



Master System Integrator – Volume 2: Scope of Work

**Implementation of Intelligent Traffic Management System,
Adaptive Traffic Control System, CCTV and Surveillance System,
Solid Waste Management and Integrated with Command and
Control Centre (ICCC)**

ISSUED BY
Agra Smart City Limited
25th March 2018

DISCLAIMER

The information contained in this Request for Proposal document (RFP) or subsequently provided to Bidder(s), whether verbally or in documentary or any other form by or on behalf of Agra Smart City Development Company Limited (ASCL) or any of its employees or advisors, is provided to Bidder(s) on the terms and conditions set out in this RFP and such other terms and conditions subject to which such information is provided. This RFP is not an Agreement and is neither an offer nor invitation by ASCL to the prospective Bidders or any other person.

The purpose of this RFP is to provide interested parties with information that may be useful to them in making their financial offers (Bids) pursuant to this RFP. This RFP includes statements, which reflect various assumptions and assessments arrived at by ASCL in relation to the Project. Such assumptions, assessments and statements do not purport to contain all the information that each Bidder may require. This RFP may not be appropriate for all persons, and it is not possible for ASCL, its employees or advisors to consider the investment objectives, financial situation and particular needs of each party who reads or uses this RFP. The assumptions, assessments, statements and information contained in the Bidding Documents, may not be complete, accurate, adequate or correct. Each Bidder should, therefore, conduct its own investigations and analysis and should check the accuracy, adequacy, correctness, reliability and completeness of the assumptions, assessments, statements and information contained in this RFP and obtain independent advice from appropriate sources.

Information provided in this RFP to the Bidder(s) is on a wide range of matters, some of which may depend upon interpretation of law. The information given is not intended to be an exhaustive account of statutory requirements and should not be regarded as a complete or authoritative statement of law. ASCL accepts no responsibility for the accuracy or otherwise for any interpretation or opinion on law expressed herein. ASCL, its employees and advisors make no representation or warranty and shall have no liability to any person, including any Applicant or Bidder under any law, statute, rules or regulations or tort, principles of restitution or unjust enrichment or otherwise for any loss, damages, cost or expense which may arise from or be incurred or suffered on account of anything contained in this RFP or otherwise, including the accuracy, adequacy, correctness, completeness or reliability of the RFP and any assessment, assumption, statement or information contained therein or deemed to form part of this RFP or arising in any way for participation in this Bid Stage.

ASCL also accepts no liability of any nature whether resulting from negligence or otherwise howsoever caused arising from reliance of any Bidder upon the statements contained in this RFP. ASCL may in its absolute discretion, but without being under any obligation to do so, update, amend or supplement the information, assessment or assumptions contained in this RFP. The issue of this RFP does not imply that ASCL is bound to select a Bidder or to appoint the Successful Bidder JV or Contractor, as the case may be, for the Project and ASCL reserves the right to reject all or any of the Bidders or Bids without assigning any reason whatsoever.

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

Contents

DISCLAIMER.....	2
1. Introduction	12
1.1. About Agra	12
1.2. About Agra Municipal Corporation	12
1.3. About Agra Smart City Limited.....	13
1.4. Project Background.....	13
1.5. Project Objectives	15
1.6. Project Scope of Work	16
1.7. Finalization and submission of a detailed technical architecture	17
1.8. Other expectations from MSI.....	20
2. COMPONENT 1 : Adaptive Traffic Management System (ATMS)	24
2.1. Overview	24
2.2. Project Intent	25
2.3. Scope of Work.....	25
2.4. Design, Integration & Maintenance of ATMS	25
2.5. Functional Specification	26
2.6. Technical Specification.....	29
3. COMPONENT 2 and 3 : Intelligent Traffic and CCTV Surveillance System	33
3.1. Overview	33
3.2. Project Intent	33
3.3. System Architecture.....	33
3.4. Solution requirements	34
3.5. Public Address system.....	34
3.6. Variable Message Signboards	34
3.7. Emergency Call Box System or Panic Box.....	35
3.8. On site Local Processing Unit with Communication & Electrical Interface	35
3.9. Automatic Number Plate Recognition	36
3.10. Red Light Violation Detection (RLVD) system	36
3.11. E Challan System	37
3.11.1. Functional Requirements of E Challan System	37
3.11.2. Hand Held Devices.....	38
3.12. Face Recognition System	39
3.13. No Helmet Detection System.....	41
3.14. Operating Conditions.....	42
3.15. Mobile Enforcement Solution for Police.....	42

3.15.1.	Police Vehicles	42
3.15.2.	Temporary Monitoring	43
3.15.3.	Wearable Monitoring	43
3.15.4.	Modern Infra and Peripherals	44
3.16.	CCTV Surveillance Cameras - Functional Specification	44
3.16.1.	Surveillance System Infrastructure at Field Locations.....	44
3.16.2.	Networking and power cables and other related infrastructure	45
3.16.3.	Supply & Installation of CCTV Surveillance Infrastructure	45
3.16.4.	Installation of Poles/Cantilevers/Gantry	46
3.16.5.	UPS for field locations	46
3.16.6.	Outdoor Cabinets / Junction Boxes	47
3.16.7.	Civil and Electrical Works	47
3.16.8.	Earthing and Lightning Proof Measures	48
3.16.9.	Miscellaneous.....	48
3.16.10.	Mounting structure	49
3.17.	Technical Functions	49
4.	COMPONENT 4 : ICT Enabled Solid Waste Management	73
5.	Component 5 : City and Enterprise GIS Solution.....	89
5.1.	Project Objective.....	89
5.2.	Expected Benefit of the Project	89
5.2.1.	Decision Support System	89
5.2.2.	Revenue Management	89
5.3.	Analysis, Planning, Operation and Maintenance	89
5.4.	Municipal Department Utility Asset Management and Maintenance	89
5.5.	Dash Board for Project Planning, Implementation and Monitoring	90
5.6.	Scope of Work Overview.....	90
5.6.1.	Base Map Creation – Pan City.....	90
5.6.2.	Data Updating and Data Creation for ABD Area	90
5.6.3.	Provide GIS Software – Pan City	90
5.6.4.	Implementation of Enterprise GIS Suite – Pan City	90
5.6.5.	Integration GIS with existing, proposed system and Future Systems	91
5.7.	Detail Scope of Work	91
5.7.1.	Geospatial Data Creation and Updating Base Map for PAN Area	91
5.7.2.	Data Collection	91
5.7.3.	Data validation and gap analysis	92
5.7.4.	Positional Accuracy.....	92
5.7.5.	Procurement of High Resolution Satellite Imagery – Pan Area	92
5.7.6.	Geo referencing and Post Processing of Satellite Imagery – PAN area	92

5.7.7.	Data Modelling Pan Area	93
5.7.8.	Digitization of Satellite Imagery, Updating and capturing of various layers.....	93
5.7.9.	Property Survey and Property Tagging – ABD Area	94
5.7.10.	Final Base Map preparation – PAN Area	94
5.7.11.	Tentative GIS Data Layers require for Geospatial Smart City Project.....	94
5.8.	Data Migration	98
5.8.1.	Supply of Desktop GIS and Image Processing Software	98
5.9.	Supply of COTS Enterprise GIS Software	105
5.9.1.	Detail Specification of Enterprise GIS Platform	105
5.10.	Design and Development of Enterprise Web GIS Smart City Department Application	111
5.10.1.	Modules and Sub Modules of Land and Estate Management System	112
5.10.2.	Estate Management	113
5.10.3.	Disaster Fire & Emergency Services Management	113
5.10.4.	Park and Gardens Management System	114
5.10.5.	Water Management System.....	114
5.10.6.	Sewerage Operation.....	115
5.10.7.	Road and Traffic Management.....	116
5.10.8.	Strom Water Drainage Management System.....	116
5.10.9.	Street Light Management System	117
5.10.10.	Capital Project Monitoring and Control	117
5.11.	Integration GIS with existing and proposed/future Smart Systems	118
6.	Component 6 : Environmental Sensors.....	119
6.1.	Project Intent	119
6.2.	Functional Specifications	119
6.3.	Technical Specifications	120
7.	Component 7 : Data Centre (DC) and Disaster Recovery (DR) Centre	122
7.1.	Introduction	122
7.2.	Design, Configuration, Installation and Commissioning of DC and DR	122
7.3.	DR Plan and Implementation	125
7.4.	Testing and Validation	127
7.5.	Post Implementation Maintenance & Support.....	127
7.6.	Security Audit.....	128
7.6.1.	Datacenter Specification	128
7.7.	IT Infrastructure at Data Centre/ Disaster Recovery Centre.....	128
7.8.	Enterprise Management System (EMS)	132
7.9.	Central Identity Management Service	136
7.10.	Authorization	136
7.11.	Physical DC/DR Technical Specification	136



- 7.12. Unified Collaboration Solution.....182
- 8. Component 8 : City Communication and Network Infrastructure205
 - 8.1. Scope of Work.....205
 - 8.2. Security Requirements for Network as a Service205
 - 8.3. Network Operations Centre.....205
- 9. Component 9 : Integrated Centralized Command and Control Centre (CCC).....207
 - 9.1. Overview207
 - 9.2. Project Intent208
 - 9.3. Scope of Work.....209
 - 9.4. Design and Implementation of Control Room209
 - 9.5. UP Dial 100 Control Room237
 - 9.6. City Operations Platform - Functional Specifications.....239
 - 9.7. Forensic Investigation Room.....240
 - 9.8. Integrated Operation Platform (IOP)242
 - 9.9. IoT Platform – Functional Specifications.....243
 - 9.9.1. Data Aggregation, Normalization and Access.....243
 - 9.9.2. GIS Map Support.....244
 - 9.9.3. IOT platform shall enable online Developer Program tools245
 - 9.9.4. Authentication.....245
 - 9.9.5. Resiliency245
 - 9.9.6. API Repository / API Guide246
 - 9.9.7. Platform upgrade and maintenance.....246
 - 9.9.8. Platform functionality API management and gateway.....246
 - 9.9.9. SDK/API Based Open Platform.....246
 - 9.9.10. Trending Service247
 - 9.9.11. Policies and Events247
 - 9.10. Visualization Layer – Functional Specifications247
 - 9.10.1. ICCC Operations.....247
 - 9.10.2. Integration capabilities.....248
 - 9.10.3. Notifications, Alerts and Alarms.....248
 - 9.10.4. Users and roles248
 - 9.10.5. Reports249
 - 9.10.6. Standard Operating Procedure.....249
 - 9.10.7. Collaboration among Stakeholders250
 - 9.10.8. Analytics Engine.....250
 - 9.10.9. API & Interface Security.....251
 - 9.10.10. Business Operations Audit & Logging.....251
 - 9.10.11. Field Responder Mobile251

