Traffic Management Expert	1	At least 80%	100%
5	Software Application Expert	1	At least 60%	100%
6	Network & Security – Infrastructure Expert	1	At least 60%	100%
7	Database Architect/DBA	1	At least 60%	100%
8	Server and Storage Expert	1	At least 60%	100%
9	GIS Expert	1	At least 80%	100%
10	IBMS & CCC Expert	1	At least 60%	Onsite Support to Project team on need basis
11	Contact Center Manpower for Call Center Operations (30 resources in each shift and total 3 shifts in a day of 8 hours each)	90	Not Applicable	100%
12	Operational Manpower for operationalization for the systems	5	Not Applicable	100%

Apart from the above mentioned manpower, MSI is required to provide suitable manpower to monitor the data feeds at the Integrated Command Control Centre and support BSCL in operationalization of the project. Total minimum number of operators required for the project is 90 in three shifts. BSCL reserves the right to increase or decrease the number of operators. The exact role of these personnel and their responsibilities would be defined and monitored by BSCL and respective departmental personnel.

However, technical engineers need to be deployed by the MSI for 24x7 technical support to network and other infrastructures at field level and at camera end-points on sharing basis in best economical way.

MSI shall be required to provide such manpower meeting following requirements:

a) All such manpower shall be minimum graduates.
b) All such manpower shall be without any criminal background / record.
c) BSCL 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.
d) MSI shall have to replace any person, if not found suitable for the job.
e) All field manpower must have independent two-wheeler for local commuting.
f) All the manpower shall have to undergo training from 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 BSCL officers on right approaches for monitoring the feeds & providing feedback to BSCL, Traffic Police and other associated government agencies.
g) Each person shall have to undergo compulsory 1 day training every month.
h) Operational Manpower shall work in 3 shifts, with no person being made to see the feeds for more than 8 hours at a stretch.

Detail operational guideline document, standard operating procedure, governance and oversight plan shall be prepared by MSI during implementation which shall specify detail responsibilities of these resources and their do's & don'ts.

The supervisors required for operationalization of the project will be provided by BSCL, as per requirements.

8.4. Change Management & Control

8.4.1. Change Orders / Alterations / Variations

a) MSI agrees that the requirements given in the Bidding Documents are minimum requirements and are only indicative. The vendor would need to etch out the details at the time of preparing the design document prior to actual implementation. It shall be the responsibility of 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 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.

d) The Change Order will be initiated only in case (i) the Purchaser directs in writing 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 MSI to incorporate changes or additions to the technical specifications already covered in the Contract.

e) 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.

f) Any change order 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.

g) 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.

h) Within ten (10) working days of receiving the comments from the Purchaser or the drawings, specification, purchase requisitions and other documents submitted by MSI for approval, 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.

8.5. Exit Management

a. This sets out the provisions, which will apply on expiry or termination of the Master Service Level 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.

8.5.1. Cooperation and Provision of Information

During the exit management period:

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

b. Promptly on reasonable request by the BSCL, 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 MSI or sub-contractors appointed by MSI). The BSCL shall be entitled to copy of all such information. Such information shall include details pertaining to the services rendered and other performance data. MSI shall permit the BSCL or its nominated agencies to have reasonable access to its employees and facilities, to understand the methods of delivery of the services employed by MSI and to assist appropriate knowledge transfer.

8.5.2. Confidential Information, Security and Data

a. MSI will promptly on the commencement of the exit management period supply to the BSCL 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 BSCL or its nominated agencies transitioning the services to its Replacement MSI in a readily available format nominated by the BSCL, its nominated agency;
- all other information (including but not limited to documents, records and agreements) relating to the services reasonably necessary to enable BSCL or its nominated agencies, or its Replacement MSI to carry out due diligence in order to transition the provision of the Services to BSCL or its nominated agencies, or its Replacement MSI (as the case may be).

b. Before the expiry of the exit management period, MSI shall deliver to the BSCL 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 MSI shall be permitted to retain one copy of such materials for archival purposes only.

8.5.3. Transfer of Certain Agreements

On request by the BSCL or its nominated agency MSI shall effect such assignments, transfers, licenses and sub-licenses BSCL, 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 BSCL or its nominated agency or its Replacement MSI. SPLA licenses under DR environment will be provided as a service to BSCL.

8.5.4. General Obligations of MSI

a. MSI shall provide all such information as may reasonably be necessary to effect as seamless a handover as practicable in the circumstances to the BSCL or its nominated agency or its Replacement MSI and which 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 MSI.

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

8.5.5. Exit Management Plan

a. MSI shall provide the BSCL 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 MSLA 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 MSI's sub-contractors, staff, suppliers, customers and any related third party as are necessary to avoid any material detrimental impact on the BSCL's operations as a result of undertaking the transfer;
- Proposed arrangements for the segregation of MSI's networks from the networks employed by BSCL and identification of specific security tasks necessary at termination(if applicable);
- Plans for provision of contingent support to BSCL, and Replacement MSI for a reasonable period after transfer.

b. 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 MSI to and approved by the BSCL or its nominated agencies.

d. The terms of payment as stated in the Terms of Payment Schedule include the costs of 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, 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 BSCL or its nominated agencies within 90 days from the Effective Date of this Agreement.

9. Project Implementation Schedule, Deliverables and Payment Terms

Table 9: Implementation Schedule

S.No.	Milestones	Deliverables	Timelines (in months)
1	**Project Implementation Phase**		**T_0 + 15 months = T_F**
1.1	Project Inception Report	Detailed site survey report including infrastructure requirement analysis, hardware deployment plan, recommended action plan to address the gaps, budget estimates for addressing the gaps uncovered during the survey, phase wise location distribution etc. Detailed Project Plan including resource deployment, Communication plan, Risk management plan, Information Security and Business Continuity, Sensitization & Training Plan, Operations management plan etc.	T_0 + 3 month = T_1
1.2	Submission of System Requirement Study(SRS), Functional Requirement Study (FRS) including Solution Architecture, Application Design Documents (HLD & LLD) of the proposed system; Integration report for external applications. Delivery of Hardware/Software of below mentioned projects etc,. (As per RFP – Volume – II – Scope of Works): • OFC laying and Network Backbone • Command & Control Centre • Data Centre and DR Site • CCTV Surveillance • ITMS	As-is Study; Detailed To-Be Design for ICCC, City IT/OFC Network and Data Centre including Data Centre Architecture, Network Architecture, Security Architecture etc; Customization/Changes in overall solution with Gap Analysis (if required); Approach & Plan with Transition Strategy for To-Be; Location list of all field systems including Lat & Long; Requirement of Electrical Power Equipements and Consumption for Temporary	

S.No.	Milestones	Deliverables	Timelines (in months)
	• Variable Message System • Public Address System • Emergency Call Box (ECB) System • Environmental Monitoring System • Smart Parking • Enterprise GIS • Web Portal & Mobile App	Data Centre, Permanent Data Centre and Field Locations;	
1.3	**Phase I: Go-Live** Design, Supply, Installation, Commissioning, Training & Operationalization: • OFC laying and Network Backbone (Guidelines issued by MoUD for cyber security requirement should be adhered to for designing for all proposed edge devices & sensors. Guidelines issued by MoUD for cyber security requirement should be adhered to for designing network for sensor & Wi-Fi traffic etc.) – 60 %. • Command & Control Centre – 60%. • Data Centre and DR Site – 60%. • CCTV Surveillance – 60%. • ITMS – 60% • Public Address System – 60% • Emergency Call Box (ECB) System – 60%. • Environmental Monitoring System –	1. Site Completion/Readiness Report 2. Delivery Acceptance Reports from BSCL/Authorized entity. 3. Installation & Commissioning Reports 4. Software Licenses details requirement	T_1 + 5 months = T_2

S.No.	Milestones	Deliverables	Timelines (in months)
	60% • Smart Parking – 60%. • Enterprise GIS – 60% • Web Portal & Mobile App – 60%.		
1.4	**Phase II: Go-Live** Design, Supply, Installation, Commissioning, Training & Operationalization: • OFC laying and Network Backbone (Guidelines issued by MoUD for cyber security requirement should be adhered to for designing for all proposed edge devices & sensors. Guidelines issued by MoUD for cyber security requirement should be adhered to for designing network for sensor & Wi-Fi traffic etc.) – 80 %. • Command & Control Centre – 80%. • Data Centre and DR Site – 80%. • CCTV Surveillance – 80%. • ITMS – 80% • Public Address System – 80% • Emergency Call Box (ECB) System – 80%. • Environmental Monitoring System – 80% • Smart Parking – 80%. Enterprise GIS – 80% Web Portal & Mobile App – 80%.	1) Site Completion/Readiness Report 2) Delivery Acceptance Reports from BSCL/Authorized entity 3) Installation & Commissioning Reports 4) UAT/FAT and Go Live Certificate from BSCL/Authorized entity 5) Nomenclature and labelling Schema Management and maintenance for various components, ports, electrical interfaces, resources, rooms etc. 6) IP Address Schema and Management	T_2+ 2 Months = T_3

S.No.	Milestones	Deliverables	Timelines (in months)
1.5	**Phase III: Go-Live** Design, Supply, Installation, Commissioning, Training & Operationalization: • OFC laying and Network Backbone (Guidelines issued by MoUD for cyber security requirement should be adhered to for designing for all proposed edge devices & sensors. Guidelines issued by MoUD for cyber security requirement should be adhered to for designing network for sensor & Wi-Fi traffic etc.) – 100 %. • Command & Control Centre – 100%. • Data Centre and DR Site – 100%. • CCTV Surveillance – 100%. • ITMS – 100% • Public Address System – 100% • Emergency Call Box (ECB) System – 100%. • Environmental Monitoring System – 100% • Smart Parking – 100%. • Enterprise GIS – 100% Web Portal & Mobile App – 100%.	1. Site Completion/Readiness Report 2. Delivery Acceptance Reports from BSCL/Authorized entity 3. Installation & Commissioning Reports 4. Software Licenses details 5. UAT/FAT and Go Live Certificate from BSCL/Authorized entity 6. Availability of Mobile App on Play Store & Apple App Store	T_3 + 2 months = T_4
1.6	**Phase IV: CCTV Integration & Project Final Go-Live** Integration with internal and external applications (existing & proposed but not limited to)- ▪ Smart Lighting ▪ Smart Parking	1. UAT/FAT and Go Live Certificate from BSCL/authorized entity 2. Training Content & Completion Certificate 3. Security Audit Certificate from Cert-In/STQC	T_4 + 3 months = T_F

S.No.	Milestones	Deliverables	Timelines (in months)
	▪ ICT Enabled Solid Waste Management ▪ Intelligent Transportation System ▪ E-Challan System ▪ Smart Water Supply System ▪ Smart Education ▪ Smart Health Management System ▪ E-Gov ▪ Etc.	4. Source code of portal, Mobile App & customized applications.	
2	**Project Operation & Maintenance Phase**		**T_F + 60 months**
2.1	Operation & Maintenance	• Monthly & Quarterly SLA Reports • Ad-hoc Reports	T_F + 60 Months

Note1:

1. T_0 = 14 Days from Contract Signing Date
2. $T_1 = T_0 + 3$ month. (i.e. 3 months 14 days)
3. $T_2 = T_1 + 5$ month. (i.e. 8 months 14 days)
4. $T_3 = T_2 + 2$ month. (i.e. 10 months 14 days)
5. $T_4 = T_3 + 2$ month. (i.e. 12 months 14 days)
6. $T_F = T_4 + 3$ month. (i.e. 15 months 14 days)

Note2:

Based on findings of the site survey activity done by MSI, 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. BSCL 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 BSCL.

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 in case BSCL 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 BSCL's decision shall be final and binding. MSI will be eligible for the payment based on the completion of activities and approval of the relevant deliverables.

9.1. Payment Schedule

The total payment shall be paid separately for **CAPEX** and **OPEX**. For payment release purpose, **CAPEX** value will not be considered more than 70% of total bid value at any stage, balance will be considered as **OPEX**. **CAPEX** payment shall be released based on below mentioned milestones.

OPEX payment will be released in twenty (20) equal quarterly instalments spread across 5 years Post Final Go-Live.

Other recurring/non-recurring expenses like for Electricity connections & bills, Diesel for Gen-set, Fees for PUC/ROW/etc. to be paid to Government Departments for Project Execution by Master System Integrator (Selected Bidder).

Table 10: Payment Schedule

Ser. No.	Milestones	Timelines	Payment
CAPEX			
1	Submission of Project Inception Report, System Requirement Study(SRS), Functional Requirement Study (FRS) including Solution Architecture, Application Design Documents (HLD & LLD) of the proposed system; Integration report for external applications. Delivery of Hardware/Software of below mentioned projects etc,. (As per RFP – Volume – II – Scope of Works): • OFC laying and Network Backbone • Command & Control Centre • Data Centre and DR Site • CCTV Surveillance • ITMS • Variable Message System • Public Address System • Emergency Call Box (ECB) System • Environmental Monitoring System • Smart Parking • Enterprise GIS • Web Portal & Mobile App	T_0 + 3 month = T_1	30% of CAPEX value restricted to the value of supplied items.
2	Phase I : Go Live	T_1 + 5 months = T_2	20% of capex value restricted to the value of supplied items
3	Phase II : Go Live	T_2+ 2 Months = T_3	20% of capex value restricted to the value of supplied items

4	Phase III : Go Live	T_3 + 2 months = T_4	15% of capex value restricted to the value of supplied items
5	Phase IV : Integration & Project Final Go-Live	T_4 + 3 months = T_F	15% of capex value plus any balance remaining for the previous phases restricted to complete integration
OPEX			
1	Project Operations & Maintenance phase for a period of 60 months from the date of Final Go Live	T_F + 60 Months	OPEX will be paid in twenty (20) equal quarterly instalments spread across 5 years Post Final Go-Live.

Note 1:

1. T_0 = 14 Days from Contract Signing Date
2. $T_1 = T_0$ + 3 month. (i.e. 3 months 14 days)
3. $T_2 = T_1$ + 5 month. (i.e. 8 months 14 days)
4. $T_3 = T_2$ + 2 month. (i.e. 10 months 14 days)
5. $T_4 = T_3$ + 2 month. (i.e. 12 months 14 days)
6. $T_F = T_4$ + 3 month. (i.e. 15 months 14 days)

Note 2: If successful bidder requests for Mobilization advance, following conditions shall be applicable:

a. Mobilization advance can be maximum of 10% of CAPEX value
b. Mobilization advance shall be interest bearing @ 10 % and released only after receipt of Bank Guarantee of 110% of the requested amount.
c. Mobilization advance shall be adjusted proportionately among all Phases Payment Release.

Note 3:

a. All payments to the Master Systems Integrator shall be made upon submission of invoices along with necessary approval certificates from BSCL.
b. The above payments are subject to meeting of SLA's, failing which the appropriate deductions as mentioned in the Volume III of this RFP would be applicable.

Annexures:

Annexure 1: Bill of Quantity

Mentioned below is the indicative Bill of Material for each proposed project component, however the below quoted quantity are minimum and MSI is required to access the exact requirement, location wise, for all the proposed solution components and shall accordingly size the hardware and software infrastructure requirement to meet the project objectives and SLA. Bidder can increase the line item/quantity, if required. **Proposed quantity should not be less than the Indicative quantity, in any case.**

Bidder has to provide proposed quantity for each line item in Technical Bid and justify as per the solution requirements during the technical bid evaluation. This quantity and the increased line-item (if any) must be reflected in the Price Bid, failing which the bid may be rejected.

Tentative Bill of Materials

SL. NO.	Work Descriptions	Item Descriptions		Unit	Quantity
1	Pancity OFC Network Backbone	Pancity OFC Network Backbone	50 mm HDPE Pipe	Kms	220
2	Pancity OFC Network Backbone	Pancity OFC Network Backbone	Manholes at every 1000m	No.	220
3	Pancity OFC Network Backbone	Pancity OFC Network Backbone	Handholes at every 200m	No.	1100
4	Pancity OFC Network Backbone	Pancity OFC Network Backbone	Backbone Fiber Cable : Loose Tube, Gel-Free Cable 144 F, Single-mode (Armoured)	Kms	10
5	Pancity OFC Network Backbone	Pancity OFC Network Backbone	Backbone Fiber Cable : Loose Tube, Gel-Free Cable 144 F, SM(Redundant) (Armoured)	Kms	10
6	Pancity OFC Network Backbone	Pancity OFC Network Backbone	Distribution Fiber Cable : Loose Tube, Gel-Free Cable 96 F, SMF for Secondary PoPs(Armoured)	Kms	40
7	Pancity OFC Network Backbone	Pancity OFC Network Backbone	Distribution Fiber Cable : Loose Tube, Gel-Free Cable 96 F, SMF	Kms	120

			For Tertiary PoPs(Armoured)		
8	Pancity OFC Network Backbone	Pancity OFC Network Backbone	Access Fiber Cable : Loose Tube, Gel-Free Cable 48F, MMF(Armoured)	Kms	40
9	Pancity OFC Network Backbone	Services	Rate contract Price for providing the OFC Connection in the premises of Government Building as and when required. Connectivity has to be provided on Fibre (upto 100 Mtr) as well as on RJ45 Ethernet.	No.	20
10	ICCC	ICCC-Video Wall	70 inches Panel for DLP based Video wall	No.	20
11	ICCC	ICCC-Video Wall	Video Wall Controller (With Required Adaptors, Converter, 4-port Display Graphic card, 4-channel HD capture card with DVI splitter cables, Cabling & Other Fixtures, etc)	No.	2
12	ICCC	ICCC-Video Wall	Video Wall Management Software	No.	1
13	ICCC	ICCC	IP Phone	No.	40
14	ICCC	ICCC	Keyboard Joystick to control PTZ Cameras	No.	10
15	ICCC	ICCC	HD LED Display (55 inches)	No.	8
16	ICCC	ICCC	Public Address System	Set	15
17	ICCC	ICCC	Audio Mixer and speaker system	Set	15

18	ICCC	ICCC	Workstation Desktop with three LED Monitors	No.	30
19	ICCC	ICCC	FRS- Master Server Database (can store upto 10,00,000 Live Templates)	No.	1
20	ICCC	ICCC	FRS –Stream Processing Servers (Capable of 50 Cameras)	No.	1
21	ICCC	ICCC	FRS –Social media/Offline Database Matching	No.	1
22	ICCC	ICCC	Online UPS (sizing as per proposed solution)	No.	1
23	ICCC	ICCC	Video Conferencing software and solution	Set	1
24	ICCC	ICCC	Network & WiFi enabled A4/A3/Legal Size MFP Colour Laser Printer/Scanner/Copier with ADF (Heavy Duty-50K per month for minimum 50 PPM speed for B/W A4 Prints)	No.	2
25	ICCC	ICCC-Security	Biometric access control system	No.	2
26	ICCC	ICCC-Security	IR IS Recognition Camera	No.	2
27	ICCC	ICCC-Security	IRIS Recognition based Administration Software	No.	2
28	ICCC	ICCC-Security	Dome cameras for internal surveillance	No.	20
29	ICCC	ICCC-BMS	Building Management System (BMS)	No.	1
30	ICCC	ICCC - Non - IT	Addressable Fire Detection and Alarm System	Set	1

31	ICCC	ICCC - Non - IT	Rodent Repellent system	Set	1
32	ICCC	ICCC - Non - IT	Gas Based fire Suppression System	Set	1
33	ICCC	ICCC - Non - IT	Portable Fire Extinguishers(5 Kgs)	No.	20
34	ICCC	ICCC - Non - IT	Site Preparation as per the RFP	Lump sum	1
35	ICCC	ICCC- Furniture	Workstation Furniture and Fixtures for ICCC	No.	10
36	ICCC	ICCC- Furniture	Revolving Chairs for office staff	No.	10
37	ICCC	ICCC- Furniture	Office Desk Furniture and Fixtures	No.	10
38	ICCC	ICCC- Furniture	Ergonomic Chairs for ICCC	No.	30
39	ICCC	ICCC- Furniture	Conference Table (for 10 personnel) & Chairs Set	Set	2
40	ICCC	ICCC Help Desk	Hand Set	No.	10
41	ICCC	ICCC Help Desk	Head Set	No.	10
42	ICCC	ICCC Help Desk	Voice Logger	Set	1
43	ICCC	ICCC Help Desk	Soft telephone	No.	10
44	ICCC	ICCC Help Desk	Desktops PC	No.	20
45	ICCC	ICCC- Furniture	Office Workstation(Furniture including one Revolving Chair and Fixtures per workstation)	Lot	20
46	Data Centre Hardware	DC-Network Items	Core Router	No.	2
47	Data Centre Hardware	DC-Network Items	Core Switch	No.	2
48	Data Centre Hardware	DC-Network Items	Internet Router	No.	2
49	Data Centre Hardware	DC-Network Items	Web Application Firewall (WAF)	No.	2
50	Data Centre Hardware	DC-Network Items	Firewall(NGFW)	No.	2