9.11.	Video Management System – Functional Specifications	252
9.11.1.	VMS Core Components	254
9.11.2.	VMS General.....	255
9.11.3.	VMS GUI Capabilities.....	256
9.11.4.	VMS Map Functionality	256
9.11.5.	VMS Configuration	257
9.11.6.	VMS User Hierarchy	258
9.11.7.	VMS Recording Requirements.....	258
9.11.8.	Manual or on demand recording.....	260
9.11.9.	VMS review system	260
9.11.10.	VMS Alarm Handling	261
9.11.11.	VMS Integration requirements.....	262
9.11.12.	VMS System Size	263
9.12.	Video Analytics – Functional Specifications	263
9.13.	Access Control System – Functional Specifications	263
9.14.	Edge Analytics and Artificial Intelligence with Continous Learning	264
9.15.	Technical Specifications	265
10.	Cyber Security Requirement – Smart City Framework.....	294
11.	Testing and Acceptance Procedures	297
11.1.	Test Plan	297
11.2.	Test scenarios	297
11.3.	Test Execution.....	298
11.4.	Testing, Commissioning & Successful Operation	300
12.	Handholding and Training	301
12.1.	Types of Trainings	302
12.1.1.	Basic IT training	302
12.1.2.	Functional Training.....	302
12.1.3.	Administrative Training	302
12.1.4.	Senior Management Training.....	302
12.2.	Post-Implementation Training.....	302
13.	Project Implementation Timelines & Deliverables.....	303
13.1.	Phase I – T + 2 months (T is the date of signing of the contract with MSI).....	303
13.2.	Phase II – T + 6 months	303
13.3.	Phase III – T + 9 months	303
13.4.	Phase IV – T1 + 60 months (T1 is the date of Go Live of all application)	303
14.	Payment Terms and Schedule	304
15.	Annexures.....	305
15.1.	Annexure 1: Junctions for Intelligent and Adaptive Traffic Signals.....	305



15.2.	Annexure 2: Intelligent Traffic Management System with General Surveillance	307
15.3.	Annexure 3: CCTV for City Surveillance System	311
15.4.	Annexure 4: Emergency Panic Button with Public Addressing System.....	319
15.5.	Annexure 5: Environment Sensors.....	321
15.6.	Annexure 6: OFC Network Availability.....	322
15.7.	Annexure 7: List of Police Stations and Chowkis	323

Definitions/Acronyms

Sr. No.	Term/ Acronyms	Description
1	AAA	Authentication, authorization, and accounting
2	ANPR	Automated Number Plate Recognition
3	ASCL	Agra Smart City Limited
4	AMC	Agra Municipal Corporation
5	AP	Access Point
6	AVLS	Automated Vehicle Locator System
7	Bid	Offer by Bidder to fulfil the requirement of ASCL for an agreed price. It shall be a comprehensive technical and commercial agreed price and response to the RFP
8	BOM	Bill of Material
9	CCC	Command and Control Centre
10	CCTV	Closed Circuit Television
11	Consortium	<p>A consortium consists of multiple members. A consortium should not consist of more than 4 (four) parties (including the Lead Bidder) entering into a Consortium Agreement for common objective of satisfying ASCL requirements & represented by lead member of consortium, designated as a "Lead Bidder". The responsibility for successful execution of the entire project will be that of defined Lead bidder. Consortium members should have relevant experience of executing similar roles and responsibilities in past as stated in the MoU in Annexure 9.</p> <p>Parent company of Bidder/ Lead bidder would be considered for only 100% subsidiary/ division/ sub division/ branch business unit.</p> <p>For technical evaluation, net worth and turnover of only the bidding entity will be considered. Net worth and turnover of any parent, subsidiary, associate or other related entity will not be considered.</p>
12	COP	Common Operating Platform
13	DBA	Database Administrator
14	DC	Data Centre
15	DCP	Deputy Commissioner of Police
16	Deliverables	Products, infrastructure and services agreed to be delivered by the Bidder in pursuance of the agreement as defined more elaborately in the RFP, Implementation and the Maintenance phases and includes all documents related to the user manual, technical manual, design, process and operating manuals, service mechanisms, policies and guidelines (such as security related, data migration related), inter alia payment and/or process related etc., source code and all its modifications.
17	DIT	Directorate of Information Technology
18	DNS	Domain Name Server
19	DR	Disaster Recovery
20	Effective	Date on which Contract Agreement for this RFP comes into effect

	Date	
21	EMD	Earnest Money Deposit
22	EMS	Enterprise Management System
23	ETA	Estimated Time of Arrival
24	ETD	Estimated Time of Departure
25	E-Procurement portal	means electronic tendering system of Government of Uttar Pradesh
26	FRS	Functional Requirement Specifications
27	GI Pipes	Galvanized iron Pipes
28	GIS	Geographical Information System
29	GoUP	Government of Uttar Pradesh
30	GPRS	General Packet Radio Service
31	GPS	Global Positioning System
32	GSM	Global Systems for Mobile Communications
33	GUI	Graphical User Interface
34	HDPE	High-Density Polyethylene
35	HO	Head Office
36	ICT	Information and Communication Technology
37	IDS	Intrusion Detection System
38	IOE	Internet of Everything
39	IG	Inspector General of Police
40	IPS	Intrusion Prevention System
41	ITIL	Information Technology Infrastructure Library
42	LAN	Local Area Network
43	LED	Light Emitting Diode
44	LOI/LOA	Letter of Intent/Letter of Award
45	MoU	Memorandum of Understanding
46	MTBF	Mean Time Between Failures
47	MTTR	Mean Time to Repair
48	MUX	Multiplexer
49	NFC	Near Field Communication
50	NIC	National Informatics Centre
51	Non-Compliance	means failure/refusal to comply with the terms and conditions of the tender
52	Non-responsive	means failure to furnish complete information in a given format and manner required as per the tender documents or non-submission of tender offer in given forms / pro forma or not following procedure mentioned in this tender or any of required details or documents is missing or not clear or not submitted in the prescribed format or non-submission of tender fee on EMD
53	O&M	Operations & Maintenance
54	OEM	Original Equipment Manufacturer
55	OFC	Optical Fibre Cable
56	OGC	Open Geospatial Consortium
57	OS	Operating Systems

58	OTP	One Time Password
59	PA System	Public Address System
60	PDU's	Power Distribution Units
61	PIS	Passenger Information System
62	PoE	Power over Ethernet
63	PoP	Points of Presence
64	PTZ	Pan Tilt Zoom
65	QR Code	Quick Response Code
66	Required Consents	Consents, waivers, clearances and licenses to use ASCL Intellectual Property Rights, rights and other authorizations as may be required to be obtained for the software and other items that DIT, GoM their nominated agencies are required to make available to Bidder pursuant to this Agreement;
67	RF	Radio Frequency
68	RFID	Radio Frequency Identification
69	RFP	Request for Proposal
70	RLVD	Red Light Violation Detection
71	RoW	Right of Way
72	RPO	Recovery Point Objective
73	RTO	Recovery Time Objective
74	Service Level	Level of service and other performance criteria which will apply to the Services delivered by the Bidder;
75	MSI	Master System Integrator
76	SLA	Service Level Agreement; Performance and Maintenance SLA executed as part of this Master Service Agreement;
77	SNMP	Simple Network Management Protocol
78	SMPS	Switched Mode Power Supply
79	SOP	Standard Operating Procedure
80	SOS	Save Our Souls. SOS is international Morse code distress signal
81	Successful Bidder	Bidder who is qualified & successful in the bidding process and is awarded the work
82	TRAI	Telecom Regulatory Authority of India
83	TRS	Technical Requirement Specifications
84	UPS	Uninterruptible Power Supply
85	URL	Uniform Resource Locator
86	VA	Video Analytics
87	VaMS	Variable Message System
88	VCA	Video Content Analytics
89	VLAN	Virtual Local Area Network
90	VMS	Video Management Software/System
91	WAN	Wide Area Network

1. Introduction

1.1. About Agra

Agra, the city of Taj Mahal, is the 3rd most populous city in Uttar Pradesh and is the administrative headquarters of the Agra district. The city is a major tourist hub with number of monuments like Agra Fort and Fatahpur Skiri Fort, other than the Taj Mahal, which have been listed as the UNESCO World Heritage sites.

In the past few decades, Agra Development Authority (ADA) Area has experienced unprecedented spatial expansion from 61.80 sq km in 1971 to 520.20 sq km in 2008 and also a steep rise in population. The city's population grew from just 5.91 lakhs in 1971 to more than 9.78 lakhs in 1991 and in the census of 2001 the city's population was found to be 12.75 lakhs. It is now a million plus city.

The administrative limits of the Agra Nagar Nigam (ANN) encompass an area of 141.0 sq. km with a population density of about 9,043 persons per sq. km. The highest density is in the old city areas where the settlements started flourishing from the Mughal period like Lohamandi, Shahganj and the density is lowest in colonial Agra.

Although the spatial growth has been considerable, disproportionate spatial development has led to pockets of high density in terms of employment and population, putting pressure on the infrastructure of the city. A phenomenal increase in commercial activities were witnessed during the post-independence period with the associated industrial development and establishment of industrial estate, which resulted in the increase of city population.

In 1998 Ministry of Environment and Forests, Government of India notified an area of 10400 square kilometer as Taj Trapezium Zone (TTZ). The CPCB delineated the Taj Trapezium Zone on the basis of the weighted mean wind speed in twelve directions from Agra to Mathura and Bharatpur. The boundaries of the zone were made keeping in mind the possible effect of pollution sources in this zone on the critical receptor- the Taj Mahal. It banned the use of coal/ coke in industries located in the TTZ with a mandate for switching over from coal/ coke to natural gas, and relocating them outside the TTZ or shutting down. Promoting bicycling shall thereby support this objective by adding a green, non – polluting mode of transportation.

1.2. About Agra Municipal Corporation

The Agra Nagar Nigam (ANN) is among the largest municipal bodies in the state of Uttar Pradesh providing civic services to the estimated population of 1,686,976 (as per 2010 est.) Within its jurisdiction are some of the most attractive tourist spots of the world including Taj Mahal and Sikandra. ANN came into existence under the Nagar Mahapalika Adhiniyam, 1959 of UP. Since then, the Municipal Body has always been responsive in its constitution and functioning to the growing needs of citizens. Agra Nagar Nigam (ANN) is a local government body committed to providing basic

infrastructure facilities including entertainment facilities to the people of the city. ANN is very well known for managing the city by using private sector participation as well as introduction of innovative mechanism in management to serve people efficiently. The city has prepared different plans for improving services and to nullify gap between services and demands. Health Department of ANN takes up the responsibility of health and sanitation management with Chief Health Officer heading the department, whereas Engineering Department assists in the procurement of the vehicles, equipment and developing the landfill site, etc. The Health Department has total employee strength of 2299 out of which 2090 (90.9%) are the sanitary workers. Agra Nagar Nigam is committed to clean & green Agra and promotes any cause help reducing pollution as in the case of bicycling. Agra Nagar Nigam is also to participate in Swachh Sarveshan 2018 to be held after January 4, 2018.

The urban local bodies in the state of Uttar Pradesh are governed by two important legislation viz. UP Municipal Corporations Adhiniyam, 1959 and UP Municipalities Act. 1916. These two acts specify the governance framework, spatial jurisdiction and the functional domain of the urban local bodies. The corporation has a democratically elected leadership from the constituencies within the geographic jurisdiction of the corporation boundaries.

1.3. About Agra Smart City Limited

Agra Smart City Limited (ASCL) is a Special Purpose Vehicle (SPV) created with representation from all major stakeholders from the city of Agra, as per the Government of India's Smart City guidelines. This SPV is responsible for the implementation of projects under the smart city mission. This SPV shall carry end to end responsibility for vendor selection, implementation, and operationalization of various smart city projects.

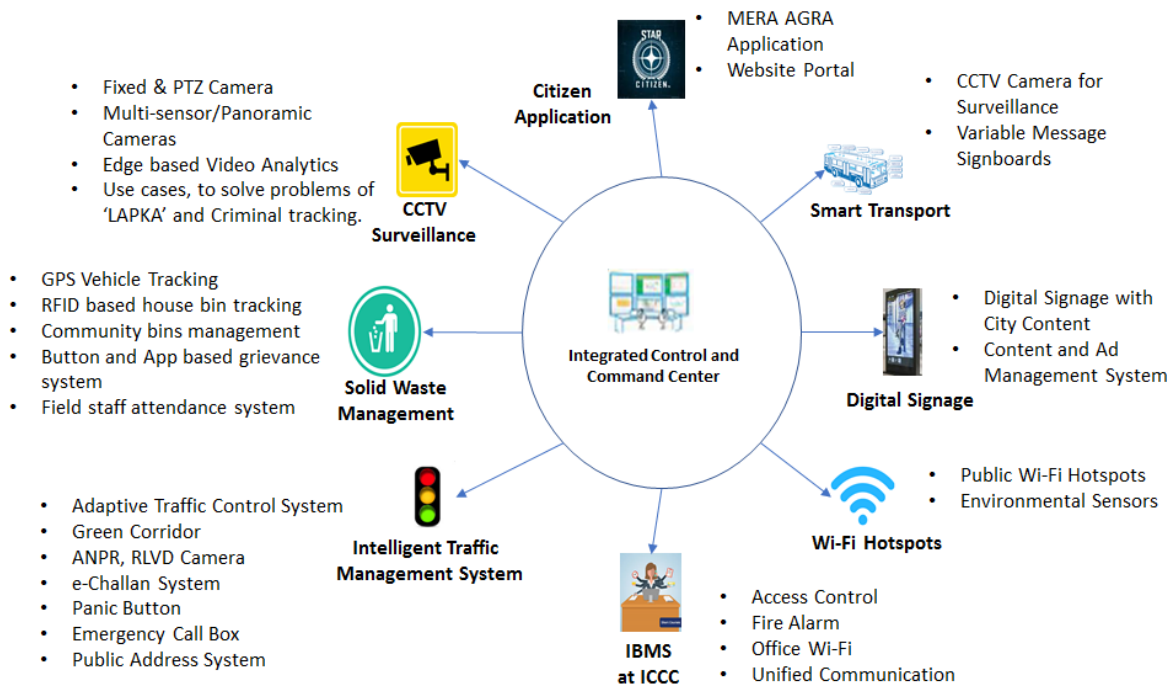
1.4. Project Background

One of the primary objective of Agra under its smart city mission is to enhance the safety and security for the citizen of Agra and worldwide tourism visiting Agra for the beauty, affection and love symbol of Heritage Monument "TAJ MAHAL". Other objective caters to bring law enforcement and public awareness among citizen of Agra on various horizon of Traffic Rules, Safe Driving, Solid Waste and Improve Sanitation which shall promote a better quality of life for residents and also enhance and improve the efficiency of municipal services.

In order to achieve these objectives, Agra Municipal Corporation desires to foster the development of a robust ICT infrastructure that supports digital applications and ensures seamless steady state operations, transport and traffic management, emergency response mechanisms and real time tracking of services and vital city metrics throughout the city and in government departments.

ASCL is considering the appointment of a MSI to set up these priority initiatives identified under the Smart City mission which will include Integrated Command and Control Centre (ICCC) and Smart Elements, CCTV Surveillance System, Intelligent Transport Management System (ITMS), Adaptive Traffic Control System (ATCS), Solid Waste Management (SWM), environment sensors, Digital Signage, Smart Parking etc.

Together with the above initiatives, Agra Smart City Limited also intends to embrace the Artificial Intelligence (AI) and Deep Learning technologies to analyze the huge amount of metadata from multiple surveillance cameras across several locations, which is saved as signatures and reproduced rapidly when time is of essence. Actionable intelligence derived from such technologies can be used to solve many local problems like "Lapka culture" (culture of touts), locating and tracking suspect individual's movements and traffic violations etc. primarily around critical infrastructures and heritage sites.



1.5. Project Objectives

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

Following are the intangibles that should be addressed by the proposed interventions:

- 1) Efficient traffic management
- 2) Efficient transport management
- 3) Enhanced safety and security
- 4) Better management of utilities and quantification of services
- 5) Asset Management
- 6) Disaster Management and Emergency Response
- 7) Integration with all existing, proposed and future services as identified by Agra Smart City limited (ASCL) in the city including but not limited to (with provision for future scalability):
 - i. CCTV Surveillance system
 - ii. Adaptive Traffic Control System
 - iii. Intelligent Transport Management System
 - iv. Solid waste management
 - v. Smart Parking
 - vi. Panic Button/Emergency Call Box
 - vii. Public Address System
 - viii. Environmental sensors
 - ix. GIS based System
 - x. Meragra Citizen Application Mobile App and ASCL Web Portal

Future Services

- i. Smart Poles
- ii. Smart Lighting
- iii. Smart Governance
- iv. City Network
- v. City Wi-Fi
- vi. Water SCADA & Smart Meters
- vii. Sewerage
- viii. Storm water Drainage
- ix. E-Medicine/Health
- x. E-Education
- xi. Disaster Management
- xii. Grievance Management
- xiii. Fire
- xiv. Any other sensors/systems
- xv. E-Governance – Including service delivery gateway like NSDG, SSDG, MSDG etc.

Smart Policing and Integrated Module

- i. Crime and Criminal Tracking Network and Systems (CCTNS)
- ii. e-Prison
- iii. e-Courts
- iv. Interoperable Criminal Justice Systems (iCJS)
- v. Shall be able to integrate directly or through bridge with all available applications which are launched by Government of UP

1.6. Project Scope of Work

Agra Smart City Company Ltd intends to select a Master System Integrator (MSI) for city of Agra by following competitive bidding process to design, develop, implement and maintain the Smart City System for a period of five years after Go Live date on turnkey basis. MSI will develop a Centralized Command & Control Centre which shall be managed by Police for City Surveillance and Law Enforcement through CCTV Cameras, Public Awareness, Proactive Monitoring for Catastrophic Situation and Manage the VIP and Emergency Movement along (CCC) and City for managing various utilities like Automated Traffic Signal, Solid Waste Management, Public Transport Movement etc. as Integrated Smart City System for Agra.

Main objective of the project is to create synergies within and across various departments of AMC for efficient city administration. To achieve this MSI shall also ensure appropriate check points are built in the various smart city solutions. This will ensure optimum and efficient delivery of public services to the citizens and visitors of Agra city.

MSI shall be responsible to carry out detailed survey prior to submission of bid for the various components of smart city solution to finalize infrastructure requirement, network bandwidth requirement, operational & administrative challenges, etc.

The subsequent sections mention the detailed scope of work, functional requirement and technical specifications for each component of smart city solution. MSI shall note that the activities defined in the scope of work mentioned in this RFP are indicative and may not be exhaustive. MSI is expected to perform independent analysis of any additional work that may be required to be carried out to fulfil the requirements as mentioned in this RFP and factor the same in its response.

More specifically, the following will be the activities to be carried out by MSI:

- i. Project Planning, Execution and Management
- ii. Assessment and Gap analysis of requirement for all smart city components under scope.
- iii. Solution Design, System Customization and development for all components mentioned in the scope of work.
- iv. Procurement, installation, deployment and commissioning of ICT and other equipment
- v. Site Preparation including required civil work, LAN/WAN Networking
- vi. Application and general awareness Training
- vii. Business Process Reengineering for the selected applications/ services, if required
- viii. STQC Certification

- ix. UAT & Go live
- x. Training & Capacity Building Support
- xi. Technical Support
- xii. Operation & Maintenance (O & M) for 5 Years starting from Go-Live date.

1.7. Finalization and submission of a detailed technical architecture

MSI will be required to prepare detailed Technical Architecture for various components of smart city solution as mentioned in the RFP and finalize the detailed architecture for the overall system, incorporating findings of site survey. MSI shall submit the detailed Technical Architecture and description of each component, along with the bid, ensuring compliance to the following guiding principles:

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

The architecture should be scalable (cater to increasing load of internal and external users and their transactions) and capable of delivering high performance till the system is operational. In this context, it is required that the application and deployment architecture should provide for Scale-Up and Scale out on the Application and Web Servers, Database Servers and all other solution components. The data centre/ disaster recovery centre infrastructure shall be capable of serving at least 1000 concurrent users.

The Applications proposed for various solutions shall be capable of handling growth for next 5 years from Go-Live date. ***MSI shall clearly quantify the expansion capabilities of the application software without incurring additional cost.***

- 2) **Availability:** The architecture components should be redundant and ensure that are no single point of failures in the key solution components. Considering the high sensitivity of the system, design should be in such a way as to be resilient to technology sabotage. To take care of remote failure, the systems need to be configured to mask and recover with minimum outage. The MSI shall make the provision for high availability for all the services of the system. Redundancy to be considered at DC/DR centre components level. The system should be designed to have uptime for 99.982%.
- 3) **Security:** The architecture must adopt an end-to-end security model that protects data and the infrastructure from malicious attacks, theft, natural disasters etc. MSI must make provisions for security of field equipment as well as protection of the software system from hackers and other threats. Using Firewalls and Intrusion Prevention Systems such attacks and theft should be controlled and well supported (and implemented) with the security policy. The virus and worm

attacks should be well defended with gateway level Anti-virus system, along with workstation level Anti-virus mechanism. There should also be an endeavour to make use of 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 ASCL would carry out the security audit of the entire system upon handover and at regular interval during O&M period.

Field equipment installed through this Project would become an important public asset. During the contract period of the Project, the MSI shall be required to repair / replace any equipment, if stolen / damaged/faulty. Appropriate insurance cover must be provided to all the equipment supplied under this project. The systems implemented for project should be highly secure, considering that it is intended to handle sensitive data relating to the city and residents of the city. The overarching security considerations are described below.

- i. The security services used to protect the solution shall include: Identification, Authentication, Access Control, Administration and Audit and support for industry standard protocols.
 - ii. Solution shall support advanced user authentication mechanisms including digital certificates and biometric registration through Aadhar Database whereas authentication post registration can be local
 - iii. 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.
 - iv. 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.
 - v. The overarching requirement is the need to comply with ISO 27001 standards of security.
- 4) **Manageability:** Ease of configuration, ongoing health monitoring, and failure detection are vital to the goals of scalability, availability, and security and must be able to match the growth of the environment. Network should be auto/manual configurable for various future requirements for the ease of maintenance / debugging.
- 5) **Interoperability:** The system should have capability to take feed from cameras installed by private / Govt. at public places. If required, MSI will also be responsible to digitize & compress the images and feeds & search as per requirements.
- 6) **Open Standards:** MSI to ensure that all the Systems should use Open Standards and protocols to the extent possible like Hadoop in case of Big Data and Analytics. No additional cost for licenses on proprietary tools shall be incurred by ASCL
- 7) **Single-Sign On:** The application should enable single-sign-on so that any user once authenticated and authorized by system is not required to be re-authorized for completing any of the services in the same session. For employees of the department concerned, the browser based application accessed on the intranet, through single-sign-on mechanism, will provide access to all the services of the departments concerned (based on their roles and responsibilities), Help

module, basic and advanced reporting etc. Similarly, for external users (citizens, etc.), based on their profile and registration, the system shall enable single-sign on facility to apply for various services, make payments, submit queries /complaints and check status of their applications.