51	Data Centre Hardware	DC-Network Items	Network Intrusion Prevention System (NIPS)	No.	2
52	Data Centre Hardware	DC-Network Items	Anti-Advance Persistent Threat (APT)	No.	2
53	Data Centre Hardware	DC-Network Items	DC 48 Ports Switch for DMZ	No.	2
54	Data Centre Hardware	DC-Network Items	Managed 24 Port L3 Edge Switches for Management	No.	2
55	Data Centre Hardware	DC-Network Items	24 Port Aggregation Switch	No.	16
56	Data Centre Hardware	DC-Network Items	42U Server Rack with necessary accessories	No.	20
57	Data Centre Hardware	DC-Compute (Server, Storage)	KVM Switch	No.	2
58	Data Centre Hardware	DC-Compute (Server, Storage)	Blade Chassis with Fabric Interconnect Switches	No.	5
59	Data Centre Hardware	DC-Network Items	Integrated DNS, DHCP and IP Address Platform	No.	1
60	Data Centre Hardware	DC-Compute (Server, Storage)	Video Management Server (Blade Server)	No.	4
61	Data Centre Hardware	DC-Compute (Server, Storage)	Video Recording Server (Blade Server)	No.	6
62	Data Centre Hardware	DC-Compute (Server, Storage)	Video Analytics Server (Blade Server)	No.	2
63	Data Centre Hardware	DC-Compute (Server, Storage)	ATCS Server (Blade Server)	No.	2
64	Data Centre Hardware	DC-Compute (Server, Storage)	ANPR Server (Blade Server)	No.	2
65	Data Centre Hardware	DC-Compute (Server, Storage)	RLVD Server (Blade Server)	No.	2
66	Data Centre Hardware	DC-Compute (Server, Storage)	TARS server (Blade Server)	No.	2

67	Data Centre Hardware	DC-Compute (Server, Storage)	Variable Message Signboard server (Blade Server)	No.	2
68	Data Centre Hardware	DC-Compute (Server, Storage)	Smart Parking Information Management Solution Server (Blade Server)	No.	2
69	Data Centre Hardware	DC-Compute (Server, Storage)	Environment Management Server (Blade Server)	No.	2
70	Data Centre Hardware	DC-Compute (Server, Storage)	Intrusion Prevention System (HIPS) (Blade Server)	No.	2
71	Data Centre Hardware	DC-Compute (Server, Storage)	Automatic Call Distributor Server (Blade Server)	No.	2
72	Data Centre Hardware	DC-Compute (Server, Storage)	Digital Voice Logger Server (Blade Server)	No.	2
73	Data Centre Hardware	DC-Compute (Server, Storage)	Continuous Learning Server (Blade Server)	No.	2
74	Data Centre Hardware	DC-Compute (Server, Storage)	GIS server (Blade Server)	No.	2
75	Data Centre Hardware	DC-Compute (Server, Storage)	Database Server (Blade Server)	No.	4
76	Data Centre Hardware	DC-Compute (Server, Storage)	Web Server (Blade Server)	No.	4
77	Data Centre Hardware	DC-Compute (Server, Storage)	Anti-Virus and Anti-Spam Server (Blade Server)	No.	2
78	Data Centre Hardware	DC-Compute (Server, Storage)	Enterprise Mail and Message Server (Blade Server)	No.	1
79	Data Centre Hardware	DC-Compute (Server, Storage)	Domain Controller (DC + ADC) Server (Blade Server)	No.	2
80	Data Centre Hardware	DC-Compute (Server, Storage)	Server Load Balancer	No.	2

81	Data Centre Hardware	DC-Compute (Server, Storage)	SAN Switch	No.	2
82	Data Centre Hardware	DC-Compute (Server, Storage)	Storage (Primary) - 4000 TB	TB	1
83	Data Centre Hardware	DC-Compute (Server, Storage)	DLP	No.	250
84	Data Centre Hardware	DC-Compute (Server, Storage)	Tape Library	No.	1
85	Data Centre Hardware	DC-Compute (Server, Storage)	AAA, Guest, Device Profiling for 25000 Concurrent Sessions	No.	1
86	Data Centre Hardware	DC-Compute (Server, Storage)	IDAM	No.	400
87	Data Centre Hardware	DC-Compute (Server, Storage)	DB Encryption	No.	1
88	Data Centre Hardware	DC-Compute (Server, Storage)	App Security	No.	1
89	Data Centre Hardware	DC-Compute (Server, Storage)	Proxy	No.	250
90	Data Centre Hardware	DC-UPS	300 KVA UPS (sizing as per proposed solution)in N+N redundancy	No.	1
91	Data Centre Hardware	DC-AC	Precision Air Conditioning System for the Server Farm Area	No.	4
92	Data Centre Hardware	DC-AC	Split Air Conditioner 2 Ton (5 star energy efficiency rating) for the Auxiliary Area	No.	4
93	Data Centre Hardware	DC - Non - IT	Site Preparation Cost	Lump Sum	1
94	Data Centre Hardware	DC - Non - IT	Water Leak Detection System	No.	2
95	Data Centre Hardware	DC - Non - IT	Rodent Repellent system	No.	2

96	Data Centre Hardware	DC - Non - IT	Fire Suppression System	No.	2
97	Data Centre Hardware	DC - Non - IT	Fire Alarm System	No.	2
98	Data Centre Hardware	DC-Network Items	Copper Cabling	Mtr	5000
99	Data Centre Hardware	DC-Network Items	Fibre Runner	No.	40
100	Data Centre Hardware	DC-Network Items	Wire basket for Copper	No.	40
101	Software Solutions	DC-Software	Server OS License	No.	1
102	Software Solutions	DC-Security	HIPS for 50 Servers farm	No.	1
103	GIS	Software Solutions	Desktop GIS software (For editing purpose) with four extensions as 3D, Spatial Analysis, Network analysis, Data Interportability	No.	1
104	Software Solutions	DC-Software	Licenses for Facial Recognition (Channels)	No.	25
105	Software Solutions	CCTV - ICCC	Licenses for Video Analytics (Channels for Person Tracking as per clause 38 in VMS)	No.	2500
106	Software Solutions	DC-Software	Virtualization Software License	No.	1
107	Software Solutions	DC-Software	Anti-virus & Anti-Spam Enterprise software for 130 endpoints	No.	1
108	Software Solutions	DC-Software	Any/All Off the Shelf Software License required for complete solution	Lot	1
109	Software Solutions	DC-Software	Enterprise Management System	No.	1
110	Software Solutions	ICCC	ICCC core application(HA)	No.	1

111	Software Solutions	SMS Gateway with annual 200,000 SMSs	SMS Gateway with annual 200,000 SMSs	No.	1
112	Software Solutions	ICCC	Video Management Software	No.	1
113	Software Solutions	ICCC	Video Analytics Software	No.	1
114	Software Solutions	ITMS - ATCS	ITMS - ATCS Software	No.	1
115	Software Solutions	ITMS - ATCS	ITMS - ANPR Software	No.	1
116	Software Solutions	ITMS-RLVD	ITMS - RLVD Software	No.	1
117	Software Solutions	ITMS-Speed Detection	ITMS - SVD software	No.	1
118	Software Solutions	ITMS – TARS	ITMS – TARS	No.	1
119	Software Solutions	ITMS	ITMS - PA Software	No.	1
120	Software Solutions	ITMS	ITMS - ECB management software	No.	1
121	Software Solutions	ITMS	ITMS - Variable Message Software	No.	1
122	Software Solutions	Environment Management System	Environment Management System	No.	1
123	Software Solutions	Smart Parking Management Information System	Smart Parking Management Information System	No.	1
124	Software Solutions	City Portal	City Portal	No.	1
125	Software Solutions	Mobile Application	Mobile Application	No.	1
126	GIS	GIS	Enterprise GIS for Web GIS with Geo Analytics as per Solution	Lump Sum	1
127	Software Solutions	ICCC Help Desk	Automated Call Distribution Software	No.	1
128	Software Solutions	ICCC Help Desk	Computer Telephony Integration Software	No.	1

129	Software Solutions	ICCC Help Desk	IVR Software	No.	1
130	Software Solutions	e-Governance Application software	e-Governance Application software	No.	1
131	Software Solutions	e-challan software	e-challan software	No.	1
132	Software Solutions	ERP solution	ERP solution	No.	1
133	Software Solutions	CCTV	Edge Analytic Devices Type 1 with 2 GPU Cards	No.	10
134	Software Solutions	CCTV	Edge Analytic Devices Type 2 with 4 GPU Cards	No.	10
135	Software Solutions	CCTV - ICCC	VMS Licenses for recording channels with redundancy	No.	2500
136	Data Centre Hardware	Diesel Genset, 650 KVA	Diesel Genset, 650 KVA	No.	2
137	Data Centre Hardware	DC-Network Items	32A IP PDU with Ethernet based Environment Monitoring System with one Temperature Sensor	No.	10
138	Data Centre Hardware	DC-Network Items	16A IP PDU with Ethernet based Environment Monitoring System with one Temperature Sensor	No.	10
139	Data Centre Hardware	DC-Network Items	Blanking Panels	No.	10
140	DR Site	DR Site	Rate Contract for Server Computing with OS, Database, Security Features as per MEITY Guidelines. (4 Core, 32 GB RAM per VM per month)	VM	1
141	DR Site	DR Site	Rate Contract for One-time DR Provisioning & Installation	VM	1

			Charges (Per VM - at the time of new VM addition)		
142	DR Site	DR Site	Rate Contract for Storage for all Critical Applications, Enterprise database, GIS data and flagged video Feed (Not for regular feed) with all security features as per MEITY guidelines.	TB	2000
143	ITMS-ATCS	ITMS - ATCS	ATCS Traffic signal controller	No.	16
144	ITMS-ATCS	ITMS - ATCS	Vehicle Detection Camera	No.	128
145	ITMS-ATCS	ITMS - ATCS	Countdown timer	No.	128
146	ITMS-ATCS	ITMS - ATCS	Supply & Installation of Signal head with 3 signal aspect - Red, Yellow, Green Arrow	No.	128
147	ITMS-ATCS	ITMS - ATCS	Supply & Installation of Signal head with 1 signal aspect - Green Arrow	No.	128
148	ITMS-ATCS	ITMS - ATCS	Supply & Installation of Signal head with 2 signal aspect - Pedestrian Red & Ped Green	No.	128
149	ITMS-ATCS	ITMS - ATCS	Supply & Installation of Galvanised Iron Class B Traffic Signal straight pole of 6 mtr height with all accessories	No.	128
150	ITMS-ATCS	ITMS - ATCS	Supply & Installation of Galvanised Iron	No.	128

			Class B Traffic Signal cantilever pole with all accessories		
151	ITMS-ATCS	ITMS - ATCS	Supply & Installation of Cabinet for UPS, Switches, etc with Mounting Structure, junction boxes, other accessories, etc	Set	256
152	ITMS-ATCS	ITMS - ATCS	8 Port PoE Ruggedized Switch	No.	20
153	ITMS-RLVD	ITMS-RLVD	Red Light Violation Detection (RLVD) Evidence Cameras	No.	128
154	ITMS-RLVD	ITMS-RLVD	RLVD Cameras with ANPR capability	No.	128
155	ITMS-RLVD	ITMS-RLVD	Local processing unit	No.	64
156	ITMS-RLVD	ITMS-RLVD	Mounting structure with junction boxes etc.	Set	128
157	ITMS-RLVD	ITMS-RLVD	8 Port PoE Ruggedized Switch	No.	64
158	ITMS-Speed Detection	ITMS-Speed Detection	Speed Detection System for covering 2 lanes in one direction with complete subcomponents including ANPR camera, sensors, wide angle evidence camera, IR illuminator, non-intrusive speed sensor, with cabling & mounting infrastructure as required	No.	8
159	Public Address Syetem	Public Address Syetem	Public Address System – IP based	No.	10

			PA with speakers, UPS etc.		
160	Public Address Syetem	Public Address Syetem	Mounting structure with all required accessories	No.	10
161	Variable Messaging System	Variable Messaging System	Variable Message Sign Board with all accessories	No.	10
162	Variable Messaging System	Variable Messaging System	Mounting structure with all required accessories	No.	10
163	Emergency Call Box	Emergency Call Box	ECB system with Mounting structure, UPS, pole etc.	No.	10
164	Environmental Sensors	Environmenta l Sensors	All type of Environmental Sensors as per Section 5.15	No.	20
165	ICCC	ICCC	SIEM Solution (Separately for Information & Event Management)	No.	2
166	CCTV-Pan City	CCTV-Pan City	IP Fixed Bullet Cameras	No.	2500
167	CCTV-Pan City	CCTV-Pan City	Outdoor PTZ Cameras- 2MP	No.	300
168	CCTV-Pan City	CCTV-Pan City	8 Port PoE Ruggedized Switch	No.	625
169	CCTV-Pan City	CCTV-Pan City	9U Racks with necessary accessories	No.	40
170	CCTV-Pan City	CCTV-Pan City	Cantilever /Gantry Poles for cameras upgradable to ANPR	Nos	1500
171	CCTV-Pan City	CCTV-Pan City	Junction Boxes (including last mile passive networking, earthing, etc.)	Nos	625
172	CCTV-Pan City	CCTV-Pan City	UPS- (500 VA with 40 Mins battery backup at full load)	Nos	625
173	CCTV-Pan City	CCTV-Pan City	Managed 24 Port L3 Edge Switches	Nos	40

174	CCTV-Pan City	CCTV-Pan City	Online UPS (3 KVA with 2hrs backup)	Nos	40
175	DC-Hardware	DC-Hardware	Supply and Underground laying of Cat 6 /cable in HDPE Pipe including Digging, Piping & Re-filling	Mtr	10000

Annexure 2: Floor Wise Layout for Final Building

This building will be constructed in an approximate time of 6 months. Desired solution is based on this layout only.

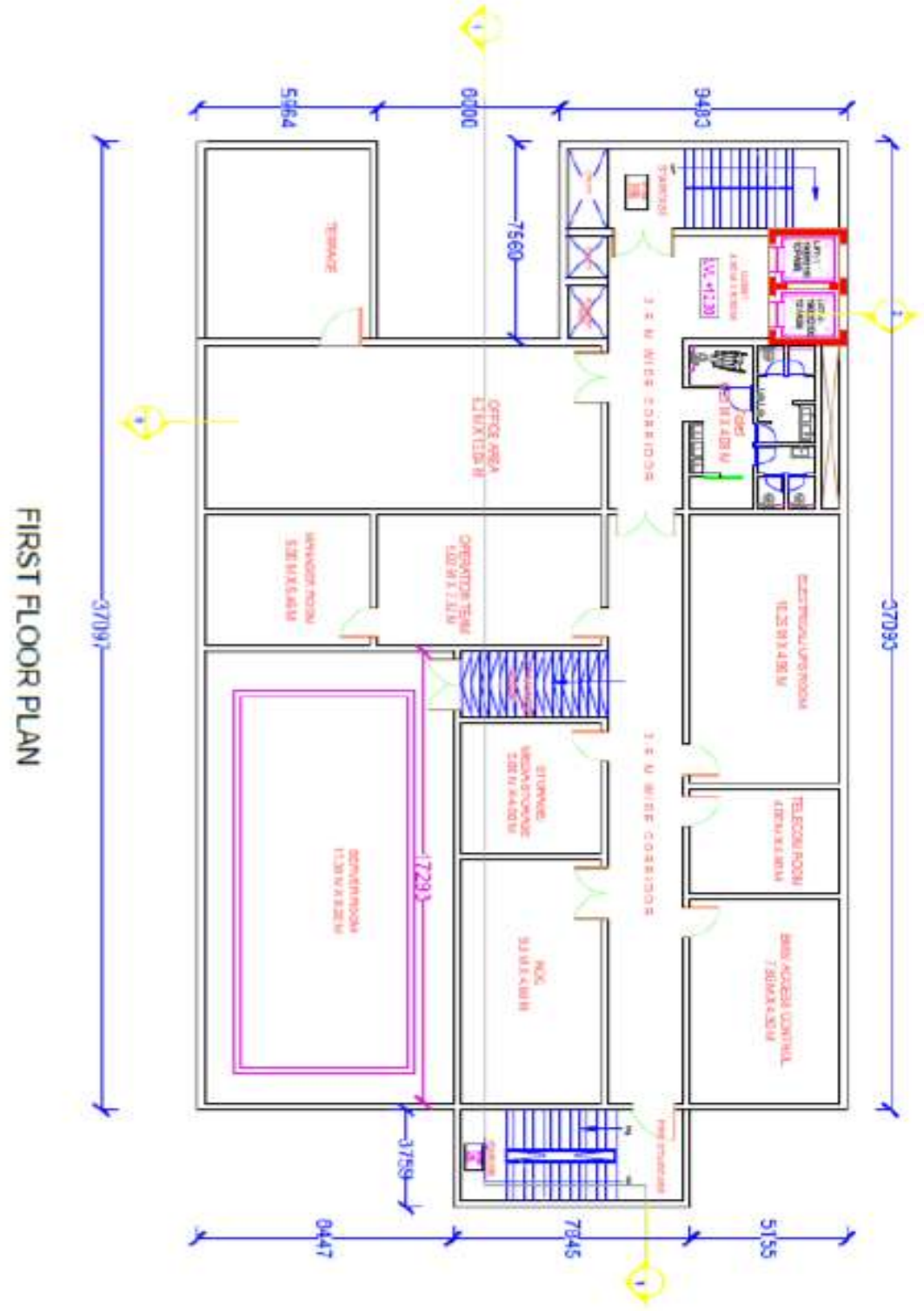


Figure : Layout of First Floor of ICCC Building

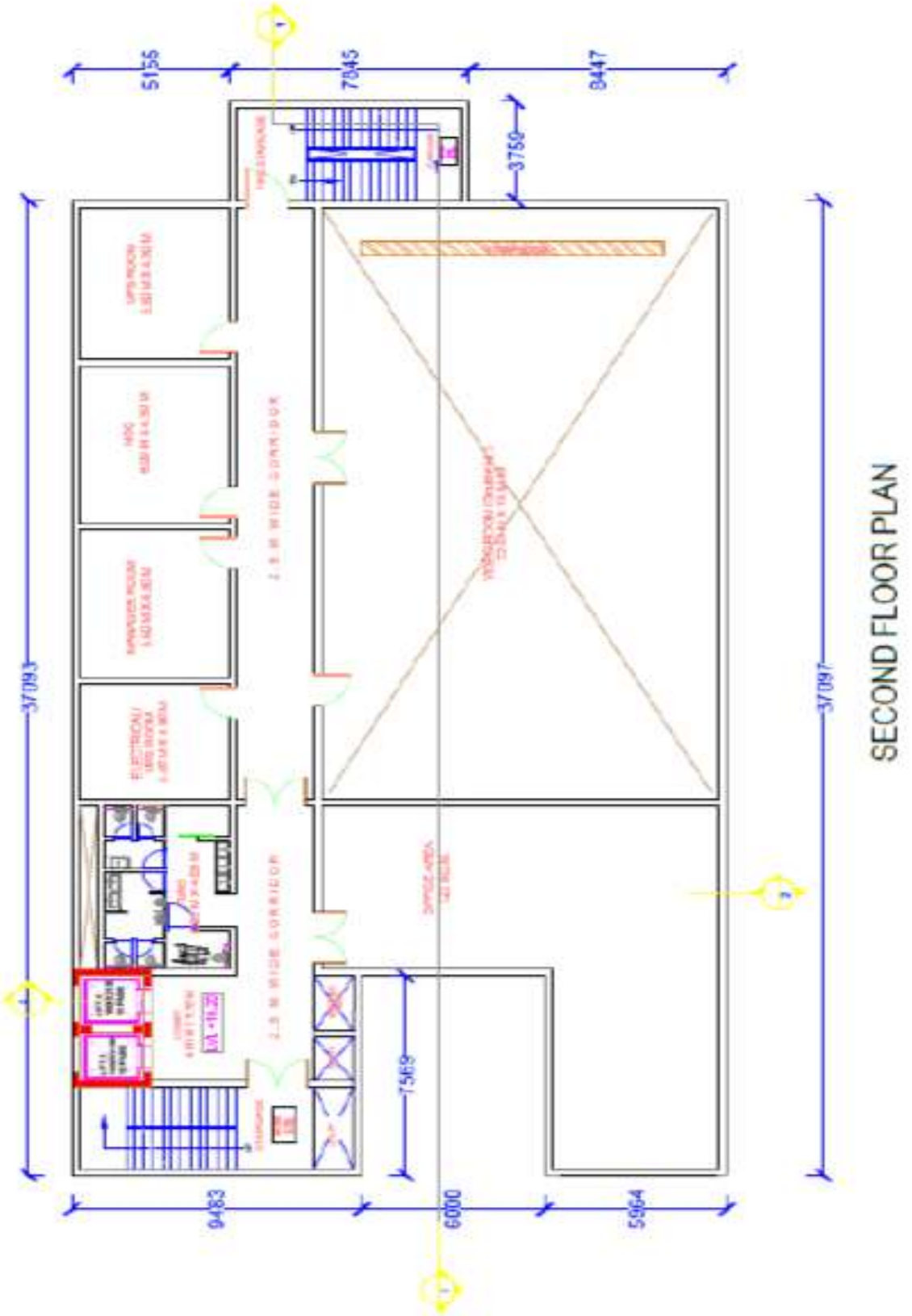


Figure : Layout of Second Floorof ICCC Building

Annexure 3: Indicative list of CCTV Locations

SL NO.	WARD NO	IP Surveillance (Locations)	Camera Type 2 - Fixed HD (Nos)	Camera Type 1 - PTZ HD (Nos)
1	**1**	NARGA CHOWK	2	1
2		MIRGIYACHAK chowk	2	1
3	**2**	VISHARI STHAN CHOWK	2	1
4	**3**	Nathnagarthana chowk	2	
5		Bababambhokar	2	1
6	**4**	Nathnagarthana chowk	2	1
7	**5**	Lalmatiya chowk	2	1
8	**6**	Manaskamna Nath Chowk	2	1
9	**9**	Sahebganj Chowk	2	
10	**10**	Mohan chowk	2	1
11		Harijan Tola chowk	2	1
12	**13**	Ashanandpur Chowk	2	1
13		Parbatti Chowk	2	1
14	**14**	Urdu Bazar chowk	2	1
15	15	Jabbar Chak Chowk	2	
16		Laheri Tola Chowk	2	1
17		Tatarpur chowk	2	1
18	16	Sarai Chowk	2	1
19		Mandroza Chowk	2	1
20		Ramsar Chowk	2	1
21	**18**	Gola Ghat Chowk	2	1
22		Buddhanath Chowk	2	1
23	**19**	Naya Bazar Chowk	2	1
24		Kotwali Chowk	2	1
25	**20**	Dhebar Gate Chowk	2	1
26	**21**	Shankar Talkies Chowk	2	1