- 8) **Interoperability Standards:** Keeping in view evolving needs of interoperability, the possibility that the solution shall become focal point of delivery of services, and may also involve cross-functionality with the e-Government projects of other departments / businesses in future, the solution should be built on Open Standards. The MSI shall ensure that the application developed is easily integrated with the existing applications. The code should not build dependency on any proprietary software, particularly, through use of proprietary 'stored procedures' belonging to a specific database product. The standards should:
 - a. At least comply with published e-Governance standards, frameworks, policies and guidelines available on <http://egovstandards.gov.in> (updated from time-to-time); and
 - b. Be of leading industry standards and /or as per standards

- 9) **GIS Integration:** MSI shall undertake detail assessment for integration of all Field level ICT interventions proposed. MSI is required to carry out seamless integration to ensure ease of use of GIS in Dashboards in Command Control Centre and Operation Command Centre. If this requires field survey, it needs to be done by MSI. If such a data is already available with city, it shall facilitate to provide the same. MSI to check the availability of such data and suitability for the project. MSI is required to update GIS maps from time to time.

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

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

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.

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

1. The Modules specified will be developed afresh based on approved requirement.
2. 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 services will be processed through department specific Application in backend.

1.8. Other expectations from MSI

- i. MSI shall engage early in active consultations with the ASCL, 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.
- ii. MSI shall assess existing infrastructure's current ability to support the entire solution and integrate the same with the proposed solution wherever applicable and possible
- iii. MSI shall judiciously evaluate the resources and time planned for undertaking current state assessment, given the overall timelines and milestones of the project.
- iv. MSI shall be responsible for supply of all the Products/equipment such as 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.
- v. MSI shall be responsible for supply of passive components indicated in the Bill of Materials section of the RFP viz. Housings, Fibre Patch Cords, Racks, etc.
- vi. Validate / Assess the re-use of the existing infrastructure if any with ASCL site
- vii. Supply, Installation, and Commissioning of entire solution at all the locations.
- viii. MSI shall provide bandwidth required for operationalizing each smart city initiative. Bandwidth requirement shall be analysed and procured by MSI at its own cost / risk.
- ix. MSI shall Install and commission connectivity across all designated locations.
- x. MSI shall ensure high availability, reliability and redundancy of the network elements to meet the Service Level requirements.
- xi. MSI shall be responsible for up gradation, enhancement and provisioning additional supplies of network (including active / passive components), hardware, software, etc. as requisitioned by ASCL.
- xii. MSI shall ensure that the infrastructure provided under the project shall not have an end of life within 12 months from the date of bidding
- xiii. MSI shall ensure that the end of support is not reached during concurrency of contract and 5 years thereafter.
- xiv. MSI shall ensure compliance to all mandatory government regulations as amended from time to time.
- xv. MSI 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, cables, software, licenses, tools, etc. are provided according to the requirements of the solution.
- xvi. ASCL shall not be responsible if MSI has not provisioned some components, sub-components, assemblies, sub-assemblies as part of Bill of Materials in the Bid. MSI shall have to provision these & other similar things to meet the solution requirements at no additional cost and time implications to ASCL.

- xvii. All software licenses that MSI 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 ASCL shall have the flexibility to use the software licenses for other requirements if required.
- xviii. MSI shall ensure there is a 24x7 comprehensive onsite support for duration of contract for respective components to meet SLA requirement. MSI shall ensure that all the OEMs understand the service levels required by ASCL.
- xix. Considering criticality of infrastructure, MSI is expected to design the solution considering RFP requirement of no single point of failure with high level of redundancy and resilience to meet the network uptime requirements.
- xx. MSI shall be responsible for periodic updates & upgrades of all equipment, cabling and connectivity provided at all locations during the contract period.
- xxi. MSI shall be responsible for setting up / building / renovating the necessary physical infrastructure including provisioning for network, power, rack, etc. at all the locations.
- xxii. MSI is expected to provide following services, including but not limited to:
 - a. Provisioning hardware and network components of the solution, in line with the proposed ASCL's requirements
 - b. Size of network devices (like router, switches, security equipment including firewalls, IPS/IDS, routers, etc. as per location requirements with required components/modules, considering redundancy and load balancing in line with RFP.
 - c. Size and provision the LAN/WAN bandwidth requirements across all locations considering application performance, data transfer, CCC/OCC, DC/DR and other requirements for smart city initiatives.
 - d. Size and provision the internet connectivity for Service Provider network and Network Backbone.
 - e. Liaise with service providers for commissioning and maintenance of the links.
 - f. Furnish a schedule of delivery of all IT/Non-IT Infrastructure items
 - g. All equipment proposed as part of this RFP shall be rack mountable.
 - h. ASCL may at its sole discretion evaluate the hardware sizing document proposed by the MSI. MSI needs to provide necessary explanation for sizing
 - i. Complete hardware sizing for the complete scope with provision for upgrade
 - j. Specifying the number and configuration of the racks (size, power, etc.) that shall be required at all the locations.
 - k. MSI shall provide for all required features like support for multiple routing protocols, congestion management mechanisms and Quality of Service support.
 - l. MSI shall ensure that all 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.
- xxiii. MSI shall directly interact with electricity boards for provision of mains power supply at all desired locations for any Field Infrastructure solution. ASCL shall facilitate, if any documentation is required from its side. MSI shall be responsible for provisioning of requisite electricity power and its recurring charges (during operational phase). MSI may provision the same under appropriate heads in the commercial bid.
- xxiv. All existing road signs which are likely to be affected by works are to be carefully taken down

- and stored. Signs to be re-erected shall be cleaned, provided with new fixings where necessary and the posts re-painted in accordance with ASCL guidelines. Road signs, street name plate etc. damaged by MSI during their operation shall be repaired or replaced at MSI's cost.
- xxv. The infrastructure of existing Traffic signal systems or any other filed Infrastructure including the poles, cantilevers, aspects, controllers and cabling and associated mountings and civil infrastructure may need to be dismantled (where ever applicable) and replaced with the new systems proposed and shall be in the scope of MSI. The dismantled infrastructure shall be delivered at ASCL designated location without damage, at no extra cost.
- xxvi. Prior to starting the site clearance, MSI shall carry out survey of field locations, for buildings, structures, fences, trees, existing installations, etc. ASCL shall be fully informed of results of survey and amount and extent of demolition and site clearance shall then be agreed with AMC.
- xxvii. Lightning Proof Measures:
- a. MSI shall comply with lightning-protection and anti-interference measures for system structure, equipment type selection, equipment earthing, power, signal cables laying.
 - b. 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 functions; capable to bear certain mechanical external force.
 - c. Signal separation of low and high frequency; equipment protective field shall be connected with their own public equal power bodies; small size/equipment signal lightning arrester shall be erected before the earthling.
 - d. 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.
 - e. Data line protection shall be installed as per zone defined in IEC 62305.
 - i. Type 1 device shall be installed between zone 0B and zone 1.
 - ii. Type 2 devices shall be installed before the equipment in zone 2 and 3.
- xxviii. After signing of contract, MSI needs to deploy team proposed for the project and ensure that a Project Inception Report is submitted to ASCL should cover following aspects:
- a. Names of Project Team members, their roles & responsibilities
 - b. Approach & methodology to be adopted to implement the Project (which should be in line with what has been proposed during bidding stage, but may have value additions / learning in the interest of the project).
 - c. Responsibility matrix for all stakeholders
 - d. Risks the MSI anticipates and plans they have towards their mitigation.
 - e. Detailed Project Plan, specifying dependencies between various project activities / sub-activities and their timelines.
- xxix. Feasibility Report for all ICT projects should be conducted. As part of feasibility report, MSI should provide detailed to-Be designs (Junction layout plans) specifying following:
1. High Level Design (including but not limited to)
 - i. Application architecture documents

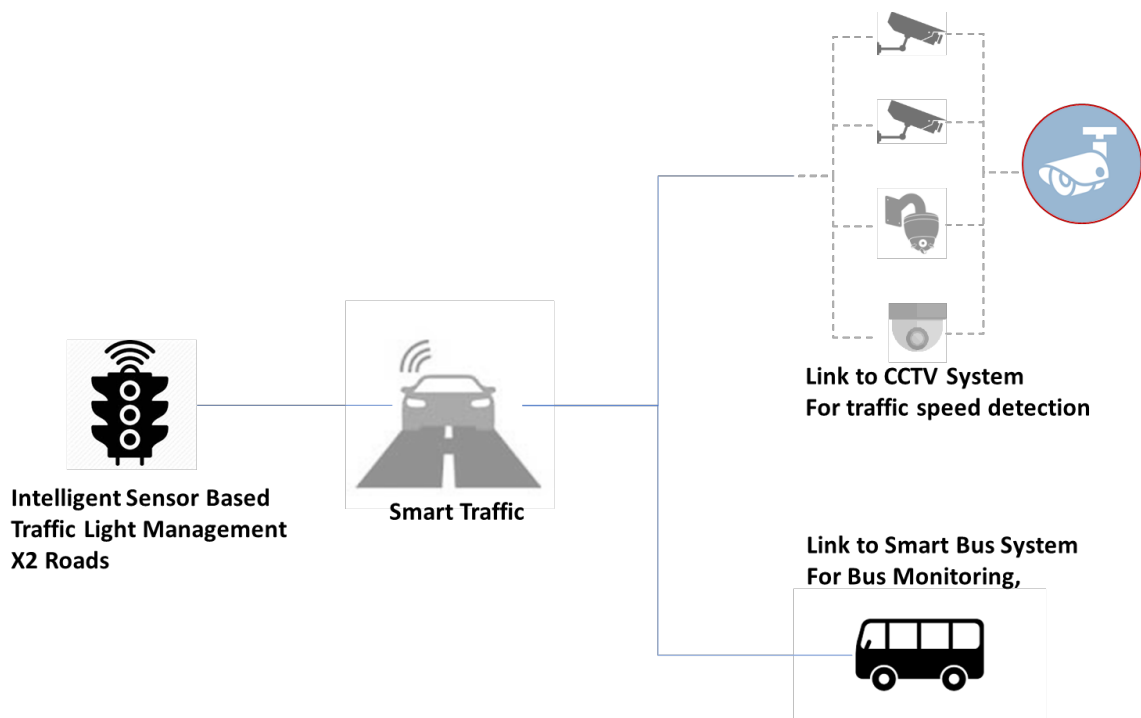
- ii. ER diagrams and other data modelling documents
 - iii. Logical and physical database design
2. Data dictionary and data definitions
- Application component design including component deployment views, control flows, etc.
 - Field equipment deployment architecture
 - Low Level Design (including but not limited to)
 - i. Application flows and logic including pseudo code o GUI design (screen design, navigation, etc.)
 - ii. Database architecture, including defining data structure, data dictionary as per standards laid-down by Government of India/ Government of Uttar Pradesh
3. Location of all field systems and components proposed at junctions/other locations,
4. Height and foundation of Traffic Signals and Standard Poles for Pedestrian signals.
5. Height and foundation of poles, cantilevers, gantry and other mounting structures for other field devices
6. Location of Junction Box
7. Location of PoP
8. Electrical power provisioning

xxx. Any functionality not expressly stated in this document but required to meet the needs of the project to ensure successful operations of the system shall essentially be under the scope of MSI and for that no extra charges shall be admissible. It is also expected for MSI to have periodic upgrades of both hardware and software as part of O&M. This shall also extend to have complete technology refresh as per latest firmware and software version at the end of contractual period (shall not limit to 5 years).

2. COMPONENT 1 : Adaptive Traffic Management System (ATMS)

2.1. Overview

As part of smart city project, major traffic junctions have been identified. Currently, the city does not have advanced ICT enabled Traffic Management and Communication tool/system and the existing system is facing problems like:



- 1) Traffic congestion and huge waiting time
- 2) No Priority for emergency vehicles like ambulance, police, etc.
- 3) VIP movement clearance
- 4) Lack of information on prominent & frequent traffic congestions both location wise and time wise for city authorities
- 5) Absence of real-time traffic and congestion information to the public
- 6) Absence of central control mechanism to monitor & regulate the city traffic flow

ASCL intends to implement an Intelligent Traffic Management System within the existing landscape to:

- 1) Automate the process of traffic management by optimally configuring traffic junction signals on real time basis
- 2) Minimize traffic congestions and waiting time
- 3) Centrally controlled traffic management system to ensure smooth movement of emergency services like ambulance, police etc.
- 4) Increase Traffic Signal Efficiency
- 5) Improve Journey Time Reliability
- 6) Managed & coordinated VIP movements

- 7) Availability of traffic data to further analyses and optimize the traffic flow
- 8) Real Time Incident Message and Advisory Messages to citizens
- 9) Improved Traffic Regulation

2.2. Project Intent

The Adaptive Traffic Management System shall be installed on specific stretch of the road to make it a model smart road. On this stretch of road, the signals will be fully automated based on sensors technology.

2.3. Scope of Work

1. MSI shall study existing traffic management systems and processes deployed by the Traffic Police, MIS reporting requirements, problem areas and expectations of Agra Traffic Police.
2. Collect data of existing operating conditions, traffic volumes across various time periods of a day, which will cover all peak and non-peak hours, weekends, etc., saturation flow rates, free flow travel time through the junction and actual travel time in peak operating conditions.
3. Journey time surveys for as-Is conditions should be conducted along designated corridors which should be designed such that all junctions are picked in at least one corridor. For major junctions, both directions (e.g. east-west and north-south) and key turning movements should also be covered.
4. Develop Feasibility report for finalization of detailed technical architecture and project plan along with following KPI's
 - i. Volume of vehicles moving on the road network
 - ii. Vehicle type distribution
 - iii. Directional distribution
 - iv. Physical and visual characteristics of the area
 - v. Travel times, delays between different points of the network
 - vi. Vehicle Emission based on emission measurement requirements of the city
 - vii. Additional dependencies with respect to available infrastructure and geometry at junctions
 - viii. Any other relevant data which MSI anticipates will assist in establishing benchmarks for the project
 - ix. Expected Measurable Improvements against each KPI
5. MSI shall identify customization or additional installations needed to deploy a standardized ATMS solution as per the functional specifications.
6. Feasibility report will include As-Is study, Improvements, Gap analysis

2.4. Design, Integration & Maintenance of ATMS

This shall consist of following activities:

1. Preparation of Solution Architecture and Gap Analysis
2. Installation of vehicle detectors, controllers and other required accessories for

- successful operation of the ATMS for ASCL.
3. Installation of ATMS software application as per functional requirements specified by ASCL.
 4. Procurement and supply of necessary software required for successful functioning of the ATMS sub module.
 5. Integration of ATMS infrastructure with existing traffic applications
 6. Configuration of traffic signal at each junction along with development of signal control plan for individual operations, coordinated signal plan for junction in sync with area wide signal plan for different operating conditions. Operating conditions may include peak, off-peak conditions, special events, contingency plans etc.
 7. MSI shall supply, install, commission and maintain the following
 - i. Adaptive Traffic Management System (ATMS) – Vehicle detectors, Signal controller, Traffic light aspects & poles, power supply and related accessories and associated civil work including cabling for successful operation of the system
 - ii. Provide software platforms in Data Centre (DC) /Disaster Recovery Centre which would aggregate incoming data streams onto a single platform, provide traffic flow estimates for near term future on a real-time basis and assist in analysing impact of alternate traffic management strategies.
 - iii. Develop individual signal control strategies including definition of signal grouping, setting of potential strategies for traffic control under various scenarios, specification of traffic management strategies for planned and unplanned events
 - iv. Develop a consolidated database of incoming real time data for future analysis and evaluation purposes. It is envisaged that the proposed adaptive traffic management system will incorporate historic trends for development of traffic management strategies and adaptive control strategies.
 - v. Field Equipment: Design, Supply, Installation, Commissioning and Maintenance of following field equipment envisaged in ATMS:
 - a. Adaptive Traffic Control/Management System at specified Signalized traffic junctions
 - b. Network Connectivity: Will use Network as a Service from the ISP to connect to the Data Centre and CCC/OCC.

2.5. Functional Specification

General:

1. The system would be used to monitor and control traffic signals, including signalized pedestrian crossings, using a traffic responsive strategy based on real-time detector data.
2. All signal controllers under Adaptive Traffic Management System shall be provided with inputs from non-intrusive vehicle detection sensors for detecting traffic state and communicating demand data to central ATCS server and to receive control instructions on the control strategy in near real-time.
3. The system should be extensible to add more signals whenever required.
4. Existing infrastructure at the junctions that might help in traffic control (e.g. ANPR cameras, CCTV cameras etc.) , where possible, should be integrated with the proposed ATMS.

Traffic detectors:

1. For major roads: Non-intrusive video based traffic detectors for detecting traffic demand on major road approaches to junctions
2. It shall provide presence detection for a minimum of 4 zones
3. The detector shall be able to detect the presence of vehicles near stop-line in non-lane based mixed traffic flow conditions.
4. It shall provide both non-directional and directional detection in up to 4 directions, user-configured for each zone.
5. The sensor firmware shall be capable of being upgraded after installation.
6. For minor roads: Non-intrusive video based traffic detectors or microwave radar based traffic detectors for detecting traffic demand on minor road approaches to junctions

Traffic signal controller:

1. The controller should support the required number of phases and stage for 3-way, 4-way and 5-way junctions for operation during different times of the day and day of the week and for special day types
2. The ATCS controller should define common inter-green period formed by the clearance Amber and Red extension period. It shall also be possible to program individual inter-green period from 3 Seconds to 10 Seconds.
3. The controller shall have a facility to list all conflicting phases at an intersection. After configuration, a traffic engineer shall verify that the signal aspects are functioning as expected for all signal plans before go live.
4. During power up the controller shall initially execute the Flashing Amber / Flashing Red plan for a time period of 3 Seconds to 10 Seconds.
5. Fault monitoring should be available for the traffic controller and the signal aspects under all modes of operations. The fault data should be communicated to the central ATCS server in near-real-time.
6. 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. The conflict data should be communicated to the central ATCS server in near-real-time.
7. The controller shall be able to interface with a wide variety of detectors having industry standard open collector interface.
8. The controller shall support the following modes of operation:
 - i. Fixed time mode - the controller shall execute a pre-set signal plan based on the time of the day and day of the week. Signal timings will not be modified dynamically using real-time traffic detector data under this mode.
 - ii. Vehicle Actuated (VA) mode - the controller shall execute a pre-set VA logic and not have fixed stage durations. The green time for each stage shall be bound by the constraints of specified minimum green and maximum green times. The actual green time is determined based on the vehicular demand obtained from the traffic detectors at the given approach and conflicting approaches using VA logic.

- iii. ATCS mode - the controller shall execute optimized signal timings determined by the ATCS application in the control center using inputs from traffic detectors, including cycle time, splits and offsets. The traffic signal controller can optionally have the ability to locally override the signal timings determined by the central ATCS.
9. The controller shall provide either a fixed operator console or support a portable one to allow traffic engineers to program the controller on-site.
10. No proprietary protocols shall be used for communication between the traffic signal controller and ATCS server.

ATCS Application:

1. The ATCS application should determine optimal signal timings dynamically using near-real-time detector data for a group of junctions using any suitable algorithm. The system should be able to determine a common cycle time for a group of junctions, splits and offsets between adjacent signals.
2. The application should support selective vehicle priority for movement of buses and other important vehicles such as ambulances, fire engines etc.. To avoid queue build-ups, the system shall also provide compensated green to the other stages after the passage of a priority vehicle
3. The application shall allow specification of green corridors for movement of Emergency Response vehicles, such as ambulances, VIP vehicles, fire engines and police vehicles.
4. The application support interfacing with a commonly used microscopic traffic simulation software for pre and post implementation analysis and study of the proposed ATCS control strategy.
5. The application shall optionally be able to estimate a common operational view of the network state by fusing data from multiple sources such as detectors as well as ANPR, GPS or any other such data collected from other third party sensors/detectors/cameras.
6. The application should be capable of operating in the following four modes:
 - i. **Fixed-time mode:** This mode should enable traffic police personnel to select and run fixed-time traffic signal timing plans using the ATCS interface available in the CCC. The signal timing plans should be able to support fixed offsets between pairs of adjacent traffic signals.
 - ii. **VA mode:** Individual signals should be able to run on stand-alone VA mode.
 - iii. **Fully adaptive mode - tactical:** Signal timings for a group of junctions should be dynamically optimized using near-real-time detector data.
 - iv. **Remote operation:** Traffic police personnel should be able to remotely control (change stages) using the ATCS interface from the control room.
7. The application shall have a Graphical User Interface (GUI) with an underlying GIS map that shall display the road network and the traffic signals, traffic cameras/detectors, Variable Message Sign (VMS) boards and Public Address (PA) systems deployed.
8. The GUI shall provide:
 - i. Flexibility to the operators to zoom and navigate with ability to interact with objects on the map.
 - ii. Interoperability across multiple platforms.
 - iii. Web browser based access, requiring no local setup on the

- iv. Graphically present signal plan execution and traffic flow at the intersection on a desktop
9. The GUI shall have the following features:
 - 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 different reports available under ATCS.
 - vi. Time-Space Diagram – The time-space diagram shall display the current stages being executed at every intersection in a corridor with immediate previous history. Junctions shall be plotted proportional to their distance on Y-axis and time elapsed for the stage in seconds on X-axis.
10. ATCS application shall graphically show the execution of the signal plans, in near-real-time.