27	**22**	ChhotiKhanjarpur Chowk	2	1
28		Manik Sarkar Chowk	2	1
29	**23**	Akashwani Chowk	2	1
30		Kutchari Chowk	2	1
31		GhantaGhar Chowk	2	1
32	**24**	Bari Khanjarpur Chowk	2	1
33		Manali chowk	2	1
34	**25**	ChhotiKhanjarpur Chowk	2	1
35	**28**	Railway Chowk	2	1
36		Sabji Chowk	2	1
37		Madhu Chowk	2	1
38		Housing Board Chowk	2	1
39	30	Tilkamanjhi Chowk	3	1
40	33	Chandni Chowk	2	1
41	34	Hatiya Chowk	2	1
42		Gmti NO. 12 Chowk	2	
43	35	Gumti NO. 1 Chowk	2	
44	36	Koila Depot Chowk	2	1
45		Bhikhanpur Chowk	2	1
46		Mini Market Chowk	2	
47	37	Vaishno Devi Chowk	2	1
48		Trimurti Chowk	2	1
49		Head Post office Chowk	2	1
50		BhikhanpurGumti No. 3	2	
51	38	Saheed Bhagat Singh Chowk	2	1
52		Khalifabag Chowk	2	
53		Veriety Chowk	2	1
54	39	GaniChak Chowk	2	
55	40	Gudhatta Chowk	2	1
56	41	Katghar Chowk	2	
57		Husainabad Chowk	2	1

58		Jagdabe Chowk	2	1
59		Bajrangbali Chowk	2	
60		Balti Karkhana Chowk	2	1
61		Aliganj Chowk	2	
62	42	Bhairavpur Chowk	2	1
63	43	Babargang Chowk	2	
64	45	Sikandarpur Chowk	2	1
65		Kaji Chowk	2	
66	46	ShitlaSthan Chowk	2	
67	48	BausiPul	2	1
68	49	Mirzan Hat Chowk	2	1
Sr. No.	**WARD NO.**	**NAME OF ROAD/ LANE**		
1		MahasaptTaraknath Ghosh Road	2	0
2		Budhiya Kali Sthan Lane	2	0
3		Burning Ghat Road	3	0
4		MahashayDyodhiGhat Road	3	0
5		Laluchak Road	3	0
6		Devi Mandap Lane	3	0
7	**1**	**Somesh Babu Lane**	**2**	**0**
8		**Garju Thakur Lane**	**2**	**0**
9		BenuKanu Lane	2	0
10		Parasnath Temple Lane	3	0
11		BadkiDadi Lane	2	0
12		Narayan Ghos lane	3	0
13		Maqdumshah Dargah Lane	2	0
14		Abir Mishra Lane	3	1
15		Badi Masjid Lane	2	1
16	**2**	ChampaNala Bandh Road	3	
17		Tanti Bazar lane	2	
18		Chamarusah Lane	3	

19	**3**	Dwarka Lal Lane	2	
20		Bhairo Lal lane	3	
21		ChampaNala Road	2	
22		Hakim Sah Lane	3	1
23	4	KauwaKoli Road	2	
24		Kailash Bihari Road	2	1
25		Ghosi Tola Lane	3	
26		Sujapur road	2	
27		Anathalaya Road	3	1
28	5	Goldar Patti Road	2	
29		Jain Mandir Road	4	1
30		NathNagar Bazar Road	2	1
31		Gudari Bazar Lane	3	
32		Lekhraj Lane	2	
33		Lalit Narayan Singh Lane	4	1
34		Ali Bux Lane	2	
35		Bhagat Sah Lane	2	
36		MatrooSah Lane	2	
37	6	VishariSthan Lane	3	
38		Manasakamna Nath lane	2	1
39		T Das lane	3	
40		Garhkutchari Road	2	1
41	7	Hussain Bux Way	2	
42		Chulahi Lane	2	
43		Chamar Tola Lane	2	1
44	8	Fort Road No.1	2	
45		Fort Road No. 2	2	1
46		St. Saviour Church	2	
47		HajariSah Lane	2	
48		Chunni Sah Lane	2	1
49	**9**	Sarover Lane	2	

50		Loknath Ganj Road	2	
51		Neelkanth Road	2	
52		BeliGhat Road	2	1
53		Muslim Tola Lane	2	
54		GwalaToli Lane	2	
55		Nasratkhani Road	2	
56	**10**	Bind Toli Road	2	1
57		Ranglal Sing Road	2	
58		Upper Jamtikri Road	2	
59		Lower Champa Nagar Road	2	1
60		Shaheb Ganj Road	2	
61	**11**	Public Garden Road	2	
62		Mahaveer Path	2	
63		PiparpaatiKalisthan Lane	2	
64	12	Kabirpur Road	2	
65		Upper Cleve Land Road	2	
66		Ashanandpur Road	2	
67	13	Lower Jamtikri Road	2	
68		LabbuPasi Lane	3	
69		Parbatti Lane	2	
70		Urdu Bazar Road	3	
71		Urdu Bazar Lane	2	1
72	**14**	Dr.ameer Hussain Road	2	
73		Irtza Hussain Lane	2	
74		Bibi Mokiman Lane	2	
75		Sarvoday Lane	2	
76		Miajee Tola Lane	2	
77	15	Bijli Chowk Lane	2	
78		M.P. Dwivedi Road	2	
79		Ram Dash Gupta Road	3	
80		Tatarpur Road	2	

81		Sahadat Hussain Lane	2	
82	16	Mandroza Road	2	
83		Soodhi Lane	2	
84		Kallu Sardar Lane	2	
85		Wajid Ali Lane	2	
86		Mahbuj Hussain Lane	2	1
87		Urdu Bazar lane	2	
88	17	Gola Ghat Road	2	
89		Sonversha Lane	2	
90		LalkhaDarga Lane	2	1
91		Kuldeep Narayan Lane	2	
92		Kamruddin Lane	2	
93		GulamRassul Lane	2	
94		Sarai Chhoti Masjid Lane	2	
95		QuilaGhat Road	2	1
96		Sarai KobiBadi Lane	2	
97		BhutNath Road	3	
99	18	Mathura Nath Ghosh Lane	2	1
100		BudhaNath Road	3	
101		Ghosh Lane	2	
102		Raj Gopal Shankar Lane	3	
103		Ghat Road	2	
104		Poddar Toli Lane	3	
105		Swami Vivekanand Path	2	
106		Rai Gopal Sharkar Lane	3	1
107		ShakhichandGhat Road	2	
108		KasbaGolaghat Road	3	
109		Sonversa Lane	2	
110		Lalkhadarga Lane	3	1
111		Gola Ghat Road	2	
112		Aagan Khan Lane	3	

113	19	Rameswar Narayan Aggrawal Road	2	
114		Mandroza Road Aagan Khan Lane	3	
115		R.B.Tarni Prasad Lane	2	
116		Raghunath Sahay Lane	3	1
117		Hakeem Devi Prasad Gupta Path	2	
118		M.P. dwivedi Road	2	
119		Dr. Rajendra Prasad road	3	
120		TikiyaToli Lane	2	1
121		Luft Ali Lane	3	
122		Tatarpur Road	2	
123		Murtja Hussain Lane	3	
124		KajbeliChak Lane	2	
125	20	Upendra Nath Bagchi Road	2	
126		AmulyaCharan Ghosh Road	3	1
127		D.N. Singh Road	2	
128		Chandi Prasad Lane	3	
129		Prakash Panday Lane	3	
130		Bansi Jha Lane	3	1
131	21	Kalika Ram Gola Lane	2	
132		Kali Thakur Lane	3	
133		Chiranjivi Lane	3	
134		Sakur Tola Lane	3	
135		Digambar Sarkar Lane	3	
136		Uma Charan Bose Lane	2	1
137	22	Yateendra Mohan Sarkar Lane	3	
138		Koyla Ghat Road	2	
139		RajaRam Mohan Rai Path	2	1
140		Faris Lane	3	
141		Kali Gati Lane	2	
142		AanandiBabu Lane	2	
143		Kailash Dham Lane	3	

144		Kaligati Lane	2	
145		Raja Shiv Chand Banerjee Lane	3	1
146		B.S.K. Tarafdar Road	2	
147		Ram Ratan Lane	3	
148		ManikSarkarGhat Road	2	
149	22	Rai T.N. Singh Lane	3	
150		Mohim Chandra Lane	2	
151		PyareCharan Sarkar Lane	3	1
152		Ladli Mohan Ghosh Road	2	
153	23	Rai Bahadur Sukhraj road	3	
154		NH80 Police line road	3	
155		Raja Ram Mohan Rai Path	3	1
156		Kutchary Road	3	
157		Red Cross Road	2	
158		T.N.Singh road	3	
159		Satish Sarkar Lane	2	
160		R.R. Sinha Road	3	1
161	24	GopalGanj Lane	2	
162		BhukiSah Lane	3	
163		KanchiSah Lane	2	
164		Sabrati Momin Lane	2	
165		Gurukishan Lane	2	
166		Kochwan Lane	3	
167		R.B.Sahay Road	2	1
168		Lalita Devi Lane	2	
169		ChotiKhanjarpur Lane	3	
170	25	ManthGhat Road	2	
171		ShoratiKabari Lane	2	
172		Mayaganj Road	2	
173		GowalToli Lane	3	
174		Maharaj Ghat Road	2	

175		Khanjarpur Road	2	
176		KhirniGhat Road	2	1
177		Jhauva Kothi Road	3	
178		Surya Prasad Lane	2	
179		ShiVaji Lane	2	1
180		Yateendra Mohan Sarkar Lane	2	
181		NewColony Road	3	
182		BeeroMistri Lane	2	
183	26	Jalim Kori Lane	2	
184		Medical colony Road	3	1
185		Rishala Road	2	
186		Aanandi Lal Lane	2	
187	27	Maharshi Mehi Ashram Road	2	1
188		Panikal Road	2	
189		Sudha Dairy Road	3	
190	28	Feri Road	2	
191		Barari Road	2	
192		BaniyaToli Road	3	1
193		Factory Road	2	
194		Rahmat Hussain Lane	2	
195	**29**	Dyodhi Road	3	
196		Feri Road	2	1
197		Vikramshilasetu Road	2	
198		Housing Board Road	2	
199		Rajendra Nagar Road	3	
200		Janta Flat Road	3	
201		Rai Hari Mohan Road	2	1
202	30	Bhagalpur CentralJail Road	3	
203		Surya Mohan Thakur Path	2	
204		NH80 Subash Chandra Bose Marg	2	
205	31	ShitlaSthan Road	3	1

206		Hanuman Path	2	
207		Ram Krishna Path	2	
208		Jawaripur Road	2	1
209	32	Off Central Jail Road	2	
210		NH 80 Police Line Road	3	1
211		Briyal Ground Road	2	
212		Bhikhanpur Road	3	1
213	33	Abdul Mojib Road	3	
214		Sahmat Hussain Lane	2	1
215		Mir Feku Lane	3	
216		Rmjan Ali Lane	2	
217	34	Aanand Bag Path	3	
218		Bhatha Road	2	
219		Moti Mishra Lane	3	
220	35	ImambaraBhattha Road	2	
221		Gnandra Nat Mukharjee Road	3	
222		Hanuman Mandir Road	2	
223	36	MirjanHaat Road	2	
224		Dickson Road	3	
225		Devi Prasad Lane	3	
226		Radha Devi Lane	3	
227		Nakul Chandra Lane	2	
228		N.C. Chaterjee Road	3	
229		Janki Prasad Lane	3	
230		PatalBabuRoad(NH80)	3	
231	37	R.B.S.S. Colony Road	3	
232		Mahatma Gandhi Road	3	
233		Sundar Lal Lane	3	
234		G.C. Banarjee Road	3	
235		Deena Sah Lane	3	
236		N.C. Chaterjee Road	3	

237	38	Sakhavatahussain lane	3	
238		Meer Dulla Lane	3	
239		Hussain Waks Lane	3	
240		Lane no. 2	4	
241		D.N. Singh Road	4	
242		SaukhiSah Lane	4	
243		R.B. Dhandhaniya Lane	4	
244		Narayan das lane	2	
245		Todarmal Lane	4	
246		Sardari Lal MarketLane	4	
247		Marwari Tola Lane	4	
248		Bhagwan Das Lane	3	
249		Anant Ram Lane	4	
250		Jain Mandir Lane	2	
251		Sujaganj Market Lane	4	
252		Railaxmi path	2	
253		Shah Lane	4	
254		Kunj Lal lane	2	
255	39	AsrafAlam Lane	4	
256		Badru Hussain lane	2	
257		Ashraf alam Lane	4	
258		Maulana chak Lane	4	1
259		ChameliChak Lane	3	
260		Maszid Road	2	
261		GanichakChameli Road	3	1
262		Ganichak Road	2	
263		Jarlahi Road	3	
264		Duid Lane	3	1
265		Bibi Mokiman Lane	2	
266	40	Garibulla Lane	3	
267		SH19 Bausi Road	2	1

268		Hussainpur Road	3	
269		Khairuddin Lane	2	
270	41	Maulana chak Road	2	
271		Balti Karkhana Road	3	
272		Habibpur Road	2	
273		Goura Chowki Road	3	1
274		Gauri Singh Lane	2	
275		Thakur Prasad road	3	
276	42	Gangti Road	2	
277		Bhairopur Road	3	1
278		Mahespur lane	2	
279		Fakruddin Lane	3	
280		Ram Mandal lane	2	1
281		Krishi Bazar Road	3	
282	43	Husainabad Road	3	
283		Panna Mill Road	2	
284		Lalji Ram Lane	2	1
285		Bainding Road	3	
286		Roshan Chak Lane	2	
287		SakrullaChak lane	3	
288		Gulabi Bag Lane	2	1
289		PoshanSah lane	3	
290	44	Hasan Ganj Road	2	
291		Bandhu Modi Lane	2	
292		Domasi Path	2	
293	45	East Gudhatta Road	3	1
294		Panna Mill Road	2	
295		Hafij Lane	3	
296		KajiChak Road	2	
297	46	Masullah Lane	2	1
298	47	LaluChak Main Road	3	

299		Durga Sthan lane	2	
300		NayaChak Road	2	
301	48	Shyamal Das Lane	2	
302		Chatpati Road	2	1
303	49	Warshaliganj Road	2	
304		Ali Ahmad Lane	3	
305	50	Girdhari Lal Lane	2	
306		Qutab Ganj Road	3	
307		Koill Road	2	
308	51	Bagbadi Road	2	
309		Raghunath Mishra Lane	3	1
310		Imambara Lane	2	
SR. NO.	**WARD NO.**	**GHAT NAME**		
1	**1**	Nargaghat	2	
2		MaahashayDyodhighat	3	
3		Umesh das ghat	2	
4		MaqdumshahDargaghat	3	
5		Hari ghat	2	
6		Tola ghat	3	
7	9	MohanpurGhat	2	
8		ShahebganjGhat	2	
9		Burning ghat	3	
10	17	Tilla Kothi Ghat	2	
11		QuilaGhat	2	
12	18	BudhanathGhat	3	
13		Kasba Gola Ghat	2	
14	21	Shankar Talkies Ghat	2	
15	22	Koyla Ghat	2	
16		AadampurZahajGhat	2	
17		Manik Sakar Ghat	3	

18		AadampurGhat	2	
19	25	ManthGhat	2	
20		KhirniGhat	2	
21		SidhiGhat	2	
22	27	KuppaGhat	2	
23		Bharari	2	1
24		BharariSmsanGhat	2	1
24		MayaganjGhat	2	
25		MushahriGhat	2	
26	28	Lunch Ghat	2	
27		HanumanGhat	2	
28	29	Ganga BarariGhat	2	
29		Siri Ghat	2	

Annexure 4: Application Hosted on existing State Data Center

S. No.	Department	Name of Application	URL
1	Directorate of Provident Fund, GoB	eGPF Management system (Intranet	Intranet
2		Application)	
3		eGPF Portal	e-gpf.bihar.gov.in
4		e-Receipt	e-receipt.bihar.gov.in
5	State Welfare Department	BC/EBC Application	http://bcebcwelfare.bihar.gov.in/
6		SC&ST Application	http://mahadalitmission.bihar.gov.in/
7	Department of Industries	Udyog Samwad	http://udyog.bihar.gov.in/
8		Startup Bihar	http://www.startup.bihar.gov.in/
9	State Health Society	ASHA Web Portal	http://192.168.21.125:8081/index.html
10		DHIS-2 Web Portal	http://bihardhis.nhsrc-hmis.org/
11		HR Job Application	http://164.100.130.11:8081/
12		HRIS Web Portal	http://healthhrisbihar.org/
13			
14	Urban Development &	e-Municipality e-Gov Solution	https://nagarseva.bihar.gov.in/

S. No.	Department	Name of Application	URL
15	Housing Department	Urban Development & Housing Department	http://urban.bih.nic.in/
16	DIT	e-Office	https://eoffice.bihar.gov.in/
17		e-Office Demo	https://eofficedemo.bihar.gov.in/
18	Department of Social Welfare	Web Portal	ipmsicds.bihar.gov.in
19	State Election Commission	Website	http://sec.bihar.gov.in
20	Bihar State Films Development & Finance Co. Ltd.	BSFDFC	http://film.bihar.gov.in
21	P&D	Student Credit Card	http://7nishchay-yuvaupmission.bihar.gov.in/
22	Cabinet Secretariat	Loksamvad	http://www.loksamvad.bihar.gov.in
23	BSNL(Inspectorate for Prison & Correctional Services, GoB)	Prison Calling	URL not assigned
24	High Court	Patna High Court	http://patnahighcourt.gov.in/
25	BSEDC	SDC Private Cloud	https://cloud.bihar.gov.in/
26	L&T	Wi-Fi	Campus-Wifi.bihar.gov.in
27	Finance Department	CFMS	e-nidhi.bihar.gov.in

Annexure 5: Application Hosted on existing State Data Center Cloud Platform

S. No.	Department	URL
1	IT Department	dit.bihar.gov.in
2	Food & Consumer Protection Dept	ePDS.bihar.gov.in
3	Home Department	home.bihar.gov.in
4	Bihar State Electronic Development Corporation Ltd.	www.bsedc.bihar.gov.in
5	State Appellate Authority	stateappellateauthority.bihar.gov.in
6	Public Health & Sanitation Mission	nnp.bihar.gov.in
7	Election Department (E.R.M.S., Office of Chief Electoral Officer, Bihar)	ceo.bihar.gov.in
8	Election Department	ele.bihar.gov.in
9	Department of Industries	lokshikayat.bihar.gov.in
10	Finance Department	nbfc.bihar.gov.in
11	Bihar Public Service Commission Department (BPSC)	onlinebpsc.bihar.gov.in

12	CM Secretariat	www.dashboard.bihar.gov.in
13		cm.bihar.gov.in
14		cmsonline.bihar.gov.in
15		cmsmoodle.bihar.gov.in
16	BCECE Board	bceceboard.bihar.gov.in

Annexure 6:Existing e-Governance Services offered by e-Muncipality

S. No.	Services Portfolio
G2C Services (Government to Citizen Services)	
1	ULB Website
2	Citizen Facilitation Center (CFC)
3	Birth and Death Certificates
4	Building Plan Approval
5	Property Tax
6	Trade License
7	Rent, Lease and Sairat
8	Advertisement and Hoardings
9	RTI (General Administration)
G2G services	
1	Personal Management System
2	General Administration (IT Support / Audit / Q&A/Legal/RTI)
3	Workflow and Document Management System

Annexure 7:Analytics Use Cases Required with the Type of Locations

The MSI shall implement all the use cases in such a way that the require video analytics can be deployed on any commercial off the shelf camera/device/computer/server. The AI functionality could be achieved through Camera (and other edge devices) and/or Server systems (VMS, ITMS, third party analytics etc) & ICCC or their combinations in any manner to achive the result.