The solution should include the following reports at a minimum:

Sr. No.	Reports	Sr. No.	Reports
1	Stage Timing report	6	Plan Change Report
2	Cycle Timing report	7	Mode Change Report
3	Mode switching report	8	Lamp Status Report
4	Power on & down	9	Loop Failure Report
5	Corridor Performance Report	10	Corridor Cycle Time Report

2.6. Technical Specification

Adaptive Traffic Management Software

Adaptive Traffic Management Software (ATMS) would be chosen which implements SCOOT (Split Cycle & Offset Optimization Techniques), CoSiCoSt (Composite Signal Control Strategy) or any other dynamic signal timing plan selection or adaptive system that uses near-real-time detector data. ATC must be chosen to provide accuracy as required for successful functioning of ATMS as per SLAs defined. ATMS software should have a centralized user interface accessible from control room and it should support remote /manual operation of traffic signals from control room. In addition, ATMS software should support selective vehicle (fire engines, ambulances and VIP vehicles) priority at traffic signals using GPS data.

The controller should provide at least one Ethernet interface as per requirement to communicate with ATCS server over TCP/IP.

The controller should provide at least 8 open-collector interfaces for interfacing with traffic detectors.

The ATCS application shall provide selective vehicle priority and compensation to avoid queue build-ups at the other approaches.

The ATCS system shall also be provided with a mobile application to provide congestion and network state information to the citizens using data from the ATCS system.

Adaptive Traffic Control- Traffic Light Aspects

Key Features:

- 1) Low power consumption for all colours
- 2) Meets or exceeds intensity, colour and uniformity specifications
- 3) Temperature compensated power supplies
- 4) Uniform appearance light diffusing
- 5) ITE products shall be Intertek/ETL/EN/Equivalent certified
- 6) All units operate on AC or DC as the per the suggested solution by MSI

LED aspects:

- 1) Red, Amber, Green-Full (300 mm diameter): Hi Flux
- 2) Red, Amber, Green-arrow (300 mm diameter): Hi flux
- 3) Red, Green-Pedestrian (300 mm diameter): Hi Flux with mask or Hi-Brite with discrete LEDs with suitable mask/stencil

Smart Traffic (Detectors & Sensors and Controllers)				
Sr. No.	Category	Minimum Requirement Description Compliance	Compliance (Yes/No)	Deviations/Remarks
INTEGRATED PRESENCE DETECTION AND DATA COLLECTION SENSOR – VIDEO BASED				
01	Camera Type	Sensor Size: 1/4” Frame Rate: 25 FPS Black & White Camera		
02	Lens Type	Wide Angle: Focal Distance 2,1mm Narrow Angle: Focal Distance 6,0mm Should support motorized zoom via configuration tool		
03	Electrical Specifications	Open collector (dry contact) interface Average Power Consumption ≤ 10W Operating Voltage - 12 to 26 V AC or DC Average Current Consumption 140mA @ 24VDC Electromagnetic Compatibility: 2004/108/EG FCC: FCC Part 15 class A		

		Shock & Vibration NEMA II specs		
04	Housing & Temperature Rating	Protection Grades: Housing - IP65 or above, Connectors - IP65 or above Temperature Range: from 0°C to +60°C		
05	Sensor Firmware & Software	Shall provide presence detection for up to 4 zones Shall provide both non-directional and directional detection in up to 4 directions, user-configured for each zone. Shall be capable of being upgraded via the PC software.		
06	Single Sensor Controller Interface Module (CIM)	Shall be DIN rail mountable can easily be fitted in Traffic controller. Shall have LED detection output indicators. Shall provide optical isolation. Shall have a port for PC connection.		
INTEGRATED PRESENCE DETECTION SENSOR – MICROWAVE RADAR BASED				
01	General	24GHz Doppler vehicle radar detector Open collector (dry contact) interface		
02	Technical	<ul style="list-style-type: none"> • Technology: CW Doppler Radar • Range/Zone Up to 150m (user selectable) • IP65 • Operating Temp 0°C to +60°C • Power 0.8W - 1.0W @ 24Vac • Approved to: ETSI EN 301 489 BS EN 50293 ETSI EN 300 440 BS EN 60950 		

Area Based Traffic Management System				
Sr. No.	Category	Minimum Requirement Description Compliance	Compliance (Yes/No)	Deviations/Remarks
ATMS.001	General Requirement	Monitor and control traffic signals, including signalled pedestrian crossings, using a traffic responsive strategy based on real time traffic flow and vehicle presence information. However, the system shall also be capable of operating under fixed time plan.		
ATMS.002	General Requirement	All junctions under Adaptive Traffic Control System shall be provided with vehicle detection system & communication equipment. Allow each intersection controller to be monitored from city operation system for proper functionality. Any corrective action can be initiated either automatically based on status information or by an operator. The real time detection data shall be communicated to the city operation centre by each controller.		

ATMS.003	General Requirement	ATCS shall be driven central control system 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 which in turn can also work in configurable manner. These calculations shall be based upon assessments carried out by the ATCS central application software running on a City Operation Centre based on the data and information gathered by vehicle detectors at strategic locations at the intersections controlled by the system		
ATMS.004	General Requirement	Signal Synchronization - manage network of signals to synchronize timing cycle to ensure probability of maximum greens to the vehicle moving in a particular direction.		
ATMS.005	General Requirement	<p>Pedestrian Priority</p> <ul style="list-style-type: none"> ▪ The controller site-specific data shall provide independent control for each of the pedestrian movements. It is also possible for a pedestrian phase to be configured to appear alone, in conjunction with other pedestrian phases, with non-conflicting vehicle phases, or in conjunction with a combination of pedestrian and non-conflicting vehicle phases. ▪ Allow pedestrian movements to be introduced automatically or by demand, whichever is required. Vehicle movements configured to run in parallel with a pedestrian phase shall continue to hold right of way until the end of the pedestrian clearance interval. ▪ Shall allow the pedestrian green and/or flashing red intervals to overlap between one or more stages with non-conflicting phases if so required. 		
ATMS.006	General Requirement	Emergency Vehicle Priority Provision to make way for emergency vehicle priority like fire, police and ambulance in some exceptionally important situations. The priority could be assigned by the central system and could be activated using an incident response system.		
ATMS.007	General Requirement	Should be able to integrate with Integrated Operation Platform for complete dashboard view		

3. COMPONENT 2 and 3 : Intelligent Traffic and CCTV Surveillance System

3.1. Overview

Protecting citizens and ensuring public safety is one of the topmost priorities for any Government. It requires advanced security solutions to effectively fight threats from activities of terrorism, organized crime, vandalism, burglary, acts of violence, and all other forms of crime. CCTV based video surveillance is a security enabler to ensure public safety. Under smart city initiative, ASCL intends to implement a holistic City Surveillance System in Agra including traffic enforcement system.

3.2. Project Intent

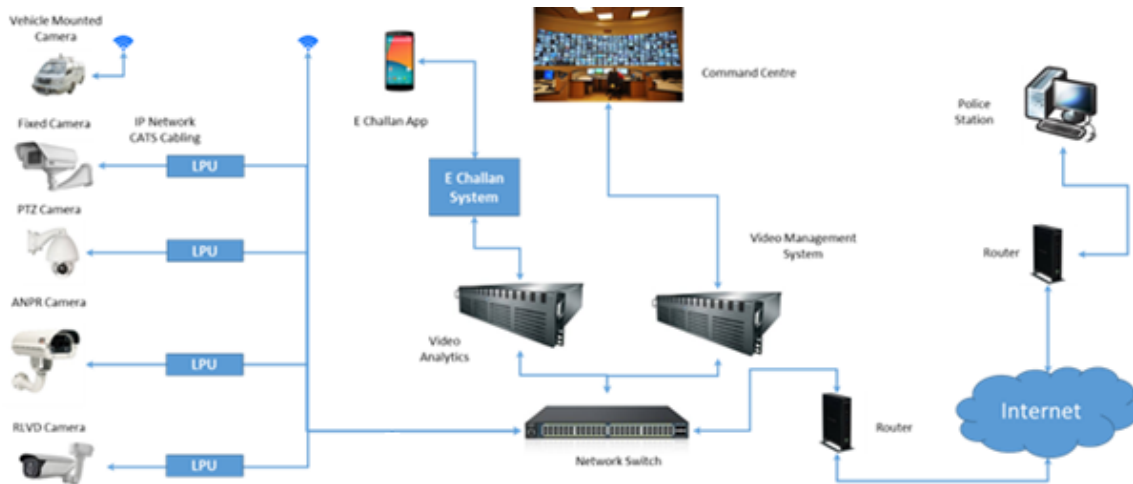
The city-wide surveillance CCTV cameras installed in the field across Agra city will help in monitoring and managing crime and enforce traffic. The CCTV cameras will include ANPR, RLVD, No Helmet Detection, PTZ, Fixed, FRS etc.

To implement holistic and integrated video surveillance system in Agra. The major stakeholders of CCTV surveillance system will Agra Traffic and Agra City Police Department. The system will help:

- 1) Support police to maintain Law and Order
- 2) Act as an aid to investigation
- 3) Improve Traffic Management
- 4) Help in deterring, detecting and thus dealing with criminal activities
- 5) Address threats from Terrorist attacks
- 6) Attain faster turnaround time for crime resolution and proper investigation
- 7) Monitoring of suspicious people, vehicles, objects etc. with respect to protecting life and property and maintaining law and order in the city
- 8) Continuous monitoring of some vital installations/ public places in Agra area for keeping eye on regular activities & for disaster management support
- 9) CCTV video surveillance system will enable the above by following:
 - i. Providing alerts/ feedback to the Police Department about abnormal movements/ suspicious objects etc.
 - ii. Better Management of Security breaches based on alerts received from system
 - iii. Improved turnaround time in responding to any investigation case, faster access to evidence in case of security breach, law violation in the prescribed areas.

3.3. System Architecture

The below figure is just indicative of how system architecture may look. This shall differ with the solution proposed when MSI bid having latest technology.



3.4. Solution requirements

MSI shall be responsible for Supply, Installation, Implementation and Operation & Maintenance of Agra CCTV based Surveillance System for a period of five (5) years from the date of Go Live. The standards should (a) at least comply with published eGovernance standards, frameworks, policies and guidelines available on <http://egovstandards.gov.in> (updated from time-to-time); and (b) be of leading industry standards.

3.5. Public Address system

Public Address system shall be used at intersections, public places, market places or those critical locations as identified by Purchaser to make important announcements for the public.

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. The system shall also deliver pre-recorded messages to the loud speakers attached to them from CD/DVD Players & Pen drives for public announcements.

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).

The MSI shall describe in detail the design, operational and physical requirements of the proposed public announcement system to demonstrate compliance with all the specified requirements of RFP.

3.6. Variable Message Signboards

Variable Message Signboard (VaMS) shall be installed at identified strategic locations. The VaMS shall communicate information & guidance about traffic, diversions, etc. to the citizens / public on the road. They shall also be used for showing emergency/ disaster related messages as and when required. The MSI shall describe in detail the design, operational and physical requirements of the proposed Variable Message Signboards to demonstrate compliance with all the specified requirements in this RFP.

The VaMS unit shall be able to communicate with the Command Control Centre system using GSM Data/SMS Channel. GSM data channel (GPRS) / Ethernet shall be used to send online messages and SMS channel shall be used to send configuration packets to configure the SIM.

Ethernet port shall also be extended to ground level using necessary cables for local troubleshooting. Each unit shall be provided with a unique identification number and shall communicate with the Command Control Centre system.

VaMS shall be managed and operated from the Command Control Centre / City Operations Centre, handled by a server where information in the form of data messages shall be fed in a manner to be displayed on a specific VaMS installed at a particular location or across all locations. The VaMS boards shall be viewable from a distance of 100 m and various angles on the road.

For installing VaMS Signboards, the MSI shall provide Gantry with spans, as required at various locations (single lane road, double lane road). Spans need to be specified depending on the number of lanes that need to be bridged. MSI shall consider additional space for lateral clearance as well as a vertical clearance height as per NHAI (National Highway Authority of India) guidelines.

3.7. Emergency Call Box System or Panic Box

- 1) A high quality digital transceiver, to be placed at certain key locations determined by Agra Police Department
- 2) Key is to make it easily accessible by public
- 3) The unit shall preferably have a single button which when pressed, shall connect to the Integrated Command and Control Centre over the existing network infrastructure setup for CCTV Surveillance system.
- 4) At some locations, this can be also used for Public Address
- 5) These shall be installed at select locations such as Traffic Junctions, Smart Bus Stops, and pedestals or within the vicinity of constant supervision to avoid misuse and vandalism of the call box.

3.8. On site Local Processing Unit with Communication & Electrical Interface

- 1) System should automatically reset in the event of a program hang up and restart on a button press. The system should start automatically after power failure.
- 2) System should have secure access mechanism for validation of authorised personnel.
- 3) Deletion or addition and transfer of data should only be permitted to authorised users.
- 4) A log of all user activities should be maintained in the system.
- 5) Roles and Rights of users should be defined in the system as per the requirements of the client
- 6) All formats of the stored data with respect to the infractions should be Non Proprietary.
- 7) Communication between the on-site outstation processing unit housed in the junction box and the detection systems mounted on the cantilever shall be through appropriate secured technology.
- 8) System should have the capability to transfer the data to CCC through proper encryption in real time and batch mode for verification of the infraction and processing of challan. Call forwarding architecture shall be followed to avoid any data loss during transfer.
- 9) In the event that the connectivity to CCC 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. There shall also be a facility 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.

3.9. Automatic Number Plate Recognition

MSI shall provide Automatic Number Plate Recognition (ANPR) solution at the identified locations. MSI shall describe in detail, the design, operational and physical requirements of the proposed ANPR system, to demonstrate compliance with all the specified requirements in this RFP.

ANPR cameras shall provide the feed to the command control Centre, where the ANPR server shall be located. The ANPR server shall process the image using OCR software for getting the registration number of the vehicle with highest possible accuracy. The system shall be able to detect, normalize and localize the image of the number plate for detection of alpha numerical characters. System shall be able to identify stolen/ suspected vehicles by cross checking the numbers with vehicle database like Vahaan. ANPR software shall be integrated with video management system.

ANPR system shall provide a user interface with live view of vehicle entry point 24x7, event notification, image captured, number detection and recognition, event reports customized report generation etc.

The analysis of image captured shall be done in real time. Database so created from the images captured & analysis shall store the following:

- 1) Details of vehicle
- 2) Number and time of entries and exits
- 3) License plate numbers
- 4) Validation/Analysis results etc.

3.10. Red Light Violation Detection (RLVD) system

Red Light Violation Detection (RLVD) system is a system for capturing details of vehicles that have crossed the stop line at the junction while the traffic light is red. System shall be able to automatically detect red light through evidence camera units and other equipment. The information so captured shall be used to issue challans to the violators.

MSI shall describe in detail, the design, operational and physical requirements of the proposed Red Light Violation Detection system, to demonstrate compliance with all the specified requirements mentioned in this RFP.

RLVD solution shall have an overview camera to capture the zoomed out picture of the entire area when there is a red light violation. Light sensors shall be placed to detect the change in traffic light. Once the traffic light has turned red, the sensors shall activate the camera to capture images of the vehicles that jumped the traffic light.

RLVD system, in case of an offence detected, shall capture details such as site name, location details, lane number, date & time, registration number of car and type of offence on the image itself. The system shall also be able to generate number of reports for analysis such as the traffic light with maximum offenders, peak time of traffic offence and other reports in discussion and as per the customization requirement of the ASCL.

3.11. E Challan System

The objective of E Challan application is as follows:

- 1) Issuing challan for traffic violations to a traffic violation defenders
- 2) Maintaining details pertaining to all activities of Traffic circles/violations/violators.
- 3) Providing requisite structured/unstructured information to traffic management officials as and when required.
- 4) Generating various statutory reports for administrative use and functioning of Traffic unit in matters of prosecution of violators and monitoring functioning of field officers.
- 5) Integrating and networking the system with state-of-the-art hardware and application software for Traffic Police to access and use information in their day-to-day work.
- 6) E-Challan System should allow for spot payment of fines using Hand-Held Terminal

3.11.1. Functional Requirements of E Challan System

- 1) E-challan software shall work in client-server mode, where the handheld (HH) devices units, workstation units will act as clients connected to the server through cellular network for data transfer.
- 2) E-challan system shall be able to retrieve vehicle owner details and vehicle data from RTO data base to minimise data entry
- 3) E-challan system shall be able to retrieve vehicle registration details and driving license details by reading appropriate smart card to minimize data entry
- 4) Server should maintain log of all current devices. Any access to the system must be recorded along with date, time, user ID and IP address
- 5) Traffic officer should log in to the handheld device through the unique user ID and password or smart card issued for the purpose
- 6) A unique challan number should be generated through client software for each challan
- 7) As soon as a vehicle registration number is entered, the Handheld device should automatically check from the server if the vehicle is stolen, wanted in any criminal case or is in the list of suspicious vehicles.
- 8) The most frequent traffic offences should be kept at the top in the drop down menu and offence ingredients should be available if required by an officer.
- 9) Date, time and GPS coordinates of place of challan should be automatically populated in the relevant fields of client software
- 10) Compounding amount must populate in the field automatically from master table
- 11) MSI should develop GUI and functionality as per requirements of Traffic Police
- 12) GUI should be Multi lingual i.e. English and Hindi
- 13) It should be possible to integrate as an enhancement when required for payment gate way operator with the system for facilitation of payment

- 14) Application Software should work in a web based environment.
- 15) Application software should be user friendly, easy to operate
- 16) Software must provide comprehensive data back-up and restoration capability.
- 17) System will function in web-based system where the hand-held device shall work as a node.
- 18) Application software should maintain logs of user activities to facilitate audit trail.
- 19) System should have sufficient security features such as firewall, access control system, biometrics, password protection, audit trail, anti-virus etc.
- 20) Database server should be able to handle the activities of all the handheld devices at one time simultaneously with huge database size of prosecution, ownerships, driving license, etc. without affecting the performance.
- 21) Software should be able to generate various periodical reports, summaries, MIS reports, query reply, etc. as per the requirements of Traffic Police.
- 22) Administrator should be able to modify the master tables as and when required and should have the capability to push the changes to hand-held devices.
- 23) All database tables, records etc. required for various dropdown menus etc. shall also be created by the vendor.
- 24) Application software is to be provided by the vendor to handle various processes of the prosecution required by the office of senior police officers, courts, etc.
- 25) MSI to ensure that e-Challan System is able to integrate through available APIs with third party applications which are available by Government of UP and follow guidelines of MORTH (Ministry of Road Transport and Highway)

3.11.2. Hand Held Devices

- 1) Once the application is loaded on the hand-held device there should be no possibility to modify the application by the user. Reloading and modifying of application should be possible only by an administrator.
- 2) On switching on the hand-held device, the system must give access only after validation through user ID and password.
- 3) The communication between the server and hand-held device would be through GSM/GPRS/ 3G or better connectivity etc.
- 4) Every challan created must have a unique self-populated number.
- 5) HH application must be able to access information from the main Server and display upon request, pop- up tables/codes, vehicle and license details, all types of offences, compounding amount, challan types, vehicle details, court calendar etc. to minimize the typing by the prosecuting officer.
- 6) HH device should be able to access data/ information on the basis of driving license number, vehicle registration number etc. from the main server data relating to previous offences.
- 7) HH application software should also suggest date of challan, place of challan, name of the court and court date, etc. to further reduce typing by the officer. These fields should be designed in consultation with Traffic Police.
- 8) When a challan is issued, the name and ID of the officer should be printed on the challan.

- 9) HH device must be able to input and print multiple offences on the same challan.
- 10) HH software must validate challan fields automatically before the challan is printed. The system must ensure that certain fields are properly completed before allowing the challan to be printed.
- 11) When downloading application software or pop-up tables or lists to the HH, or uploading challan records to the Server, synchronization of HH system must be automatic, to minimize human intervention.
- 12) Uploading data to the Database Server should be automatic in consistent manner.
- 13) Application should provide features wherein when a driving license/ vehicle registration number is entered, it should be able to pull from the server all the details relating to the driving license holder/ vehicle owner including history of previous offences.
- 14) Software should capture the list of documents seized during prosecution and such list must be reflected on the printed court challan.
- 15) HH application software shall allow the user to generate a summary report to facilitate evaluation of his daily work.
- 16) Once the challan is complete and saved any further editing should not be possible unless so authorized by administrator.
- 17) Each hand-held device should be provided with original printed user manual and appropriate carry case for HH device with charger.
- 18) Application software should allow online payment and direct payment at HH device
- 19) There should be automatic rejection of payment for the settlement of expired notices or challans. Partial payment of an offence must not be accepted by the system.
- 20) Software should update Driving License/Vehicle Registration smart card of the violator with the booked offence.
- 21) Mobile Swiping of Credit and Debit Cards should be possible, and violator can enter the PIN number on the HH device keypad securely.

3.12. Face Recognition System

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.

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 FRS algorithm/engine should have appeared in top 10 listing of latest NIST benchmark test.

The system shall be able to:

- 1) Capture face images from CCTV feed and generate alerts if a blacklist match is found.
- 2) Search photographs from the database matching suspect/people features.
- 3) 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.

- 4) Add photographs obtained from newspapers, raids, sent by people, sketches etc. to the criminal's repository tagged for sex, age etc. for future searches.
- 5) Investigate to check the identity of individuals upon receiving such requests from Police Stations.
- 6) Enable Handheld mobile with app to capture a face on the field and get the matching result from the backend server.

The facial recognition system shall be enabled at cameras identified by the purchaser.

The facial recognition system in offline mode shall be provided by the SI in line with the requirement specified in the RFP.