S. No.	Type of Analytics and Location	Number of Locations	Video Analytics Use case
1	Vehicle Related	150	Vehicle Classification
			No Seat Belt on Four Wheel vehicles
			Driver's Smoking in Four Wheel vehicles while driving
			Use of Mobile phones by Driver while driving
			Wrong side driving detection
			Illegal Parking
			Stopped Vehicle/Accident Detection
			Speed Violation Detection
2	Solid Waste/Garbage Related	100	Litter/Debris and garbage detection
			Attendance of santitation worker by facial recognition
			Sweepping and cleaning of streets/bins
			Tracking of garbage truck movement
3	Surveliance Related at Property of interest (Bus Stop, Important Buidings, Monuments, Parks, Stadium, Tourist Locations, Education Institutes, etc.)	200	Overcrowding Detection/confilcts in crowd
			Abandoned Object Detction
			Vandalism Detection
			Graffiti Detection
			Intrusion Detection
			Person Collapsing
			Loittering
			People Counting
			People Tracking across cameras

Annexure 8:ICCC Design Considerations

Key Design Considerations

- Designed for 24x7 online availability of application.
- Scalable solution on open protocols; no propriety devices/ applications
- API based architecture for Integration with other web applications and Mobile applications. Key guiding principles considered for building the integrated solution are the following:
    - Continuous adoption of rapidly evolving Technology - Technology evolves too fast and Government projects similar to Smart City with its long procurement cycles do not align naturally to adapt to this trend. Also, any changes to existing implementations require contract changesetc. Hence the entire system would be built to be open (standards, open API, plug-n-play capabilities), components coupled loosely to allow changes in sub-system level without affecting other parts, architected to work completely within a heterogeneous compute, storage, and multi-vendor environment.
    - Selection of best solution at best rate as and when required - Large integrated systems of Smart City operations should be designed to get best cost and performance advantages of natural technology curve (constant increase of speed and decrease of cost) and still aligned to open procurement practices of the Government. For this to happen, architecture should be open and vendor neutral, use commodity hardware, and designed for horizontal scale. This allows buying of commodity compute, storage, etc. only when needed at best price.
    - Distributed Access and Multi-channel service delivery -With high penetration of mobile devices and very large percentage of internet usage using mobile devices, it is imperative that the Smart City applications provide multiple channels of service delivery to its stakeholders. An important consideration is that the access devices and their screen capabilities (including browser variations) are numerous and constantly evolve. Hence, it is imperative to design the system such that the ecosystem of Smart City-integrated mobile apps also evolves.
    - Security and privacy of data - Security and privacy of data within the integrated Project will be foundational keeping in view of the sensitivity of data and critical nature of the infrastructure envisioned to be built for Smart City operations. Security and privacy of data should be fundamental in design of the system without sacrificing utility of the system. When creating a system of this scale, it is imperative that handling of the sensitivity and criticality of data are not afterthoughts, but designed into the strategy of the system from day one.
    - Provision of a Sustainable, Scalable Solution - The motive of the technological enhancements to provide a system that would be sustainable for the next few years. The expectation is that the system should sustain at least 5 years from GO-Live. The solution would be done keeping in mind the scalability of the system. The simplified procurement processes and ease of compliance is expected to lead to huge growth in contract's base. Every component of BSCLsystem needs to scale horizontally to very large volume of data.

The Application Software will have the capability to scale up to future requirements given below:

- Managing the entire Property Life Cycle (Data Collaboration between various govt.

departmental systems)

- Maintaining Information on Citizen Life Cycle (Right from Birth to Marriage, Health, Education, Driving License, Interactions with BSCL)
- API Approach- BSCL has decided to adopt Open API as the guiding paradigm to achieve the above goals. Though BSCL system would develop a portal but that would not be the only way for interacting with the BSCL system as the stakeholders via his choice of third party applications, which will provide all user interfaces and convenience via desktop, mobile, other interfaces, will be able to interact with the BSCL system. These applications will connect with the BSCL system via secure BSCL system APIs. This architectural approach has been taken as the UI based integration through a ubiquitous web portal requires manual interaction and does not fit most consumption scenarios. The following benefits are envisaged from API based integration,
  - Consumption across technologies and platforms(mobile, tablets, desktops, etc.) based on the individual requirements
  - Automated upload and download of data
  - Ability to adapt to changing taxation and other business rules and end user usage models
  - Integration with customer software (GIS, Accounting systems).
- Business Rule Driven Approach-All configurations including policy decisions, business parameters, rules, etc. shall be captured in a central place within the system. The system shall provide facility to the decision makers to add new or edit/delete existing policies or make changes with appropriate permission control and audit trace. Managing these in a central repository ensures only once source of truth is used across many application servers and reduces issues of inconsistent application behavior. Decoupling of the business parameters/rules/master data from the rest of the solution architecture and making them configurable allows for a great deal of flexibility.
- Data Distribution Service-As a future roadmap it is envisaged that the functionalities provided by the BSCL Project should be available as services that could be offered to other stakeholders on request. Keeping this in mind the system shall be able to provide data on subscription-publication basis. The organization of the information exchange between modules is fundamental to publish-subscribe (PS) systems. The PS model connects anonymous information producers (publishers) with information consumers (subscribers). The overall distributed application (the PS system) is composed of processes. The goal of the DDS architecture is to facilitate efficient distribution of data in a distributed system. Participant using DDS can ‘read’ or ‘write’ data efficiently and naturally with a typed interface. Underneath, the DDS middleware will distribute the data so that each reading participant can access the ‘most current’ values.

Guiding Architecture Principle

The IT architecture principles defined in this section are the underlying general rules and guidelines that will drive the subsequent development, use and maintenance of architectural standards, frameworks and future state target architecture.

BSCL system will be built on the following core principles:

Platform Approach

It is critical that a platform based approach is taken for any large scale application development, to ensure adequate focus and resources on issues related to scalability, security and data management. Building an application platform with reusable components or frameworks across the application suite provides a mechanism to abstract all necessary common features into a single layer. Hence the ICCC system is envisaged as a system with 100% API driven architecture at the core of it. BSCL portal will be one such application on top of these APIs, rather than being fused into the platform as a monolithic system.

Open APIs designed to be used form the core design mechanism to ensure openness, multi-user ecosystem, specific vendor/system independence, and most importantly providing tax payers and other ecosystem players with choice of using innovative applications on various devices (mobile, tablet, etc.) that are built on top of these APIs.

Openness

Adoption of open API, open standards and wherever prudent open source products are of paramount importance for the system. This will ensure the system to be lightweight, scalable and secure. Openness comes from use of open standards and creating vendor neutral APIs and interfaces for all components. All the APIs will be stateless. Data access must be always through APIs, no application will access data directly from the storage layer or data access layer. For every internal data access also (access between various modules) there will be APIs and no direct access will be there.

Data as an enterprise asset

Information is a high value asset to be leveraged across the organization to improve performance and decision making. Accurate information would ensure effective decision making and improved performance.

Effective and careful data management is of high importance and top priority should be placed on ensuring where data resides, that its accuracy can be relied upon, and it can obtained when and where needed.

Performance

A best of breed solution using the leading technologies of the domain should be proposed in the solution ensuring the highest levels of performance. It will also ensure that the performance of various modules should be independent of each other to enhance the overall performance and also in case of disaster, performance of one module should not impact the performance other modules.

The solution should be designed in a manner that the following can be achieved:

- Modular design to distribute the appropriate system functions on web and app server
- Increase in-memory Operations (use static operations)
- Reduce number of I/O operations and N/w calls using selective caching
- Dedicated schemas for each function making them independent and avoiding delays due to other function accessing the same schema.
- Solution should provide measurable and acceptable performance requirements for users, for different connectivity bandwidths.
- The solution should provide optimal and high performance Portal Solution satisfying response time for slow Internet connections and different browsers.

Scalability

The component in the architecture will be capable of being scaled up to more user requests or handling more no. of input resources in various modules. Even inclusion of additional application functionalities can be catered to by upgrading the software editions with minimal effort.

The design of the system to consider future proofing the systems for volume handling requirements

- The application functions to be divided logically and developed as Modular solution.
- The system should be able to scale horizontally & vertically.
- Data Volume- Ability to support at least 20 % projected volume growth (year on year) in content post system implementation & content migration.
- Functionality – Ability to extend functionality of the solution without significant impact to the existing functional components and infrastructure.
- Loose coupling through layered modular design and messaging - The architecture would promote modular design and layered approach with clear division of responsibility and separation of concerns at the data storage, service and integration layer in order to achieve desired interoperability without any affinity to platforms, programming languages and network technologies. The architecture has to be scalable, maintainable and flexible for modular expansion as more citizen and business services are provided through the Project. Each of the logical layers would be loosely coupled with its adjacent layers
- Data partitioning and parallel processing - Project functionality naturally lends itself for massive parallel and distributed system. For linear scaling, it is essential that entire system is architected to work in parallel within and across machines with appropriate data and system partitioning. Choice of appropriate data sources such as RDBMS, Hadoop, NoSQL data stores, distributed file systems; etc. must be made to ensure there is absolutely no “single point of bottleneck” in the entire system including at the database and system level to scale linearly using commodity hardware.
- Horizontal scale for compute, Network and storage – Project architecture must be such that all components including compute, network and storage must scale horizontally to ensure that additional resources (compute, storage, network etc.) can be added as and when needed to achieve required scale.

No Vendor lock-in and Replace-ability

Specific OEM products may only be used when necessary to achieve scale, performance and reliability. Every such OEM component/service/product/framework/SI pre-existing product or work must be wrapped in a vendor neutral API so that at any time the OEM product can be replaced without affecting rest of the system. In addition, there must be at least 2 independent OEM products available using same standard before it can be used to ensure system is not locked in to single vendor implementation.

Security

The security services will cover the user profile management, authentication and authorization aspects of security control. This service run across all the layers since service components from different layers will interact with the security components. All public

contents should be made available to all users without authentication. The service will authenticate users and allows access to other features of the envisaged application for which the user is entitled to.

The system should be designed to provide the appropriate security levels commensurate with the domain of operation. Also the system will ensure data confidentiality and data integrity.

The application system should have the following

- A secure solution should be provided at the hardware infrastructure level, software level, and access level.
- Authentication, Authorization & Access Control: 3 factors (User ID & Password, Biometric, and Digital Signature) security mechanisms should be implemented to enable secure login and authorized access to portal information and services.
- Encryption Confidentiality of sensitive information and data of users and portal information should be ensured.
- Appropriate mechanisms, protocols, and algorithms necessary to protect sensitive and confirmation data and information both during communication and storage should be implemented.
- Data security policies and standards to be developed and adopted across the Smart City departments and systems
- In order to adequately provide access to secured information, security needs must be identified and developed at the data level. Database design must consider and incorporate data integrity requirements.
- Role based access for all the stake holders envisaged to access and use the system
- Appropriate authentication mechanism adhering to industry good practice of Password Policies etc.
- Ability to adopt other authentication mechanism such as Electronic Signature Certificates
- Authorization validity to be ensured for the users providing the Data to the system. Data should be accepted only from the entity authorized
- Data should be visible only to the authorized entity
- Audit trails and Audit logging mechanism to be built in the system to ensure that user action can be established and can investigated if any can be aided(e.g. Logging of IP Address etc.)
- Data alterations etc. through unauthorized channel should be prevented.
- Industry good practice for coding of application so as to ensure sustenance to the Application Vulnerability Assessment

System must implement various measures to achieve this including mechanisms to ensure security of procurement data, spanning from strong end-to-end encryption of sensitive data, use of strong PKI national standards encryption, use of HSM (Hardware Security Module) appliances, physical security, access control, network security, stringent audit mechanism, 24x7 monitoring, and measures such as data partitioning and data encryption.

Activities such as anti-spoofing (no one should be able to masquerade for inappropriate access), anti-sniffing (no one should be able get data and interpret it), anti-tampering (no

one should be able to put/change data which was not meant to be put/changed) should be taken care for data in transit, as well as data at rest, from internal and external threats.

User Interface

The architecture and application solutions to be designed should promote simplicity and ease of use to the end users while still meeting business requirements. It should provide a simpler and more cost-effective solution. Reduces development time and makes the solution easier to maintain when changes in requirements occur.

This will be accomplished by the implementation of rich User Interfaces along with its integration with the DMS, Relational Data Store, Messaging and other external applications.

- Efficient and layout design are the key considerations that enhance usability which should be factored in while designing the application. Standard and consistent usability criteria must be defined. An intuitive, user friendly, well-articulated navigation method for the applications greatly enhances the usability of the application.
- Effective information dissemination
- Enhanced functionalities including personalized delivery of content, collaboration and enriching GUI features
- The load time for all web page user interfaces must satisfy both the following response time targets on 1 mbps connection:
    - 3 sec for welcome page
    - 5 sec for static pages
    - 10 sec for dynamic pages
- Ability to perform a simple search within 10 seconds on 1 mbps connectivity and a complex search (combining four terms) within 15 seconds regardless of the storage capacity or number of files and records on the system.
- Mobile Application Platform
    - Applications and services including all appropriate channels such as SMS/USSD/IVRS and development of corresponding mobile applications to the applications and services leveraging the Mobile Service Delivery Gateway (MSDG) and Mobile App Store.
    - Application platform should support the following smart phone mobile OS (Android 4.0 and above, iOS 4, 5 and above, Windows Phone OS 8.0 and above, Mobile Web App)
    - Support the target packaging components like (Mobile Website, Hybrid App, Native App, Web App and Application Development, Eclipse tooling platforms)
    - Support the ability to write code once and deploy on multiple mobile operating systems
    - Support integration with native device API
    - Support utilization of all native device features
    - Support development of applications in a common programming language

- Support integration with mobile vendor SDKs for app development and testing
- Support HTML5, CSS3, JS features for smartphone devices
- Support common protocol adapters for connection to back office systems (i.e. HTTP, HTTPS, SOAP, XML for format)
- Support JSON to XML or provide XHTML message transformations
- Support multi-lingual and language internalization
- Support encrypted messaging between server and client components

Reliability

This is a very crucial system and data are of high sensitivity, the data transfer and data management should be reliable to keep the confidence of the stakeholders. The system should have appropriate measures to ensure processing reliability for the data received or accessed through the application.

It may be necessary to mainly ensure the following

- Prevent processing of duplicate incoming files/data
- Unauthorized alteration to the Data uploaded in the BSCL system should be prevented
- Ensure minimum data loss(expected zero data loss)

Manageability

It is essential that the application architecture handles different failures properly; be it a hardware failure, network outage, or software crashes. The system must be resilient to failures and have the ability to restart, and make human intervention minimal.

All layers of the system such as application, infrastructure must be managed through automation and proactive alerting rather than using number of people managing manually.

The entire application must be architected in such a way that every component of the system is monitored in a non-intrusive fashion (without affecting the performance or functionality of that component) and business metrics are published in a near real-time fashion. This allows data centre operators to be alerted proactively in the event of system issues and highlight these issues on a Network Operations Centre (NoC) at a granular level. The solution should be envisaged to utilize various tools and technologies for management and monitoring services. There should be management and monitoring tools to maintain the SLAs.

Availability

The solution design and deployment architecture will ensure that the application can be deployed in a centralized environment offering system High Availability and failover.

The solution should meet the following availability requirements

- Load Balanced across two or more Web Server avoiding single point of failure
- Deployment of multiple application instances should be possible

- Distributed or load balanced implementation of application to ensure that availability of services is not compromised at any failure instance.
- Network, DC, DR should be available 99.741 % of the time.

SLA driven solution

Data from connected smart devices to be readily available (real-time), aggregated, classified and stored, so as not to delay the business processes of monitoring and decision making, and will enable appropriate timely sharing across the Smart City organization.

Readily available and consumed device data will facilitate timely access of analytics reports at every level and department of the Smart City and provide timely analysis of data as well as monitoring of KPIs through SLAs resulting in effective service delivery and improved decision making.

Integration Architecture

This section recommends the proposed integration architecture aligning with the overarching architectural principles.

The following are the integration specifications for the various integration scenarios -

Real-time integration

All the Smart City applications will be deployed in the Data Centre while any external application of the Smart City ecosystem will reside in outside premises.

The need for an OPC Unified Architecture (OPC- UA) is felt that will facilitate BSCL in defining an enterprise integration platform. An OPC platform will help in data exchange across applications in real-time mode (both synchronous and asynchronous), promote loose coupling with ease of maintenance and change, facilitate rapid composition of complex services, achieve scalability through modularity, and improved business visibility.

The OPC UA architecture is a service-oriented architecture (SOA) and is based on different logical levels. It is an architectural style that allows the integration of heterogeneous applications & users into flexible service delivery architecture. Discrete business functions contained in enterprise applications could be organized as layers of interoperable, standards-based shared "services" that can be combined, reused, discovered and leveraged by other applications and processes.

The following are the various integration modes and techniques that could be leveraged:-

- OPC Base Services are abstract method descriptions, which are protocol independent and provide the basis for OPC UA functionality. The transport layer puts these methods into a protocol, which means it serializes/de-serializes the data and transmits it over the network. Two protocols are specified for this purpose. One is a binary TCP protocol, optimized for high performance and the second is Web service-oriented.
- SOAP web service based interfacing technique will be leveraged as the real-time point to point synchronous integration mode with external or third party systems. The following integration points could be considered for SOAP web service based interfacing:-
    - Payment gateway of the authorized banks to enable authorized users make

financial transactions for the Smart City services availed by them. This should support a unified interface to integrate with all Payment Service Providers using web services over secured protocols.

- SMS application, acting as the SMS Gateway, will make use of APIs for SMS communication to GSM network using the GSM modem, which can be both event-driven as well as time- driven. The API will be exposed to initiate the broadcasting or alert notification.
- Social Media Apps and NoSQL data stores to exchange photos, videos and message feeds, based on interactions with Citizens and Business as well as comments/posts to inform stakeholders.
- IVR/Customer Support solution with ERP and Transactional Data Repository to exchange citizen and business demographic, registration and payment data as well as transactional data related to citizen services and municipal operations.

- Message based interfacing technique will be leveraged for real-time asynchronous integration mode. The following integration points could be considered for message based interfacing -
  - Central LDAP with ERP to synchronize member and employee user registration data
  - Payment solution and ERP to exchange payment data for tracking of beneficiary's payment transactions against different services (citizen, workers, transporter, vendor), master data (employee, vendor/supplier, location, facilities, price table)
  - Employee attendance data with ERP (HR Module) to capture data pertaining to employee location and attendance
  - Departmental applications with ERP (Asset Management module) to exchange data for procurement and maintenance of any assets or infrastructure items for each department.
  - Municipal operations application with ERP (Material Management module) to capture materials related transaction and inventory data for public works
  - Other Government Applications with Smart City application to exchange data for Government procurement, public health schemes, welfare schemes, citizen health, etc.
- RESTful API service based interfacing technique will be leveraged for the following integration areas-
  - Access and use of various services provided by the different departments for citizens and business community will be done through a RESTful, stateless API layer.
  - Access and use of various internal functions related to operations and administration of Smart City for departmental and BSCL employees will be done through a RESTful, stateless API layer
- Data integration in batch mode will be through ETL. The following integration points could be considered for ETL based data integration -
  - Initial data migration to cleanse, validate and load the data extracted from source systems into target tables.

- Data load from all the individual transactional systems like ERP, Grievance Redressal to central enterprise data warehouse solution for aggregation, mining, dashboard reporting and analytics.

Process Integration layer of the BSCL solution will automate complex business processes or provide unified access to information that is scattered across many systems. Process Integration will provide a clean separation between the definition of the process in the process model, the execution of the process in the process manager, and the implementation of the individual functions in the applications. This separation will allow the application functions to be reused in many different processes.

An enterprise service bus (ESB) is a software architecture model used for designing and implementing the interaction and communication between mutually interacting software applications in Service Oriented Architecture. As software architecture model for distributed computing it is a variant of the more general client server software architecture model and promotes strictly asynchronous message oriented design for communication and interaction between applications. Its primary use is in Enterprise Application Integration of heterogeneous and complex landscapes. Following are the requirement for an ESB system:

- The solution should support static/deterministic routing, content-based routing, rules-based routing, and policy-based routing, as applicable in various business cases.
- The solution should have capabilities to receive input message in heterogeneous formats from various different systems, interpret those messages, process and transform those messages to generate output and feed them to various different clients as per formats applicable.
    - The solution should have features to communicate across different services, process them and expose as single aggregate service to facilitate business functionality
    - ESB should support SOA standards such as XML, XSLT, BPEL, web services standards and messaging standards.
    - ESB should support all industry standards interfaces for interoperability between different systems

There are four integration gateways envisaged as part of the solution design. The key requirements with respect to each of these are mentioned below:

SMS Gateway: SMS services are envisaged to be made available as part of the solution design. The service provider may integrate the solution with MSDG, and use the services available through it, or deploy its own SMS Gateway services at no extra charge to BSCL, but it is a mandatory requirement that all the SMS based services (alerts and notifications) should be available as part of the solution. Following are some of the key requirements for the SMS services through the solution:

- Should contain required details/information and targeted to the applicant or designated officers of tax departments and other stakeholders and users as per prevailing TRAI norms
- Facilitate access through access codes for different types of services
- Support automated alerts that allows to set up triggers that will automatically send out reminders

- Provide provision for International SMS
- Provide provision to receive messages directly from users
- Provide provision for personalized priority messages
- Resend the SMS in case of failure of the message
- Provide messaging templates

Email Services: Email services are envisaged to be made available as part of the solution design to send alerts/intimations/automated messages to registered email ids, based on preferences set up/opted by individual users. An authenticated SMTP mail service (also known as a SMTP relay or smart host) is envisaged to be integrated with the solution for sending mail from the solution, and delivered to intended inbox. Support anti-spam features.

Payment Gateway: The solution is envisaged to have integration with payment gateways, to enable authorized Users make financial transactions, as per rights and privileges provided to him/her. The service provider is required to make the provisions for integration with such third party gateways and provide payment services, as per requirement of the BSCL. Some of the key features of payment gateway are mentioned below:

- Should support secure integration with Payment Service Providers
- Should support a unified interface to integrate with all Payment Service Providers
- Should support integration with Payment Service Providers using web services and over HTTP/S protocol
- Should manage messages exchange between UI and payment service providers
- Should support beneficiary's payment transactions tracking against various services
- Should support bank accounts reconciliation
- Should provide logs for all transactions performed through the Payment Gateway for future financial dispute resolution that might arise between entities and either beneficiaries or Payment Service Providers
- Should maintain and keep transactions logs for time period required and specified by the financial regulations followed in country
- Should support redundant Payment Discovery
- Should submit Periodic Reconciliation Report to Government entities
- Should support transaction reports to monitor and track payments
- Should support real-time online credit card authorization for merchants
- Should support compliance with emerging trends and multiple payment options such debit card, credit card, cash cards and other payment gateways
- Should provide fraud screening features
- Should support browser based remote administration
- Should support multicurrency processing and settlement directly to merchant account
- Should support processing of one-time or recurring transactions using tokenization
- Should support real time integration with SMS and emails

IVR Services: IVR services are envisaged as part of Call Centre facility, which will be integrated with the solution, to provide information and services to the people who would contact the Call Centre: Some of the key features of the IVR services are mentioned below:

- Should provide multi-lingual content support
- Should facilitate access through access codes for different types of services
- Should support Web Service Integration
- Should support Dual Tone Multi Frequency (DTMF) using telephone touchpad - in-band and out-of-band
- Should support redirection to human assistance, as per defined rules
- Should be able to generate Data Records – (CDRs) and have exporting capabilities to other systems

There are multiple ways of integration of the solution with other systems is envisaged. These may be through Web Services, Message Queuing, File based or API based. The integration and data sharing mechanism may be either in Batch Mode or Need basis (synchronous or asynchronous). Some of the key requirements of the interface/integration are mentioned below:

- Interface Definition
- Interface Owner
- Interface Type
- Interface Format
- Frequency
- Source System
- API/Service/Store Procedure
- Entitlement Service
- Consuming System
- Interface Layout (or) Schema

- Should have provision for exceptional scenarios
- Should have syntax details such as data type, length, mandatory/option, default values, range values etc.
- Error code should be defined for every validation or business rule
- Inputs and outputs should be defined
- Should be backward compatible to earlier datasets
- Data exchange should provide transactional assurance
- Response time and performance characteristics should be defined for data exchange
- The failover scenarios should be identified
- Data exchange should be auditable

Note: Bidder is free to proposed their own design to be meet the scope and SLA

requirement

p) Security

Data exchange should abide by all laws on privacy and data protection Security Architecture. Proposed solution shall adhere to the guidelines & frameworks issued by Bihar Government/GoIfrom time-to-time for security for smart city solutions.

This section recommends the proposed security architecture aligning with the overarching architectural principles. The basic tenets of Smart City security architecture are the design controls that protect confidentiality, integrity and availability of information and services for all the stakeholders.

User Security and Monitoring Authentication & Authorization

A strong authentication mechanism should be considered to protect unauthorized access to the Smart City applications. Consider use of at least two of the following forms of authentication mechanism:

- Something you know, such as a password, PIN etc.
- Something you have, such as a smart card, hardware security token etc.
- Something you are, such as a fingerprint, a retinal scan, or other biometric methods

Levels of Authentication

Based on the security requirements the following levels of authentication should be evaluated.

- For applications handling sensitive data it is recommended that in the least one factor authentication key in the form of a password is essential. Strong password complexity rules should be enforced to ensure confidentiality and integrity of the data
- For applications handling highly sensitive data it is recommended that two factor authentication mechanisms should be considered. The first line of defense is the password conforming to the password complexity rules'. Along with the password next user has to provide a one-time password which varies for each session. One time passwords are valid for each session and it is not vulnerable to dictionary, phishing, interception and lots of other attacks. A counter synchronized One-Time Password (OTP) solution could be used for this purpose.

Authorization

Authorization of system users should be enforced by access controls. It is recommended to develop access control lists. Consider the following approach for developing access control list -

- Establish groups of users based on similar functions and similar access privilege.
- Identify the owner of each group
- Establish the degree of access to be provided to each group

Data Security

BSCL should protect Integrated Project information against unauthorized access, denial of service, and both intentional and accidental modification. Data security, audit controls and integrity must be ensured across the data life cycle management from creation, accessed, viewed, updated and when deleted (or inactivated). This provides a proactive way to build defense against possible security vulnerabilities and threats, allowing errors to be corrected and system misuse to be minimized.

The implications for adhering to an effective data security and integrity guideline related to the Project are the following –

- Data security policies and standards to be developed and adopted across BSCL Smart City applications and stakeholders
- Data security controls to be put in place to restrict access to enterprise data based on roles and access privileges. Data audit logs should be maintained for audit trail purposes. Security controls will be able to be reviewed or audited through some qualitative or quantitative means for traceability and to ensure that risk is being maintained at acceptable levels.
- In order to adequately provide access to secured information, security needs must be identified and developed at the data level, not the application level. Database design must consider and incorporate data integrity requirements.
- Procedures for data sharing need to be established. Data integrity during data synchronization needs to be ensured across the enterprise.
- Audit Capabilities: The system provides for a system-wide audit control mechanism that works in conjunction with the RDBMS.
- Maintaining Date/Time Stamp and User Id: Every transaction, with a date and time and User ID, is captured. The system allows generating various audit reports for verification.
- Access Log: The BSCL Project should have extensive inbuilt security and access control mechanisms. Based on this, the system keeps track of the various functions accessed by any users.

Audit Trail & Audit Log

Audit trails or audit logs should be maintained. Log information is critical in identifying and tracking threats and compromises to the environment.

There are a number of devices and software that should be logged which include hardware & software based firewalls, web servers, authentication servers, central/domain controllers, database servers, mail servers, file servers, routers, DHCP servers etc.

It is essential to decide what activities and events should be logged. The events which ideally should be captured include

- Create, read, update and delete of confidential information;
- User authentication and authorization activities in the system, granting, modification or revoking of user access rights;
- Network or service configuration changes;
- Application process start up, shutdown or restart, abort, failure or abnormal terminations, failure of network services;

- Detection of suspicious activities such as from Intrusion Detection and Prevention system, anti- virus, anti-spyware systems etc.

Application Security

- Project must comply with the Application Security Plan and security guidelines of Government of India as applicable
- Secure coding guidelines should be followed. Secure coding guidelines should include controls against SQL injection, command injection, input validation, cross site scripting, directory traversal, buffer overflows, resource exhaustion attacks etc. OWASP Top 10 standard should be mapped in the secure coding guidelines to cover all major vulnerabilities.
- Validation checks should be incorporated into the application to detect any corruption of information through processing errors or deliberate acts.
- Data output from an application should be validated to ensure that the processing of stored information is correct and appropriate to the circumstances
- Should implement secure error handling practices in the application
- Project should have Role based access, encryption of user credentials. Application level security should be provided through leading practices and standards including the following:
    - Prevent SQL Injection Vulnerabilities for attack on database
    - Prevent XSS Vulnerabilities to extract user name password (Escape All Un-trusted Data in HTML Contexts and Use Positive Input Validation)
    - Secure Authentication and Session Management control functionality shall be provided through a Centralize Authentication and Session Management Controls and Protect Session IDs from XSS
    - Prevent Security Misconfiguration Vulnerabilities (Automated scanners shall be used for detecting missing patches, misconfigurations, use of default accounts, unnecessary services, etc. maintain Audits for updates
    - Prevent Insecure Cryptographic Storage Vulnerabilities (by encrypt off-site backups, ensure proper key storage and management to protect keys and passwords, using a strong algorithm)
    - Prevent Failure to Restrict URL Access Vulnerabilities (By providing authentication and authorization for each sensitive page, use role-based authentication and authorization and make authentication and authorization policies configurable
    - Prevent Insufficient Transport Layer Protection Vulnerabilities (enable SSL for all sensitive pages, set the secure flag on all sensitive cookies and secure backend connections
    - Prevent Id Redirects and Forwards Vulnerabilities
    - For effective prevention of SQL injection vulnerabilities, MSI should have monitoring feature of database activity on the network and should have reporting mechanism to restrict or allow the traffic based on defined policies.

Infrastructure Security

The following focused initiatives to discover and remedy security vulnerabilities of the IT systems of BSCL Smart City should be considered to proactively prevent percolation of any threat vectors -

- Deploy anti-virus software to all workstations and servers to reduce the likelihood of security threats;
- Deploy perimeter security technologies e.g. enterprise firewalls to reduce the likelihood of any security threat;
- Deploy web content filtering solutions to prevent threats from compromised websites to help identify and block potentially risky web pages;
- Install enterprise-level e-mail anti-security software to reduce vulnerability to phishing and other e-mail security spams. This would check both incoming and outgoing messages to ensure that spam messages are not being transmitted if a system becomes compromised.
- Perform periodic scanning of the network to identify system level vulnerabilities
- Establish processes for viewing logs and alerts which are critical to identify and track threats and compromises to the environment. The granularity and level of logging must be configured to meet the security management requirements.
- Deploy technology to actively monitor and manage perimeter and internal information security.
- Deploy network Intrusion Detection System (IDS) on the perimeter and key points of the network and host IDS to critical systems. Establish process to tune, update, and monitor IDS information.
- In case of cloud deployment, cloud services can be disrupted by DDoS attacks or mis-configuration errors which have the potential to cascade across the cloud and disrupt the network, systems and storage hosting the cloud application.
- Deploy security automation techniques like automatic provisioning of firewall policies, privileged accounts, DNS, application identity etc.

Network Security for Smart Devices

The core principles of security for any smart device network rest on the three most important data security concerns of confidentiality, integrity and authentication. Hence the security for smart device networks should primarily focus on the protection of the data itself and network connections between the nodes. From a network perspective, following are to be considered for designing the smart devices network -

- Protection of fair access to communication channels (i.e. media access control)
- Concealing of physical location of the nodes
- Defense against malicious resource consumption, denial of service, node capturing and node injection
- Provision for secure routing to guard the network from the effects of bad nodes
- Protection of the mobile code

Smart devices have a triple role in most networks - data collectors, processors and traffic forwarders for other devices in the network. The typical attacks for which countermeasures are to be defined and implemented are: Radio Jamming, Nodes Reporting Wrong Data,

Data Aggregation Attacks and Battery Attacks.

The following guidelines need to be considered for security enhancement of smart devices and their networks:

- Use of IP-based network for smart devices
- Use of Link Layer Security for password-based access control and encryption
- Protection of smart devices nodes behind a firewall for carrying out SSL-based application data transfer and mechanism to avoid distributed DoS attacks
- Public-key-based authentication of individual devices to the network and provisioning them for secure communications
- Conformance of the security solution to the standards of IETF, IEC and IEEE to ensure maximum security and interoperability, with support for the following commonly used protocols at a minimum - IPSec/IKE, SSH and SSL/TLS

Software Development Lifecycle Continuous Build

The BSCL Project should be highly modular and parallel development should be carried out for faster execution using industry's best Software Development Lifecycle practices. All application modules within the same technology platform should follow a standardized build and deployment process.

A dedicated 'development / customization' environment should be proposed and setup. MSI must provision separate development and testing environment for application development and testing. Any change, modifications in any module must follow industry standard processes like change management, version control and release management in large and complex application development environment.

Application source code could be maintained in source control and could be broken up into a number of projects. Source control projects are created to abstract related set of modules or feature that can be independently included in another application.

It is a mandatory to create, update and maintain all relevant documentation throughout the contract duration. Also it should be ensured that a bug tracking toll is maintained for proper tracking of all bugs fixes as per various tests conducted on the application.

Quality Assurance

A thorough quality check is proposed for the BSCL Project and its modules, as per standard Software Development Life Cycle (SDLC). MSI is expected to lay down a robust Quality Assurance program for testing of the developed application for its functionality, performance and security before putting in production environment. The program must include an overall plan for testing and acceptance of system, in which specific methods and steps should be clearly indicated and approved by BSCL. MSI is required to incorporate all suggestions / feedback provided after the elaborate testing of the system, within a pre-defined, mutually agreed timeline. MSI must undertake the following:

- Outline the methodology that will be used for testing the system.
- Define the various levels or types of testing that will be performed for system.
- Provide necessary checklist/documentation that will be required for testing the system.

- Describe any technique that will be used for testing the system.
- Describe how the testing methodology will conform to the requirements of each of the functionalities and expected outcome.
- Indicate / demonstrate to BSCL that all applications installed in the system have been tested.

Performance and Load Testing

MSI is expected to implement performance and load testing with following features:

- Testing workload profiles and test scenarios based on the various functional requirements should be defined. Application as well as system resource utilization parameters that need to be monitored and captured for each run also needs to be defined.
- Should support application testing and API testing including HTTP(s), web services, mobile applications and different web 2.0 frameworks such as Ajax/Flex/HTML5.
- MSI should perform the load testing of BSCL Project for multiple workload profiles, multiple scenarios, and user loads to handle the envisaged users of the system.
- Different activities before load testing i.e. identification of work load profiles, scenarios, information capturing report formats, creation of testing scripts, infrastructure detailing and workload profile should be prepared before the start of actual load testing exercise.
- Solution parameters needs to be tuned based on the analysis of the load testing reports. The tuning process could be iterative until the issues are closed. Multiple load runs needs to be executed for users to simulate different scenarios, such as peak load (year end, quarter end, etc.), load generation within the LAN, Load generation across WAN or mobile network simulator while introducing configurable latency/jitter/packet loss etc.
- Should eliminate manual data manipulation and enable ease of creating data-driven tests.
- Should provide capability to emulate true concurrent transactions.
- Should identify root cause of performance issues at application or code level. Include code performance analysis to quickly pinpoint component-level bottlenecks: Slowest classes and methods, most frequently called methods, most costly (aggregate time spent for each method), response time variance etc.
- Should allow selection of different network bandwidth such as analog modems, ISDN, DSL, or custom bandwidth.
- Should be able to monitor various system components e.g. Server (OS, Web, Application & Database) Monitoring, Network (between Client & Server) Delay Monitoring, Network Devices (Firewall, Switch & Router) Monitoring during the load test without having to install any data capturing agents on the monitored servers/components
- Should correlate response times and system performance metrics to provide quick insights in to root cause of performance issues.
- Reports on following parameters (but not limited to) such as transaction response time, transaction per second (Passed), user interface rendering time, transaction per second

(Failed), web transaction breakdown graphs, hits per second, throughput, HTTP responses per Second, pages downloaded per second, system infrastructure performance metrics etc.

- Should provide End-to-End system performance analysis based on defined SLAs. Should monitor resource utilization including memory leakage, CPU overload and network overload. Should have the ability to split end-to-end response time for Network & Server(s) and provide drill-down capability to identify and isolate bottlenecks.

Annexure 9: 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. In case of addition/update in number of license for the products, MSI is required to meet of technical specifications contained in the RFP and for the upward revisions and/or additions of licenses is required be made as part of change order and cost would be commensurate to the itemized rate approved at the LOI issuance.
3. Any manufacturer and product name mentioned in the Tender should not be treated as a recommendation of the manufacturer / product.
4. **None of the IT / Non-IT equipment's proposed by MSI should be End of Life product. It is essential that the technical proposal is accompanied by the OEM certificate in the format given in Volume I of this Tender, where-in the OEM will certify that the product is not end of life product & shall support for at least 6 years from the date of Bid Submission.**
5. All IT Components should support IPv4 and IPv6.
6. Technical Bid should be accompanied by OEM's product brochure / datasheet. MSIs should provide complete make, model, part numbers and sub-part numbers for all equipment/software quoted, in the Technical Bid.
7. MSI should ensure that only one make and model is proposed for one component in Technical Bid for example all Field cameras must belong to a single OEM and must be of the same model etc.
8. MSIs should ensure complete warranty and support for all equipment from OEMs. All the back-to-back service agreements should be submitted along with the Technical Bid.
9. **All equipment, parts should be original and new.**
10. The user interface of the system should be a user friendly Graphical User Interface (GUI).
11. Critical core components of the system should not have any requirements to have proprietary platforms and should conform to open standards.
12. 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 empaneled vendors) to ensure that the application is free from any vulnerability; and approved by the BSCL.
13. All the Clients Machines / Servers shall support static assigned IP addresses or shall obtain IP addresses from a DNS/DHCP server.
14. The Successful MSI should also propose the specifications of any additional servers / other hardware, if required for the system.
15. The indicative architecture of the system is given in this volume. The Successful MSI must provide the architecture of the solution it is proposing.

16. 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 Centre equipment are in safe custody and have access from only the authorized personnel and should be in line with the requirements& SLAs defined in the Tender.
17. The Servers provided should meet industry standard performance parameters (such as CPU Utilization of 60 percent or less, disk utilization 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.
18. 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.
19. All the hardware and software supplied should be from the reputed Original Equipment Manufacturers (OEMs). BSCL reserves the right to ask replacement of any hardware / software if it is not from a reputed brand and conforms to all the requirements specified in the tender documents.
20. All servers, active networking components (for edge level switches, please refer below for additional information), security equipment, storage systems and COTS Application.
21. Cameras, Network Video Recorder (NVR) and the Video Management / Video Analytics Software should be ONVIF Core Specification '2.X' or 'S' compliant and provide support for ONVIF profiles such as Streaming, Storage, Recording, Playback, and Access Control.
22. MSI shall place orders on various OEMs directly or through distributor and not through any sub-contractor / partner. All licenses should be in the name of the BSCL.

Annexure 10: Standards for Bio-Metrics

Bio-Metrics Standards

The Indian Government proposes to use biometric data for identification and verification of individuals in e-Governance applications. The biometric data includes fingerprint image, minutiae, face image and iris data.

The Indian e-Governance applications will have both biometric identification and verification phases, to ensure there is no duplication of identity and to verify the identity of a person for access to the services of the application.

1) Face Image Data Standard

Manual Facial recognition is not sufficient currently for de-duplication. Computer based face recognition has reasonable accuracy under controlled conditions only. Hence for de-duplication purposes, other biometrics like finger print/iris image is also recommended.

With the objective of interoperability among various e-Governance applications, the face image data standard for Indian e-Governance Applications will adopt **ISO /IEC 19794-5:2005(E)**. While the ISO standard is broad to cover all possible applications of computer based face recognition and human visual inspection, this standard is more restrictive, as it is limited to human visual inspection.

The ISO standard specifications are tailored to meet specific needs of civilian e-Governance applications by specifying certain prescriptive values and best practices suitable in Indian context.

Standard	Description
ISO /IEC 19794-5:2005(E)	This standard includes capture and storage specifications of face images for human visual inspection and verification of the individuals in Indian E-Governance applications. It specifies a format to store face image data within a biometric data record compliant to the Common Biometric Exchange Formats Framework (CBEFF), given in ISO 19785-1. It also includes best practices recommended for implementation of the specifications in different categories of e-Governance applications. The scope of this standard includes: o Characteristics of Face Image capturing device o Specifications of Digital Face Image & Face Photograph Specifications intended only for human visual inspection and verification o Scene requirements of the face images, keeping in view a future possibility of computer based face recognition o Face Record Format for storing, archiving, and transmitting the information of face image within a CBEFF header data structure for the purpose of interoperability and usage in future for computer based face recognition.

2) Fingerprint Image and Data Standard

Fingerprint is an important and unique biometric characteristic of an individual. There are many vendors selling finger print devices for acquisition of the data in different ways. Also various algorithms are available for fingerprint features extraction and matching.

It is necessary that these vendors follow fingerprint standards and best practices to ensure interoperability of devices and algorithms to avoid vendor lock-in, and also ensure long term storage of data with technology independence.

Usually, the fingerprint image data captured during enrolment is stored / transmitted for 1:1 (verification) and 1: N (identification) in an e-Governance application life cycle.

The matching of the fingerprints is done by extracting the minutiae of fingerprint data already stored in the enrolment stage, with the minutiae of data captured at the time of verification / identification. This process may even require transmission of fingerprint image data / minutiae data among various e-Governance applications by following the best practices.

Standard	Description
ISO/IEC 19794-4:2005(E)	This standard deals with usage of fingerprint image data and minutiae data for identification and verification of an individual. To ensure interoperability among vendors, it is required that these images be stored in a format compliant with the international standard ISO 19794-4, within the overall Common Biometric Exchange Formats Framework (CBEFF) as per ISO 19785-1. The Government of India would adopt ISO/IEC 19794-4:2005(E) as Fingerprint Image standard, and ISO 19794-2:2005(E) as Minutiae data format standard. The current version of Fingerprint image data standard has been tailored from the ISO 19794-4:2005(E) standard to meet specific needs of e-Governance applications in Indian context. It also includes best practices recommended for implementation of the specifications in different categories of e-Governance applications. This standard specifies fingerprint image specifications in different stages like acquisition for enrolment / verification / identification, storage and transmission. It also includes minutiae template specifications and best practices for implementation of the standard specifications in different categories of e-Governance applications based upon the volume of data, and verification/ accuracy requirements. The current version of the standard is applicable to all civilian e-governance applications as the present version does not include specifications for latent fingerprint data required by certain law enforcement applications.

3) Iris Image Data Standard

In the recent years, Iris recognition has emerged as an important and powerful Biometric characteristic. The Indian Government anticipates that, iris biometric would be deployed for identification and verification in e-Governance applications where identity management is a major issue.

In order to capture the Iris image, special devices are available in the market providing different formats for image acquisition and storage. Also many algorithms have been developed by vendors to extract the features of iris images to decide on a match during verification / identification stage. To ensure interoperability among the e-Governance applications requiring iris recognition, it is necessary to standardize iris specifications including the storage and transmission formats.

Thus, to allow the application developer maximum flexibility in usage of algorithms and devices from different vendors and to address interoperability requirements, the iris image must be captured and stored as per standard specifications included in this document.

This Standard would be applicable to all e-Governance applications in India as per the Government's Policy on Open Standards.

There are two types of interchange formats to represent the Iris image data. The first is a rectilinear (rectangular or Cartesian) image storage format that specifies raw, uncompressed or compressed intensity values. The second format is based on polar image specification with specific pre-processing and segmentation steps, producing a compact data structure containing only Iris information.

The Indian e-Governance applications will deal with Iris image data during multiple stages. Some of these stages are given below:

a. Image acquisition, its processing and its storage in the Enrolment stage
b. Image acquisition and storage for off line / on line verification of Iris image data in 1:1 matching stage
c. Image acquisition and storage for the purpose of identification in 1:N matching stage
d. Transmission of Iris image data to other e-Governance applications
e. Extraction of features of Iris images (enrolment or recognition stage), their storage, and matching (Not covered in the present version of the standard).

The interchange format type of the Iris images that is defined in this standard is for rectilinear images only.

If the image is collected by a camera that captures only one eye at a time and is stored using a rectilinear coordinate system no specific pre-processing is required. Cameras that capture images of both eyes simultaneously may use the following processing steps to calculate the rotation angle of the Iris images.

Standard	Description
ISO/IEC 19794-4:2005(E)	The Government of India would broadly adopt ISO 19794-6:2005(E) Iris Image Data Standard, by tailoring the standard specifications to meet specific needs of civilian e-Governance applications in Indian context and as per the GoI Policy on Open Standards. This Standard specifies Iris image data specifications, acquisition, storage and transmission formats. It also includes best practices for implementation of the Standard specifications in different categories of e-Governance applications, based on the volume of data and verification/ accuracy requirements. This version of the Standard does not include features extraction & matching specifications.

Reference Standards:

1. GoI Face Image data standard version 1.0 published in November, 2010
2. GoI Fingerprint Image data Standard version 1.0 published in November, 2010
3. GoI Iris Image Data Standard Version 0.4, document published in March, 2011

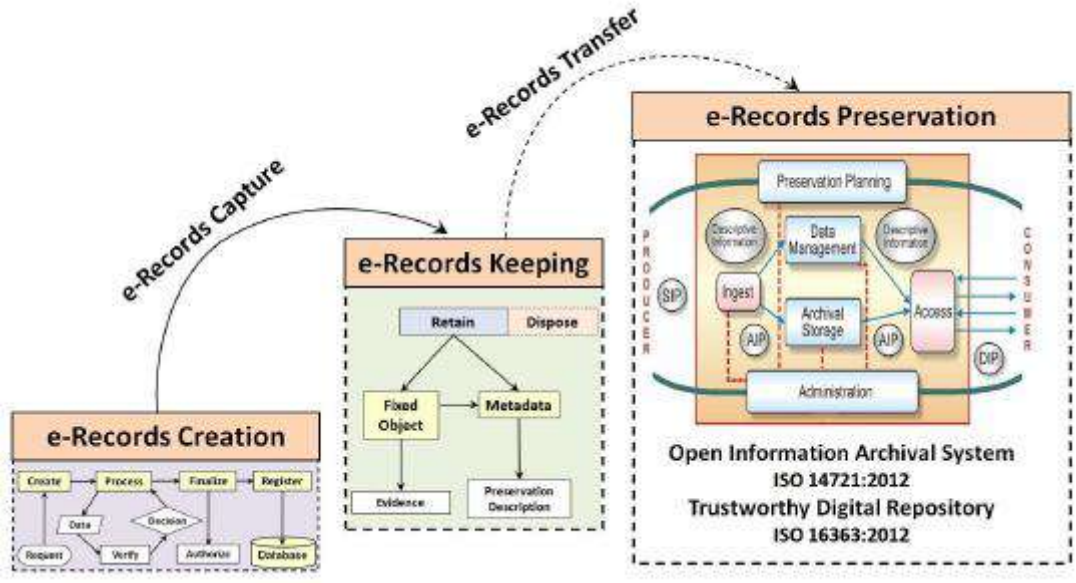
Annexure 11: Standards for Digital Preservation Standards

The **e-Governance Standard for Preservation Information Documentation (eGOV-PID) of Electronic Records (eGOV-PID)** provides a standardized metadata dictionary and schema for describing the "preservation metadata" of an electronic record. This standard proposes to capture most of the preservation information (metadata) automatically after the final e-record is created by the e-Government system. Such preservation information documentation is necessary only for those e-records that need to be retained for long durations (e.g. 10 years, 25 years, 50 years and beyond) and the e-records that need to be preserved permanently.

The implementation of this standard helps in producing the valid input i.e. Submission Information Package (SIP) for archival and preservation purpose as per the requirements specified in the ISO 14721 Open Archival Information Systems (OAIS) Reference Model.

The eGOV-PID allows to capture the preservation metadata in terms of cataloguing information, enclosure information, provenance information, fixity information, representation information, digital signature information and access rights information.

The core concepts of 'preservability' are based on the requirements specified in IT ACT, ISO/TR 15489-1 and 2 Information Documentation - Records Management and ISO 14721 Open Archival Information Systems (OAIS) Reference Model. It introduces 5 distinct steps of e-record management i.e. e-record creation, e-record capturing, e-record keeping, e-record transfer to designated trusted digital repository and e-record preservation which need to be adopted in all e-Governance projects.



Standard	Description
ISO 15836:2009	Information and documentation - The Dublin Core metadata elements
ISO/TR 15489-1 and 2	Information and Documentation - Records Management: 2001
ISO 14721:2012	Open Archival Information Systems (OAIS) Reference Model
ISO/DIS 16363: 2012	Audit & Certification of Trustworthy Digital Repositories
METS, Library of Congress, 2010	Metadata Encoding and Transmission Standard (METS) -
InterPARES 2	International Research on Permanent Authentic Records - A Framework of Principles for the Development of Policies, Strategies and Standards for the Long-term Preservation of Digital Records, 2008
ISO 19005-1:2005 Use of PDF 1.4 (PDF/A-1b) with Level B	Capture of e-records in PDF for Archival (PDFA) format - PDF/A-1a is based on the PDF Reference Version 1.4 from Adobe Systems Inc. (implemented in Adobe Acrobat 5 and latest versions) and is defined by ISO 19005-1:2005. Conformance is recommended for archival of reformatted digital documents due to following reasons: o PDF/A-1b preserves the visual appearance of the document o Digitized documents in image format can be composited as PDF/A-1b **PDF/A for e-governance applications** o Apache FOP 1.1 library can be used in the application logic for dynamically publishing the e-records in PDF/A format. **PDF/A for document creation** o Libre Office 4.0 supports the exporting of a document in PDF/A format. o MS Office 2007 onwards the support for “save as” PDF/A is available. o Adobe Acrobat Professional can be used for converting the PDF documents to PDF/A format.
ISO 19005-2:2011 Use of ISO 32000-1 (PDF/A-2)	Recommended for preservation of documents requiring the advanced features supported in it. PDF/A-2a is based on ISO 32000-1 – PDF 1.7 and is defined by ISO 19005-2:2011. Its features are as under: o Support for JPEG2000 image compression o Support for transparency effects and layers o Embedding of OpenType fonts o Provisions for digital signatures in accordance with the PDF Advanced Electronic Signatures – PAdES standard o Possibility to embed PDF/A files in PDF/A-2 for archiving of sets of documents as individual documents in a single file

	PDF/A-2 does not replace the PDF/A-1 standard but it co-exists alongside with an extended set of features. PDF/A-1a and PDF/A-1b compliance are minimum essential for e-government records as recommended in the IFEG technical standard of DeitY.
JPEG2000 (ISO/IEC 15444-1:2004) and PNG (ISO/IEC 15948:2004)	Image file formats - which support lossless compression are recommended as raster image file formats for e-governance applications as specified in Technical Standards for Interoperability Framework for e-Governance (IFEG) in India, published in 2012 by e-Gov Standards Division, DeitY.
ISO/IEC 27002: 2005	Code of practices for information security management for ensuring the security of the e-records archived on digital storage.

Annexure 12: Standards for Localization and Language Technology

1. Character Encoding Standard for Indian Languages

The lack of availability of information in the locally understandable language is the main reason for the slow progress in the Information and Communication Technology (ICT) sector. In today's age, access to ICT plays a major role in the overall development of a country, it has become a challenge to bridge the digital divide caused by the language barrier.

Standardisation is one of the baselines to be followed in localisation. Standardisation means to follow certain universally accepted standards, so that the developers from any part of the globe could interact through the application. Standardisation becomes applicable in almost everything specific to the language – for instance, a standard glossary of terms for translation, a standard keyboard layout for input system, a standard collation sequence order for sorting, a standard font etc.

Character Encoding standard for all constitutionally recognized Indian Languages should be such that it facilitates global data interchange.

ISCII is the National Standard and Unicode is the global character encoding standard. The average data packet size is less for representation of any Indian languages using ISCII. However, being limited code space, coexistence of multiple languages within the same code page is not possible in ISCII. The migration from ISCII to Unicode has become imperative due to the following reasons:

All major operating systems, browsers, editors, word processors and other applications & tools are supporting Unicode.

- It is possible to use Indian languages and scripts in the Unicode environment, which will resolve the compatibility issue.
- The documents created using Unicode may be searched very easily on the web.
- As Unicode is widely recognized all over the world and also supporting Indian languages, it will ease Localization applications including e-Governance application for all the constitutionally recognized Indian languages.
- Since Indian languages are also used in the other part of the world, it is possible to have Global data exchange.

Unicode shall be the storage-encoding standard for all constitutionally recognised Indian Languages including English and other global languages as follows:

Specification Area	Standard Name	Owner	Nature of the Standard	Nature of Recommend Actions
Character Encoding for Indian Languages	Unicode 5.1.0 and its future up-gradation as reported by Unicode consortium from time to time.	Unicode Consortium, Inc.	Matured	Mandatory

Character: Character is the smallest component of any written language that has semantic value.

ISCII: Indian Script Code for Information Interchange (ISCII - IS 13194:1991) is the character-encoding standard approved by Bureau of Indian Standards (BIS). ISCII is an 8 bit-encoding scheme, catering to 128 code spaces for representation of Indian languages.

Nine Indian scripts are included in ASCII standard to represent 10 Indian languages i.e. Assamese, Bengali, Devnagari, Gujarati, Gurmukhi, Kannada, Malayalam, Oriya, Tamil and Telugu.

Unicode: Unicode is a 16-bit character-encoding standard. All the major written scripts of the world are included in the Unicode Standard. The first version of Unicode was published in year 1991.

Unicode vis-à-vis ISO10646

Unicode is a 16 bit Character Encoding standard. All the major written scripts are included in the Unicode Standard. Indian scripts are also included in the standard. There are 22 constitutionally recognised Indian Languages, written in 12 different scripts. ISO/IEC 10646 is the character-encoding scheme evolved by the International Organisation for Standardisation (ISO) in 1990.

In 1991, the ISO Working Group responsible for ISO/IEC 10646 (JTC 1/SC 2/WG 2) and the Unicode Consortium decided to create universal standard for coding multilingual text. Since then, the ISO 10646 Working Group (SC 2/WG 2) and the Unicode Consortium are working together closely to extend the standard and to keep their respective versions synchronised.

In addition to the code tables as per ISO/IEC 10646, the Unicode Standard also provides an extensive set of character specifications, character data, algorithms and substantial technical material, which is useful for developers and implementers.

2. Font Standard for Indian Languages

A single International Standard to comply with UNICODE data storage. This ensures data portability across various applications and platforms.

True Type Fonts (TTF) was used in various applications earlier by various vendors. TTF had no encoding standard due to which vendors and developers had their own encoding schemes, thereby jeopardizing data portability. ISO/IEC 14496-OFF (Open Font Format) on the other hand is based on a single International Standard and complies with UNICODE for data storage. This ensures data portability across various applications and platforms. Open type font is a smart font which has built- in script composition logic.

Most often it has been observed that the use of proprietary fonts of different standards in Government Offices, which are not compatible with each other, is causing serious problems in information exchange amongst offices. By using Unicode compliant ISO/IEC 14496-OFF (Open Font Format) for font standard, the problem relating to the exchange of documents/files is completely solved.

Open standard under the International Organization for Standardization (ISO) within the MPEG group, which had previously adopted Open Type by reference, now adopted the new standard with appropriate language changes for ISO, and is called the "ISO/IEC 14496-OFF

(Open Font Format)" for which formal approval reached in March 2007 as ISO Standard ISO/IEC 14496-OFF (Open Font Format) and it is a free, publicly available standard.

ISO/IEC 14496-OFF (Open Font Format) for font standard would be the standard for Indian Languages in e-Governance Applications. **ISO/IEC 14496-OFF (Open Font Format) for font standard is mandatory for all 22 constitutionally recognized languages.**

TTF (True Type Font)

A Font Format developed by Apple and licensed to True type, is the native Operating System Font Format for Windows and Mac operating systems.

ISO/IEC 14496-OFF (Open Font Format)

OFF fonts allow the handling of large glyph sets using Unicode encoding. Such encoding allows broad international support for typographic glyph variants.

OFF fonts may contain digital signatures, which enable operating systems and browsing applications to identify the source and integrity of font files, (including the embedded font files obtained in web documents), before using them. Also, font developers can encode embedding restrictions in OFF fonts which cannot be altered in a font signed by the developer.

Annexure 13: Standards for Metadata and Data

Standardization of data elements is the prerequisite for systematic development of e-Governance applications.

Data Standards may be defined as the agreed upon terms for defining and sharing data. Data Standards promote the consistent recording of information and are fundamental to the efficient exchange of information. They provide the rules for structuring information, so that the data entered into a system can be reliably read, sorted, indexed, retrieved, communicated between systems, and shared. They help protect the long-term value of data.

Once the data standards are in place, there is a need to manage data, information, and knowledge. Metadata of standardized data elements can be used for this purpose.

Metadata is structured information that describes, explains, locates or otherwise makes it easier to retrieve, use or manage an information resource. Metadata is often called data about data or information about information. A metadata is a matter of context or perspective -what is metadata to one person or application can be data to another person or application.

In other words, Metadata facilitates the user by providing access to the raw data through which the user can have an understanding of the actual data. Hence, Metadata is an abstraction layer that masks the underlying technologies, making the data access friendlier to the user.

Data and Metadata Standards provide a way for information resources in electronic form to communicate their existence and their nature to other electronic applications (e.g. via HTML or XML) or search tools and to permit exchange of information between applications.

The present document "Data and Metadata Standards- Demographic" focuses on Person Identification and Land Region codifications. It includes the following:

a) **Mechanism for allocation of reference no**. to the identified Generic data elements, and their grouping.

b) **Generic data elements** specifications like:

- Generic data elements, common across all Domain applications
- Generic data elements for Person identification
- Generic data elements for Land Region Codification
- Data elements to describe Address of a Premises, where a Person resides

c) **Specifications of Code Directories like:**

- Ownership with rights to update
- Identification of attributes of the Code directories
- Standardization of values in the Code directories

d) Metadata of Generic Data Elements

- Identification of Metadata Qualifiers
- Metadata of the data elements

e) Illustration of data elements to describe:

- Person identification
- Address of a premises

This Standard would be applicable to all e-Governance applications in India as per the Government's Policy on Open Standards (refer http://egovstandards.gov.in/policy/policy-onopen-

standards-for-e-governance/)

Reference Standards:

4. ISO Standard 1000:1992 for SI Units
5. MNIC Coding for Person Identification
6. ISO 693-3 for International language codes
7. RGI's coding schemes for Languages
8. Top level document provided by Working Group on Metadata and Data Standards
9. EGIF (e- Government Interoperability Framework) Standard of U.K.
10. uidai.gov.in/UID_PDF/Working Papers/A_UID_Numbering_Scheme.pdf
11. http:// www.dolr.nic.in for conversion table of units as used by Department of Land Records
12. GoI Policy on open standards version 1.0 released in November, 2010
13. UID DDSVP Committee report, Version 1.0, Dec 09, 2009
14. ANSI92 Standard

Annexure 14: Standards for Mobile Governance

Framework for Mobile Governance (m-Governance)

Mobile Governance (m-Governance) is a strategy and its implementation to leverage available wireless and new media technology platforms, mobile phone devices and applications for delivery of public information and services to citizens and businesses.

The m-Governance framework of Government of India aims to utilize the massive reach of mobile phones and harness the potential of mobile applications to enable easy and round the-clock access to public services, especially in the rural areas**.** The framework aims to create unique infrastructure as well as application development ecosystem for m-Governance in the country.

In cognizance of the vast **mobile phone subscriber base, peaked to more than 1 billion users in the country**, the Government has decided to also provision for access of public services through mobile devices, thereby establishing mobile Governance (m-Governance) as a compelling new paradigm.

Government of India will progressively adopt and deploy m-Governance in a time-bound manner to ensure inclusive delivery of public services to both the urban and rural populace in the country in accordance with this framework.

The following are the main measures laid down:

i. Web sites of all Government Departments and Agencies shall be made mobile compliant, using the "**One Web"** approach.

ii. **Open standards** shall be adopted for mobile applications for ensuring the interoperability of applications across various operating systems and devices as per the Government Policy on Open Standards for e-Governance.

iii. **Uniform/ single pre-designated numbers** (long and short codes) shall be used for mobile-based services to ensure convenience.

iv. All Government Departments and Agencies shall develop and deploy mobile applications for providing all their public services through mobile devices to extent feasible on the mobile platform. They shall also specify the service levels for such services.

The success of the proposed initiative on m-Governance will greatly depend upon the ability of the Government Departments and Agencies to provide frequently needed public services to the citizens, create infrastructure for anytime anywhere mobile-based services, adopt appropriate open standards, develop suitable technology platforms, make the cost of services affordable, and create awareness, especially for people in underserved areas.

To ensure the adoption and implementation of the framework in a time-bound manner, following actions will be taken:

1. Creation of Mobile Services Delivery Gateway (MSDG)

MSDG is the core infrastructure for enabling the availability of public services through mobile devices. This will be developed and maintained by an appropriate agency within DIT. MSDG is proposed to be used as a shared infrastructure by the Central and State Government Departments and Agencies at nominal costs for delivering public services through mobile devices.

Various channels, such as voice, text (e-mail and SMS), GPRS, USSD, SIM Toolkit (STK), Cell Broadcast (CBC), and multimedia (MMS) will be incorporated to ensure that all users are able to access and use the mobile based services. The various delivery channels are expected to entail innovative ways of providing existing services as well as development of new services.

To ensure successful implementation of the platform with requisite levels of security and redundancy, following actions will be taken:

a) **End User Interface:** End-user devices include landline phones, mobile phones, smart phones, personal digital assistants (PDAs), tablets, and laptops with wireless infrastructure. Mobile applications developed shall take into consideration appropriately the wireless-device interface issues, such as bandwidth limitations, micro-browser and micro-screen restrictions, memory and storage capacities, usability, etc.

b) **Content for Mobile Services:** Due to lower-bandwidth and smaller-screen characteristics of mobile devices, successful development and deployment of m-Governance will require development of separate mobile-ready content. Similarly, to meet the needs of all the potential users, the applications will need to be developed in the relevant local languages for the various channels of delivery. Open standards and open source software, to the extent possible, will be used to ensure interoperability and affordability of the content and applications developed.

c) Mobile Applications (Apps) Store: A mobile applications (m-apps) store will be created to facilitate the process of development and deployment of suitable applications for delivery of public services through mobile devices. The m-apps store shall be integrated with the MSDG and it shall use the MSDG infrastructure for deployment of such applications. It is proposed that the store will be based upon service oriented architecture and cloud based technologies using open standards as far as practicable. The open platform will be developed and deployed in conjunction with the MSDG for making the additional value added services available to the users irrespective of the device or network operator used by them

d) Application Programming Interfaces (APIs) for Value-Added Services (VAS) providers: MSDG shall offer suitable APIs to VAS providers with appropriate terms and conditions to ensure interoperability and compliance with standards for development of applications for delivery of public services.

e) **Mobile-Based Electronic Authentication of Users**: For electronic authentication of users for mobile-based public services, MSDG shall incorporate suitable mechanisms

including Aadhaar-based authentication. This will also help in ensuring appropriate privacy and confidentiality of data and transactions.

f) **Payment Gateway**: MSDG shall also incorporate an integrated mobile payment gateway to enable users to pay for the public services electronically.

g) **Participation of Departments**: The Government Departments and Agencies both at the Central and State levels will be encouraged to offer their mobile-based public services through the MSDG to avoid duplication of infrastructure.

2. Creation of Mobile Governance Innovation Fund

Department of Information Technology (DIT) shall create a Mobile Governance Innovation Fund to support the development of suitable applications by Government Departments and Agencies and also by third-party developers including start-ups. The fund shall be created and managed by DIT for a minimum period of 3 years. The objective of this fund will be to accelerate the development and deployment of the mobile applications across the entire spectrum of public services.

3. Creation of Knowledge Portal and Knowledge Management Framework on Mobile Governance

DIT shall develop and deploy a state-of-the-art knowledge portal and knowledge management framework that acts as a platform for awareness generation and dissemination for various Central Government Ministries and the State Governments. This will enhance the absorptive as well as the service provision capabilities of various stakeholders in m-Governance. Since m-Governance is in its nascent stage both in India and globally, the knowledge portal will act as a reference and guide for Government Departments and Agencies in India.

4. Creation of Facilitating Mechanism

An appropriate facilitating mechanism will be created to ensure compliance with the standards for mobile applications and ensure seamless interoperability of services and implementation of short and long codes for public services across multiple service providers. The proposed mechanism shall be established and managed by the Department of Information Technology, Government of India.

Guidelines for Delivery Channels for Provision of Public Services through Mobile Devices

The Objective is to provide:

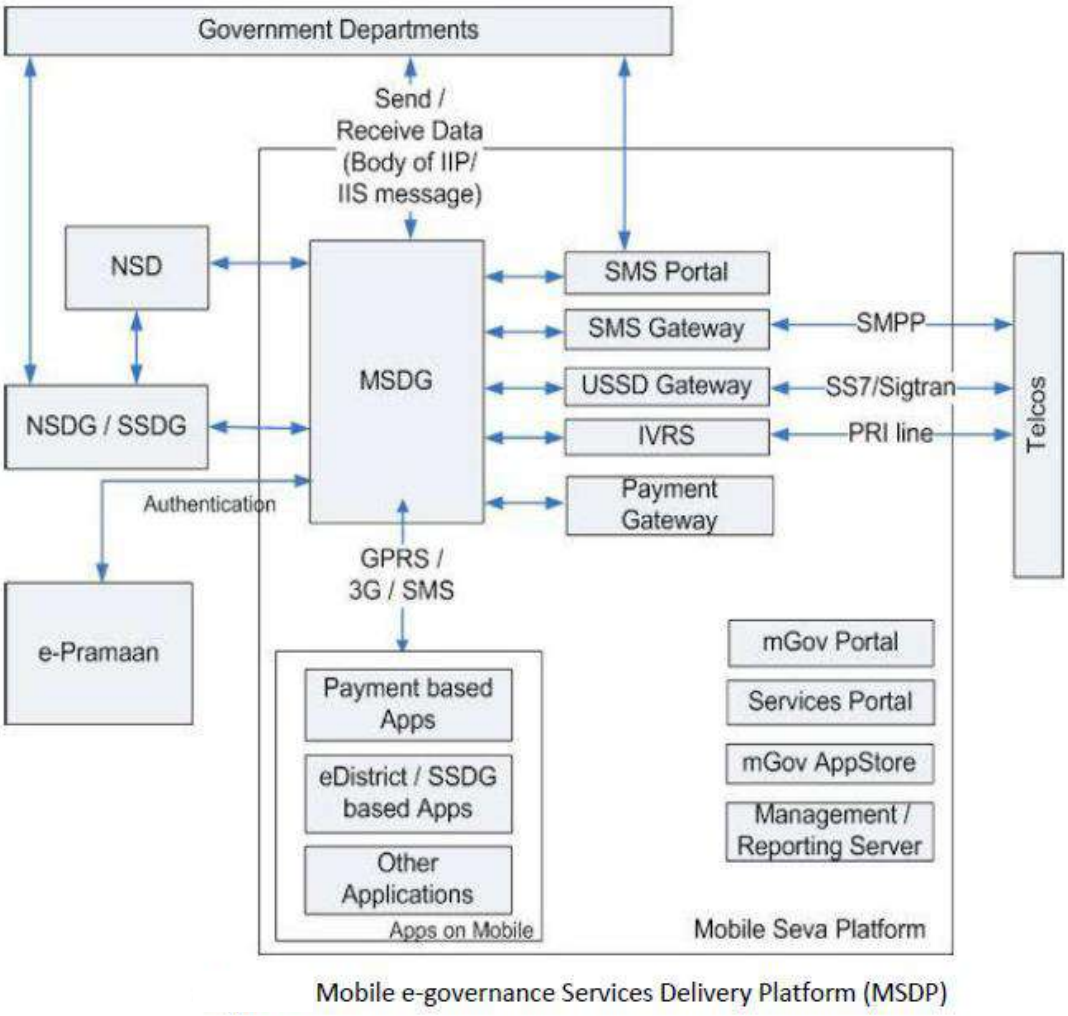
a. Guidelines to deliver public services round-the-clock to the users using m-Governance
b. Guidelines to develop standard based mobile solutions
c. Guidelines to integrate the mobile applications with the common e-Governance infrastructure

As part of the initiative a shared technical infrastructure **Mobile Services Delivery Gateway (MOBILESEVA)** has been created to enable integration of mobile applications with the common e-Governance infrastructure and delivery of public services to the users.

The objective of creating the MOBILE SEVA is to put in place government-wide shared infrastructure and services to enable rapid development, mainstreaming and deployment of m-Governance services. It will enhance interoperability across various public services as well as reduce the total cost of operation of m-Governance services by providing a common pool of resources aggregating the demand for communication and e-Governance services, and act as a platform for various Government Departments and Agencies to test, rapidly deploy, and easily maintain m-Governance services across the country.

MSDP (Mobile e-governance Services Delivery Platform) provides an integrated platform for delivery of government services to citizen over mobile devices using Mobile Service Delivery Gateway (MSDG), SMS Gateway, m-App Store, m-Payment Services, Location Based Services (LBS), Unstructured Supplementary Services Data (USSD), Unstructured Supplementary Service Notify (USSN), Unstructured Supplementary Service Request (USSR), MMS, Cell Broadcasting Service (CBS), SIM Toolkit (STK), IVRS etc.

MSDG is a messaging middleware to facilitate e-Governance services delivery based on e-Governance Standard protocols which are IIP (Interoperability Interface Protocol), IIS (Interoperability Interface Specifications), IGIS (Inter-Gateway Interconnect Specifications) and Gateway Common Services Specifications (GCSS).



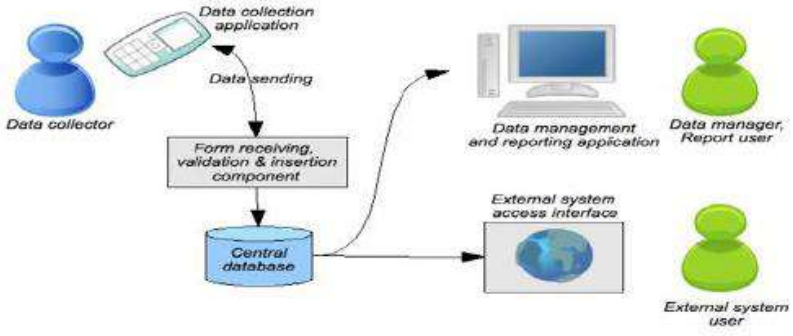
Mobile Application (m-Apps)

Mobile application software is applications software developed for handheld devices, such as mobile

phones, tablets etc. These applications can be pre-installed on phones during manufacture or downloaded by users from various mobile software distribution platforms, or delivered as web applications using server-side or client-side processing (e.g. JavaScript) to provide an application like experience within a Web browser.

1. **Mobile Application Dependency on Handset and O/S**
   Mobile Application software developers also have to consider a lengthy array of screen sizes, hardware specifications and configurations because of intense competition in mobile software and changes within each of the platforms.

2. **Data Collection: m-forms**
   Mobile Application can also make use of the various forms for data collection. Many data collection systems are built from existing commercial or open source components, or even come packaged as an end-to-end solution. The components of data collection relate to each other as shown below:



The data collection may be done by various methods. Following are the most common types of data collection client applications which may be used:

1. **Fixed format SMS based Forms:** The 'client application' in this case is the phone's built-in SMS functionality. The user writes and sends SMS in a predefined format, representing answers to successive questions.

2. **Java Micro Edition Platform (J2ME) Application based Forms:** A J2ME application is written in the Java programming language, and loaded onto the phone over Bluetooth or by downloading the application from the Internet. To use the client application, the data collector navigates through questions in an application on the phone, which collects the answers and submits the completed form to a server.

3. **Mobile Operating System based Forms:** Mobile Operating Systems such as Android, Windows Mobile can also be used for developing native platform-dependent applications which can have various forms for data collection.

4. **Web-based Forms:** The 'client application' for web-based forms is the phone's web browser. The user browses to a website, where the form is published in an optimized format for mobile browsers.

5. **Voice-based based Forms:** The user dials a number and then chooses from options on a menu, useful when there are low levels of literacy among data collectors, or when a system is needed that caters for both landline and mobile phones.

6. **Wireless Internet Gateway (WIG) based Forms:** WIG uses a programming language (Wireless Markup Language, or WML) that is internal to almost all SIM cards. The menu definition is easy to write, but the size limit is 1MB, making it difficult to support long menus or multiple languages.

7. **Unstructured Supplementary Service Data (USSD) based Forms:** This is a real-time question-response service, where the user initiates a session and is then able to interact with

the remote server by selecting numeric menu options. The phone needs to be continuously connected during the session, which needs a good, consistent signal.

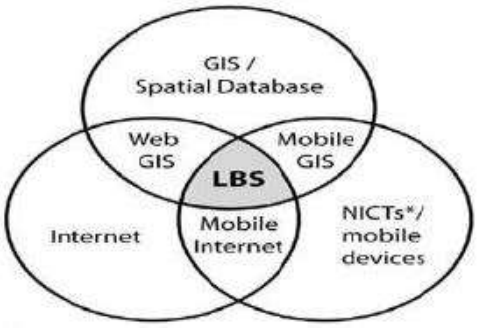
Once data has been captured on the phone, the completed form generally needs to be submitted to a central back-end server.

Other Mobile Technologies

1. Location Based Services (LBS)

Location-based services (LBS) denote services offered to mobile users according to their geographic location. LBS give the possibility of a two way communication and interaction. Therefore the user tells the service provider his actual context like the kind of information he needs, his preferences and his position. This helps the provider of such location services to deliver information tailored to the user needs. LBS enable to retrieve and share information related to their current position. For e.g. Google Latitude.

It works as an intersection of the following features in a system:



***NICT – New Information and Telecommunication technologies**

Geographical Information System (GIS) is a hardware, software and procedures designed to support the capture, management, manipulation, analysis, modelling and display of spatially referenced data for solving complex planning and management problems.

Internet is used to utilize the database dynamically so as to provide the appropriate service.

Mobile Devices as an end- device to execute the service.

2. Cell Broadcast Centre

Cell Broadcast is a mobile technology which allows text messages to be broadcasted to all mobile handsets and similar devices within a designated geographical area.

It is a one-to-many geographically focused service, in contrast to SMS which is a one-to-one or one-to-few service. It is usually used for providing location-based services, especially emergency services, as it utilizes minimum network resources for message broadcast and provides instantaneous delivery to all subscribers in a geographic area.

A Cell Broadcast message is an unconfirmed push service, meaning that the originator of the message does not know who has received the message, allowing for services based on anonymity. Mobile telephone user manuals describe how the user can switch the receiving of Cell Broadcast messages on or off.

Also known as Short message service-Cell Broadcast (SMS-CB), CB messaging is a mobile technology feature defined by the ETSI's GSM committee and is part of the GSM standard. It is also supported by UMTS, as defined by 3GPP.

a) Localization

Given that only a miniscule segment population in India can read and write English, it is important to deploy local/ regional languages to ensure all-round success of m-Governance initiatives. For detailed guidelines please refer to the Mobile Localization Guidelines.

b) Indian Language SMS

Currently, Indian language SMS services are offered by some operators but unlike the English SMS service, the language service is not necessarily interoperable across networks and cannot be availed on all types of handsets. The lack of a standard for Indian SMS comes in the way of providing scalable, interoperable and affordable SMS services in Indian languages.

To realise the goal of interoperable and affordable Indian language SMS, the following are the priority areas:

i. **Text entry standards (i.e. keypad)**
ii. **Encoding standards to support all the major Indian languages**
iii. **Font support standardization for handsets to send and receive Indian language SMS**

i. Text entry methods

The two methods in vogue are:

a. **Mapping the Indian language characters on the handset keypad**
b. **Screen-assisted text inputting mechanisms available from a few OEMs and vendors**

The keypad for the English language has been standardized by ITU. Although efforts on supporting the Indian languages on handheld devices are on, acceptable standards are yet to be evolved. In the absence of any national standards specifying mapping of the Hindi (and other Indian Languages) alphabets to the 12-key mobile devices, the handset vendors

keen on penetrating the large Indian market are using their own mappings (which can differ across vendors).

ii. Encoding standard

The Unicode standard supports the 22 major Indian languages but uses more bandwidth (2 octets for each character) and hence the maximum size of SMS that can be sent using Unicode (70 characters) would be less than half of that of an English language SMS (170 characters).

iii. Font Support

Solutions for aesthetic display of Indian language scripts on small handset screens are being worked out. Similarly, solutions are tried out for handsets already in use so that they can receive and display messages in Indian languages, even if they cannot be used to send such messages.

3. Mobile Payment (M-Payment)

Mobile payment is an alternative payment method. Instead of paying with cash, check, or credit cards, a consumer can use a mobile phone to pay for a wide range of services; after having authenticated the user using AADHAR or any other means. The basic aim of mobile payments is to enable micropayments on low-end mobile devices which support only voice and text, in addition to higher end phones which could support web-browsing or Java application capabilities. The envisaged mobile applications will get integrated with various interoperable payment platforms including UPI, BBPS etc.

a. Mobile banking (M-Banking or mBanking)

M-Banking is a term used for performing balance checks, account transactions, payments, credit applications and other banking transactions through a mobile device. The earlier mobile banking services were offered over SMS, a service known as SMS banking. With the introduction of smart phones with WAP support the mobile web is also being used for M-Banking. Latter with the advancements of web technologies such as HTML5, CSS3 and JavaScript it became feasible to launch mobile web based services to compliment native and hybrid applications.

b. Immediate Mobile Payment Services (IMPS)

The Immediate Mobile Payment System (IMPS) has been developed by the National Payments Corporation of India (NPCI) to expand the scope of mobile payments to all sectors of the population. IMPS offer an instant, 24X7, interbank electronic fund transfer service through mobile phones.

An IMP provides an inter-operable infrastructure to the banks for enabling interbank real time funds transfer transactions. IMPS rides on the existing NFS Interbank ATM transaction switch infrastructure and message format making it easy for banks to adopt.

To enable the transfer of money, both the sender and the receiver of payment have to link their bank accounts with their phone numbers through their respective banks. The sender has to register for mobile banking service with her/his bank. Upon registration, the bank will provide a link to the Mobile banking software which needs to be installed in the mobile phone to enable payments.

Both the sender and the receiver will receive a Mobile Money Identifier (MMID) while the sender will also receive a Mobile PIN (MPIN) for authentication of transactions. While transacting, the sender has to input the MPIN, receiver's mobile number and MMID, and the amount of funds to transfer.

IMPS will authenticate the sender, check the receiver's mobile number and MMID, and transfer the funds to the receiver's account in real-time. Both the sender and the receiver receive messages notifying them about the success or failure of the transaction.

c. Contactless cards and Mobile Phones

These cards are based upon a technology known as NFC (Near Field Communication) that allows NFC enabled cards to be ready by taping them on or by passing them by, a card reader than swiping them through or inserting into, the POS terminal. They are now being integrated into mobile phone handset for m-Payments.

NFC enabled phones are expected to become more widely available. The NFC chip inside the phone will be connected to the secure element within the SIM card, allowing information stored in an m-wallet to be accessed by the NFC card reader. Authorization for payments involves entering a PIN.

The contactless smart cards will be open loop EMV cards as per NCMC specification, envisaged by MoUD. The POS devices should also be EMV compliant and as per NCMC specification.

d. Airtime balance for payment

Airtime as balance for payment was realized because of the need for the unbanked majority to easily and cheaply transfer funds around the country. The facility required is the most basic of mobile phones, an account, which can be opened at any one of vendors to start transferring and receiving money.

Since the system uses either SIM toolkit or USSD technology depending on the country, the network charges are minimal to non-existent. It has lowest entry barriers, since it works on more than 95 percent of handsets and has low transaction costs and no bank account or credit card required.

e. Mobile Wallet

A Mobile Wallet is functionality on a mobile device that can securely interact with digitized valuables thereby making payments using the mobile phone. Mobile wallet may reside on a phone or on a remote network / secure servers. It is controlled by the user of the wallet.

Using a mobile wallet to make a payment is incredibly simple. When it is time to pay, the user turns on his or her phone's screen (if the screen is off, when the phone is dormant for instance, the NFC chip will not work), opens the wallet application, enters their pin number, and passes the phone within a few inches of the contactless payment symbol. The payment transaction is then processed just like a conventional card transaction. In addition, relevant offers, discounts, and coupons can be passed from the wallet along with the payment in that same tap of the phone.

4. SIM Application Toolkit

The SIM Application Toolkit is a standard set of commands, under GSM, which defines how the card should interact with the outside world and extends the communication protocol between the card and the handset. It is designed as a client server application.

With SIM Application Toolkit, the card has a proactive role in the handset, i.e., the SIM initiates commands independently of the handset and the network. This enables the SIM to build up an interactive exchange between a network application and the end user and access, or control access to, the network. The SIM also gives commands to the handset such as displaying menus and/or asking for user input.

Annexure 15: Standards for GIGW

Guidelines for Indian Government Websites

India, the largest democracy in the world, is set to emerge as an ICT Superpower in this millennium. Realising the recognition of 'electronic governance' as an important goal by Governments world over, Indian Government has also laid a lot of emphasis on anytime, anywhere delivery of Government services. As of today, there are over five thousand Government websites in India.

Awareness about the fast changing ICT world and keenness to keep pace with the latest has ensured that almost all the State Governments in India already have their websites up and running. In fact each state has multiple websites belonging to different Departments.

However, these websites follow different Technology Standards, Design Layouts, Navigation Architecture, or, in simple terms, different look and feel as well as functionality.

The need for standardisation and uniformity in websites belonging to the Government cannot be stressed enough, in today's scenario.

As a first step, it is suggested that the Indian Government websites adhere to certain common minimum standards which have been derived, in the form of guidelines discussed in this document, as prerequisites for a Government website to fulfil its primary objective of being a citizen centric source of information & service delivery. These guidelines could eventually form the basis for establishment of the desired standards.

Compliance to these guidelines will ensure a high degree of consistency and uniformity in the content coverage and presentation and further promote excellence in Indian Government Web space.

These Guidelines have been framed with an objective to make the Indian Government Websites conform to the essential pre-requisites of UUU trilogy i.e. Usable, User-Centric and Universally Accessible. They also form the basis for obtaining Website Quality Certification from STQC (Standardisation Testing Quality Certification) an organisation of Department of Information Technology, Government of India.

These Guidelines are based on International Standards including ISO 23026, W3C's Web Content Accessibility Guidelines, Disability Act of India as well as Information Technology Act of India.

A. Indian Government Entity

All websites and Portals belonging to the Indian Government Domain at any hierarchical level (Apex Offices, Constitutional Bodies, Ministries, Departments, Organisations, States/UTs, District Administrations, and Village Panchayats et al) must prominently display a strong Indian Identity and ownership of Indian Government.

The above objective can be achieved through the following:

1. The National Emblem of India MUST be displayed on the Homepage of the websites of Central Government Ministries/Departments. The usage of National Emblem on an Indian

Government website must comply with the directives as per the 'State Emblem of India (Prohibition of improper use) Act, 2005'.

Further, the State Governments should also display the State Emblem (or the National Emblem in case the State has adopted the National Emblem as its official State Emblem) as per the Code provided in the above Act. The Public Sector organisations and autonomous bodies should display their official logo on the Homepage of the website to re-enforce their identity.

2. The Homepage and all important entry pages of the website MUST display the ownership information, either in the header or footer.

3. The lineage of the Department should also be indicated at the bottom of the Homepage and all important entry pages of the website. For instance, at the bottom of the Homepage, the footer may state the lineage information, in the following manner:

   i. This Website belongs to Department of Heavy Industries, Ministry of Heavy Industries and Public Enterprises, Government of India' (for a Central Government Department).

   ii. This Website belongs to Department of Industries, State Government of Himachal Pradesh, India' (for a State Government Department).

   iii. This is the official Website of Gas Authority of India Limited (GAIL), a Public Sector Undertaking of the Government of India under the Ministry of Petroleum and Natural Gas (for a Public Sector Undertaking).

   iv. This is the official Website of the District Administration of Thanjavur, State Government of Tamil Nadu (India)' (for a District of India).

4. All subsequent pages of the website should also display the ownership information in a summarised form. Further, the search engines often index individual pages of a website and therefore, it is important that each webpage belonging to a site displays the relevant ownership information.

5. In case of those websites which belong to Inter-Departmental initiatives involving multiple Government Departments which are difficult to list on the Homepage, the Government ownership should still be reflected clearly at the bottom of the page with detailed information provided in the 'About the Portal/Website' section.

6. The page title of the Homepage (the title which appears on the top bar of the browser) MUST be complete with the name of the country included, for instance, instead of the title being just Ministry of Health and Family Welfare, it should state, Government of India, Ministry of Health & Family Welfare.

   Alternatively, in case of a State Government Department, it should state 'Department of Health, Government of Karnataka, India '. This will not only facilitate an easy and

unambiguous identification of the website but would also help in a more relevant and visible presence in the search engine results. Further, it is important since the screen readers used by the visually impaired users first read the title of the page and in case the title is not explanatory enough, it may confuse or mislead them.

B. Government Domains

The URL or the Web Address of any Government website is also a strong indicator of its authenticity and status as being official. In today's era with a large proliferation of websites, which resemble Government websites and fraudulently claim to provide reliable Government information and services, the role of a designated Government domain name assumes a lot of significance.

Hence, in compliance to the Government's Domain Name Policy, all Government websites MUST use 'gov.in' or 'nic.in' domain exclusively allotted and restricted to Government websites. The military institutions and organisations in India may also use 'mil.in' domain in place of or in addition to the gov.in /.nic.in domain. The above naming policy applies to all Government websites irrespective of where they are hosted.

Those Departments and Government entities that are using and have been publicising a domain name other than the above should take appropriate early action to register official government domain names and use the existing ones as 'alias' for a period of six months. An intermediary page with a clear message notifying the visitors about the change in the URL and then auto redirecting them to the new URL after a time gap of 10 seconds should be used.

The Domain Name Conventions, as specified in the '.IN Registration' policy should be followed while registering a 'gov.in' Domain Name.

National Informatics Centre (NIC) is the exclusive Registrar for GOV.IN domain names. The use of GOV.IN Domain is restricted to the constituents of Indian Government at various levels right from Central, State/UT, District & Sub-District, block, village etc.

For detailed information and step-by-step procedure on how to register a .GOV IN Domain, one may visit http://registry.gov.in **.**

C. Link with National Portal

1) **india.gov.in:** The National Portal of India is a single window source for access to all information and services being provided by the various constituents of the Indian Government to its citizens and other stakeholders.

There are exclusive sections on Citizens, Business, Overseas, Government, Know India, Sectors etc. catering to the information needs. Sections targeting special interest groups such as Government Employees, Students, Senior Citizens, Kids etc. are also present.

a) **Since the National Portal is the official single entry Portal of the Indian Government, all Indian Government websites MUST provide a prominent link to the National Portal from the Homepage and other important pages of citizens' interest**.

b) **The pages belonging to the National Portal MUST load into a newly opened browser window of the user.** This will also help visitors find information or service they could not get on that particular website. It is quite common that citizens are not aware which information or service is provided by which Department.

As per linking Policy of the National Portal, no prior permission is required to link 'india.gov.in' from any Indian Government website. However, the Department providing a link to the National Portal is required to inform the National Portal Secretariat about the various sections of the National Portal that they have linked to, so that they can be informed of any changes, updations / additions therein. Also, it is not permitted that the National Portal Pages be loaded into frames on any site. These must be loaded into a new browser window.

Special Banners in different sizes and colour schemes for providing a link to the National Portal have been given at http://india.gov.in/linktous.php

Instructions on how to provide a link have also been given. The Government websites / portals may choose any banner from the ones provided, depending upon their site design and place the same on their Homepage.

D. Content Copyright

Copyright is a form of protection provided under law to the owners of "original works of authorship" in any form or media. It is implied that the original information put up on the website by a Government Department is by default a copyright of the owner Department and may be copied, reproduced, republished, uploaded, posted, transmitted, or distributed only if the copyright policy of the concerned Department allows so.

Hence, the information, material and documents made available on an Indian Government website MUST be backed up with proper copyright policy explaining the terms and conditions of their usage and reference by others. The copyright policy of a Department could be liberal, moderate or conservative depending upon their preferences based on the kind of information available on their website. However, since it is a duty of a Government Department to provide all the information in the public domain freely to the citizens, the Departments should aim to have a liberal copyright policy.

The Departments should also be sensitive towards publishing any information having a third party copyright. The Government Departments MUST follow proper procedures to obtain the permission, prior to publishing such information on their websites.

If any published Government Document/Report is being reproduced on any website, whether as excerpts or in full, the source of the same i.e. Full Title of the Report/Document along with the name of the concerned Department and year of publication MUST be provided.

E. Content Hyper linking

Since Government websites often receive queries and requests from owners of other websites who might want to provide a hyper link to their web pages, every Indian Government website

MUST have a comprehensive and clear-cut hyper linking policy defined and spelt out for those who wish to hyper link content from any of its sections. The basic hyper linking practices and rules should ideally be common across the websites of a State/Ministry.

The hyperlinking policy enumerating the detailed criteria and guidelines with respect to hyperlinks with other sites may be made available under the common heading of **'Hyperlinking Policy'** and displayed at a common point on the Homepage of all sites under the ownership a State/Ministry.

a) To create a visual distinction for links that lead off site, Cascading Style Sheets (CSS) controls or XSL or some such similar mechanism should be used. In case the link takes the user to another website of the same Department/Ministry/ State, a seamless transition should be used through appropriate CSS controls.

b) Third party content should only be linked when consideration about the copyright, terms of use, permissions, content authenticity and other legal and ethical aspects of the concerned content have been taken into account.

c) The overall quality of a website's content is also dependent, among other things on the authenticity and relevance of the 'linked' information it provides.

d) Further, it MUST be ensured that 'broken links' or those leading to 'Page Not Found' errors are checked on a regular basis and are rectified or removed from the site immediately upon discovery.

F. Privacy Policy

Government websites should follow an extremely cautious approach when it comes to collecting personal details/information about the visitors to the sites. It should be an endeavour to solicit only that information which is absolutely necessary.

In case a Department solicits or collects personal information from visitors through their websites, it MUST incorporate a prominently displayed Privacy Statement clearly stating the purpose for which information is being collected, whether the information shall be disclosed to anyone for any purpose and to whom.

Further, the privacy statement should also clarify whether any cookies shall be transferred onto the visitor's system during the process and what shall be the purpose of the same.

Whenever a Department's website allows e-commerce and collects high risk personal information from its visitors such as credit card or bank details, it MUST be done through

sufficiently secure means to avoid any inconvenience. SSL (Secure Socket Layer), Digital Certificates are some of the instruments, which could be used to achieve this.

Annexure 16: Standards for Open APIs

Policy on Open Application Programming Interfaces (APIs)

Under the overarching vision of Digital India, Government of India (GoI) aims to make all Government services digitally accessible to citizens through multiple channels, such as web, mobile and common service delivery outlets.

To meet this objective, there is a need for an interoperable ecosystem of data, applications and processes which will make the right information available to the right user at the right time.

Interoperability among various e-Governance systems is an important prerequisite for upgrading the quality and effectiveness of service delivery. For promoting Open Standards for software interoperability across various Government departments and agencies, GoI has already notified the "Policy on Open Standards for e-Governance" and "Technical Standards on Interoperability Framework for e-Governance".

Open API is the API that has been exposed to enable other systems to interact with that system. Open API may be either integrated with the host application or may be an additional piece of software that exposes any proprietary API with an Open API equivalent. The Open API, whenever possible, may be free of charge and without restrictions for reuse & modifications.

Policy on Open APIs for Government of India" (hereinafter referred to as the "Policy") will encourage the formal use of Open APIs in Government organizations. This policy sets out the Government's approach on the use of "Open APIs" to promote software interoperability for all e-Governance applications & systems and provide access to data & services for promoting participation of all stakeholders including citizens.

The objectives of this policy are to:

i. Ensure that APIs are published by all Government organisations for all e-Governance applications and systems.
ii. Enable quick and transparent integration with other e-Governance applications and systems.
iii. Enable safe and reliable sharing of information and data across various e-Governance applications and systems.
iv. Promote and expedite innovation through the availability of data from e-Governance applications and systems to the public.
v. Provide guidance to Government organizations in developing, publishing and implementation using these Open APIs.

Government of India shall adopt Open APIs to enable quick and transparent integration with other e-Governance applications and systems implemented by various Government organizations, thereby providing access to data & services and promoting citizen participation for the benefit of the community.

The Open APIs shall have the following characteristics for publishing and consumption:

i. The relevant information being provided by all Government organisations through their respective e-Governance applications shall be open and machine readable.
ii. All the relevant information and data of a Government organisation shall be made available by Open APIs, as per the classification given in the National Data Sharing and Accessibility Policy (NDSAP-2012), so that the public can access information and data.
iii. All Open APIs built and data provided, shall adhere to National Cyber Security Policy.
iv. The Government organizations shall make sure that the Open APIs are stable and scalable.
v. All the relevant information, data and functionalities within an e-Governance application or system of a Government organisation shall be made available to other e-Governance applications and systems through Open APIs which should be platform and language independent.
vi. A Government organisation consuming the data and information from other e-Governance applications and systems using Open APIs shall undertake information handling, authentication and authorisation through a process as defined by the API publishing Organisation.
vii. Each published API of a Government organization shall be provided free of charge whenever possible to other Government organizations and public.
viii. Each published API shall be properly documented with sample code and sufficient information for developers to make use of the API.
ix. The life-cycle of the Open API shall be made available by the API publishing Government organisation. The API shall be backward compatible with at least two earlier versions.
x. All Open API systems built and data provided shall adhere to GoI security policies and guidelines.
xi. Government organizations may use an authentication mechanism to enable service interoperability and single sign-on.

The policy shall be applicable to all Government organisations under the Central Government and those State Governments that choose to adopt this policy for the following categories of e-Governance systems:

- All new e-Governance applications and systems being considered for implementation.
- New versions of the legacy and existing systems.

Annexure 17: Standards for Internet of Things

1. Sensor & Actuators

a. IEEE 1451

IEEE 1451 is a set of smart transducer interface standards developed by the Institute of Electrical and Electronics Engineers (IEEE) Instrumentation and Measurement Society's Sensor Technology Technical Committee describing a set of open, common, network-independent communication interfaces for connecting transducers (sensors or actuators) to microprocessors, instrumentation systems, and control/field networks.

b. Identification Technology

ISO/IEC JTC 1/SC31 Automatic identification and data capture techniques

It develops and facilitates standards within the field of automatic identification technologies. These technologies include 1D and 2D barcodes, active and passive RFID for item identification and OCR.

c. Domain Specific Compliance:

Sensors/IoT Devices/Actuators should follow the compliance to respective domain specific standards, like healthcare devices HL7, automobile/bus UBS-II (ITS sensor parameter & standards), OBD-II, Electric Vehicle Charging etc.

2. Communication Technology

a. Thread:

Networking protocol called Thread that aims to create a standard for communication between connected household devices.

b. AllJoyn:

Open source AllJoyn protocol was initially developed by Qualcomm provides tools for the entire process of connecting and maintaining devices on a Wi-Fi network.

c. IEEE 802.15.4:

It offers physical and media access control layers for low-cost, low-speed, low-power Wireless Personal Area Networks (WPANs).
IEEE 802.15.4e-2012, IEEE 802.15.4-2011, IEEE 802.15.4-2003, IEEE 802.15.4-2006

d. IETF IPv6 over Low power WPAN (6LoWPAN):

It defines encapsulation and header compression mechanisms that allow IPv6 packets to be sent to and received over IEEE 802.15.4 based networks.
6LoWPAN Frame Format
Fragmentation and Reassembly
Header Compression

Support for security mechanisms

e. **IETF "Routing Over Low power and Lossy (ROLL):**
IPv6 Routing Protocol for Low power and Lossy Networks (LLNs) (RPL)
RPL Topology Formation (Destination Oriented Directed Acyclic Graphs - DODAGs)
RPL Control Messages

f. **IETF Constrained Application Protocol (CoAP):**
It offers simplicity and low overhead to enable the interaction and management of embedded devices.

3. Use Case/ Application Specific:

i. **Industrial IoT (IIoT):** Object Modelling Group (OMG) has been active in IIoT standardization efforts. OMG IIoT standards and activities include (but are not limited to):
- Data Distribution Service (DDS)
- Dependability Assurance Framework For Safety-Sensitive Consumer Devices
- Threat Modelling
- Structured Assurance Case Meta-model
- Unified Component Model for Distributed, Real-Time and Embedded Systems
- Automated Quality Characteristic Measures
- Interaction Flow Modelling Language™ (IFML™)

(Source: http://www.omg.org/hot-topics/iot-standards.htm)

ii. **eHealth:** IEEE has many standards in the eHealth technology area, from body area networks to 3D modelling of medical data and personal health device communications. IEEE 11073 standards are designed to help healthcare product vendors and integrators create devices and systems for disease management.

iii. **eLearning:** The IEEE Learning Technology Standards Committee (LTSC) is chartered by the IEEE Computer Society Standards Activity Board to develop globally recognized technical standards, recommended practices, and guides for learning technology.

iv. **Intelligent Transportation Systems (ITS):** IEEE has standards activities on many aspects of ITS, such as vehicle communications and networking (IEEE 802 series), vehicle to grid interconnectivity (IEEE P2030.1), addressing applications for electric sourced vehicles and related support infrastructure, and communication for charging (IEEE 1901).

4. Consortia

a. **Open Interconnect Consortium:**

OIC (Atmel, Dell, Broadcom, Samsung, and Wind River as members) is an open environment to support the billions of connected devices coming online.

b. Industrial Internet Consortium:

It was founded by Intel, Cisco, AT&T, GE & IBM with the goal of developing standards specifically for industrial use of the Internet of Things.

5. Architecture Technology

a. IEEE P2413: Standard for an Architectural Framework for the Internet of Things

The architectural framework for IoT provides a reference model that defines relationships among various IoT verticals (e.g., transportation, healthcare, etc.) and common architecture elements.

The standard also provides a reference architecture that builds upon the reference model. The reference architecture covers the definition of basic architectural building blocks and their ability to be integrated into multi-tiered systems.

6. Further Readings for Standards

a. ITU Standardization Roadmap

This document was released on 6 May 2016. It contains a collection of Standards/ITU-T Recommendations that fit into the scope of Joint Coordination Activity for IoT and Smart Cities. It includes Standards/ITU-T Recommendations related to Internet of Things (IoT), smart cities and communities (SC&C), network aspects of identification systems, including RFID (NID) and ubiquitous sensor networks (USN). Refer References for the link.

b. IERC Position Paper on IoT Standardization:

It presents an inventory of existing standards and provides an overview of past and current activity in relation to standardization in the area of Internet of Things, and assembles a series of examples of standardization activities in this area.

Annexure 18: Standards for Disaster Management

The aim of the local disaster management standards and guidelines is to support local government / municipal corporations to develop a community specific disaster management system, including governance arrangements, a Local Disaster Management Plan (LDMP) using the comprehensive approach to disaster management.

This standard establishes a common set of criteria for all hazards disaster/emergency management with fundamental criteria to develop, implement, assess, and maintain the program for prevention, mitigation, preparedness, response, continuity and recovery.

International Standards used in Disaster Warning and Management

S. No.	Standards	Description
1.	ISO 22320:2011	Societal security – Emergency management – Requirements for incident response deals with overall approach for preventing and managing emergencies /disasters
2.	ISO 22322:2015	Societal security -- Emergency management -- Guidelines for Public warning deals with guidelines for developing, managing, and implementing Public warning before, during, and after incidents / disasters
3.	ISO 22324:2015	Societal security — Emergency management — Guidelines for colour-coded alerts deals with guidelines for the use of colour codes to inform people at risk as well as first response personnel about danger and to express the severity of a situation. It is applicable to all types of hazard in any location.
4.	ISO 31000:2009, *Risk management – Principles and guidelines*	It deals with principles, framework and a process for managing risk. It helps organizations / local bodies to increase the likelihood of achieving objectives, improve the identification of opportunities and threats and effectively allocate and use resources for risk treatment.
5.	IEC 31010:2009, Risk management -- Risk assessment techniques	It helps the decision makers understand the risks that could affect the achievement of objectives as well as the adequacy of the controls already in place. It focuses on risk assessment concepts, processes and the selection of risk assessment techniques.
6.	ISO 11320:2011	Nuclear criticality safety -- Emergency preparedness and response
7.	ASCE/SEI 41-06 *-Seismic Rehabilitation of Existing Buildings*	Standards for Seismic retrofitting of existing building including steps to better protect non-structural components (suspended ceilings, non-load-bearing walls and utility systems) and building contents (furnishings, supplies, inventory and equipment)
8.	ISO 19115-1:2014	Defines the schema required for describing geographic information and services by means of metadata. It provides information about the identification, the extent, the quality, the spatial and temporal aspects, the content, the spatial reference, the portrayal, distribution, and other properties of digital geographic data and services

Sd/-
Chief Executive Officer
Bhagalpur Smart City Limited (BSCL)