Functional requirement –

- 1) 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 or the video management system.
- 2) The facial recognition system should be able to work on the server/ desktop OS as recommended by OEM and provided by the System Integrator.
- 3) The user interface of the facial recognition system should have a report management tool 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.
- 4) 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.
- 5) The system should have ability to handle initial real-time watch list of 10,000 Faces (should be scalable to at least 1 Million faces) and 50 Camera Feeds simultaneously and generate face matching alerts.
- 6) The algorithm for facial recognition or the forensic tool should be able to recognize partial faces with varying angles.
- 7) The system should be able to detect multiple faces from live single video feed
- 8) The system should have combination of eye-zone extraction and facial recognition
- 9) The system should have short processing time and high recognition rate
- 10) The system should be able to recognize faces regardless of vantage point and any facial accessories/ hair (glasses, beard, expressions)
- 11) 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 of GPU technology instead of Traditional CPUs, to greatly improve the computational performance in crowded environments.
- 12) The system should be able to identify and authenticate based on individual facial features

- 13) The system should be compatible with the video management system being proposed by the system integrator
- 14) The system should have capability for 1:1 verification and 1:N identification matching
- 15) The system should be able to integrate with other systems in the future such as 'Automatic fingerprint identification system (AFIS)' etc.
- 16) The system should be able to support diverse industry standard graphic and video formats as well as live cameras
- 17) The system should be able to match faces from recorded media.
- 18) The system should be able to detect a face from a group photo
- 19) The system should be able to detect a face from stored videos of any format
- 20) The system should have bulk process of adding faces in the system
- 21) The system should be an independent system, with capability to integrate with industry standard Video Management Systems (VMS) for alert viewing.
- 22) 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
- 23) 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
- 24) The system should have the facility to categorize the images like "Remember this person" or "hit-list" or "wanted".
- 25) The OEM should have support facility in India

3.13. No Helmet Detection System

- 1) System shall have capability to capture image of two-wheeler rider not wearing helmet and shall have automatic number plate recognition (ANPR) of violating vehicle with auto-localization and OCR conversion.
- 2) On detection of No-Helmet system shall generate events, store them and shall allow retrieval of such events on need basis for later analysis
- 3) System shall have capability to identify and eliminate riders covering their face using scarf and mark them as invalid.
- 4) System shall integrate with challan generation software and RTO database to generate challans for No-Helmet violation event with details like violation image, time stamp, date, vehicle number.
- 5) No- Helmet detection system shall seamlessly integrate with traffic management systems like ANPR, RLVD, Speed Detection and shall have unified user interface.
- 6) System shall make available event reports such as number of detections per day, list of repeat offenders, etc. for further analysis by traffic department.
- 7) Proposed system shall support single server architecture or distributed network architecture with possibility of cloud based deployment in future.
- 8) System shall have dedicated camera units for no-helmet detection in field of view of that camera unit to be installed at identified locations within city limits. Such cameras shall be independent of existing city surveillance and traffic violation detection cameras.

- 9) System shall use high computing unit to analyze huge amount of visual data from multiple cameras efficiently and accurately for automatic detection of riders without helmet.

3.14. Operating Conditions

- 1) **Reliability:** Proposed equipment must be designed to cater for 24x7 round-the-clock operations.
- 2) **Maintainability:** MSI shall maintain the uptime for entire system as mentioned in SLA. This uptime is exclusive of regular maintenance. The minimum down-time for all the components, factors such as ease of replacement, mean-time-to-repair (MTTR) shall be incorporated in the system design.
- 3) **User-friendly:** System server should be based Linux or Unix OS. At the same time, administrative and dispatch console should be world-wide-web based, the multi-channel PTT SW client should operate on Windows XP/Vista/7/8/10 operating system. Server system can be based on windows/Linux/Unix OS.
- 4) **Security:** System should be fully secured so that system can't be hacked or compromised by anybody in any circumstances.
- 5) **Upgradeability:** each part of the system produced should be modular and easily re-configurable and upgradeable. System should be based on an open system concept.
- 6) **Electromagnetic compatibility:** IP interoperability and collaboration System shall be able to operate without any complication due to any electromagnetic interference exists in or between sub-systems. At expiry of contract, for smooth handing over/transfer of the system, all system with detailed diagrams and drawings (software, hardware, connectivity, control room, field equipment, components and subcomponents, etc. used in the project) shall be fully functional.
- 7) **Scalability:** Network and bandwidth capacity should be expandable. Hardware, software for control room shall be expandable.

3.15. Mobile Enforcement Solution for Police

Public security and law enforcement personnel have to be in the right place, at the right time, every time. Your communication devices have to be completely mobile, as well as rugged and reliable. Permanently installed surveillance systems are great, but it can be limited in scope. In the real world, surveillance systems need to be completely mobile, too. When you need surveillance equipment and support to go where you go.

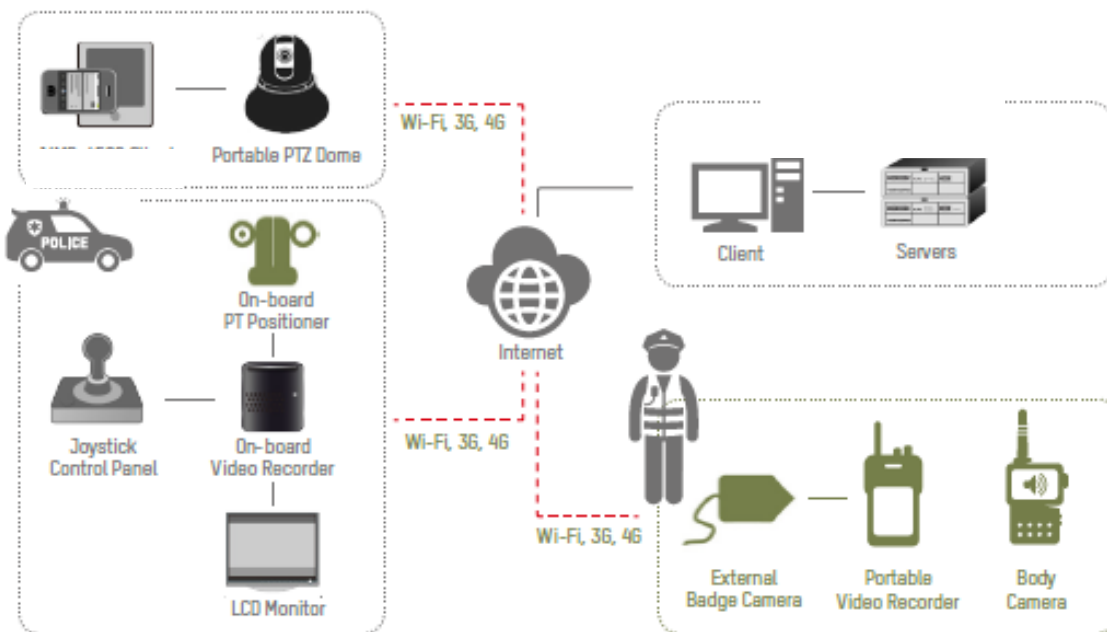
3.15.1. Police Vehicles

Packed with gear for emergency response vehicles, temporary security installations, wearable tech, and more, Smart Mobile Enforcement arms you for every situation. Keep personnel accountable, track events for forensics, and safely secure data for Smart analysis.

Extreme weather can cause major traffic disasters. Peaceful public demonstrations can turn into unlawful events. Earthquakes, floods, and lightning storms can interrupt power and water supplies. The unpredictability of these incidents requires civic authority personnel to be mobile, nimble, and always ready to go. And the equipment has to be just as mobile, too. Turn enforcement vehicles into

temporary mobile monitoring stations and move your gear to where it’s most needed with our on-board systems.

In Uttar Pradesh, there is an existing robust infrastructure for UP Dial 100 meant ‘to take prompt action in a fixed minimum time limit by sharing the information received through phone calls with the concerned police station/police post of concerned district and other officers.’ The intent of the project is to use the existing infrastructure of UP Dial 100, and make technology up gradations for the 48 vehicles in the city of Agra which shall even have supporting peripherals of Smart Phones, Tablets which complement the e-Challan System along with Breath-Analyzer to detect the defaulters for enforcing stringent actions.



3.15.2. Temporary Monitoring

When permanent surveillance installations are not possible, mobile enforcement solutions have to fill in the gap. On the roads, at the public squares, in rural areas – wherever you need surveillance equipment to go. Tripod-mounted dome cameras, for example, reliably capture everything in view.

3.15.3. Wearable Monitoring

Rugged, wearable body cameras record activities of citizens and civil authorities as they happen. Their advanced technology, portability, and ease-of-use make them extremely effective companions for law enforcement. Equipped with GPS locators, you’ll know where the emergency exists as it happens. These cameras build forensic evidence with safely stored data, and play back video footage clearly and accurately. Protect people and peacekeepers with wearable video recording devices.



3.15.4. Modern Infra and Peripherals

Considering the need of immediate response system for Police to detect and identify the event, with the upcoming technology advancement, it requires a basic infra in terms of OFC to have all the major Police Stations and Chowkis connected in a mesh for faster resolution of event. This should be accompany with basic peripherals like Smart Phones, Tablets, High End Computers and Screens for local monitoring the visuals.

3.16. CCTV Surveillance Cameras - Functional Specification

3.16.1. Surveillance System Infrastructure at Field Locations

This Component covers planning & implementation of the Surveillance system comprising cameras and other field equipment at identified locations. Actual placement of pole & number of cameras at each location, type of cameras, fixation of height & angle for the cameras to ensure maximum coverage shall be done in consultation with Agra Police Department.

Category	Scope of Work
Surveillance System Infrastructure at field locations	Supply, install, implement and maintain: <ul style="list-style-type: none"> Full HD IP Pan-tilt-zoom camera (PTZ) Camera Full HD IP Fixed Box Camera for ANPR/ RLVD Face Recognition Camera Pole, Junction box, LPU, UPS, LAN switch, passive items, etc.
	Other Components: <ul style="list-style-type: none"> Public Address System Variable Messaging System Panic/Emergency Button
Surveillance System Application	<ul style="list-style-type: none"> Video Management System (VMS) Video Analytics (VA) Red Light Violation Detection (RLVD) System Automatic Number Plate Recognition (ANPR) System No Helmet Detection Wrong Lane Intrusion Detection E Challan System with Payment integration

A detailed survey shall be conducted, by the MSI along with a team of ASCL and Agra police, at each of the strategic locations. This survey shall finalize the position of all field equipment and the orientation/ field of view of the cameras. Appropriate field of view snapshot shall be taken by a handheld camera for future reference at the time of survey. The surveyors shall also finalize the approximate location of foundation for junction box and camera poles.

The route for all the underground cable laying shall be finalized during this survey (wherever required). Every detail, finalized during the survey, shall be demarcated on an AutoCAD drawing by the SI and submitted to Purchaser in the form of a detailed site survey report along with other details for its approval.

System shall provide inter-operability of hardware, operating system, software, networking, printing, database connectivity, reporting, and communication protocols. SI shall prepare the detailed report for field level requirements e.g. Cameras (types & numbers), Camera Mounting requirements, Power Requirements, Connectivity Requirements etc. for perusal of Purchaser. Indicative list of the field level hardware to be provided by SI is as follows:

- Cameras (Fixed Box Cameras, PTZ Cameras, ANPR cameras etc.)
- IR Illuminators
- Local processing unit for ANPR / RLVD cameras
- Switches
- Outdoor Cabinets
- Pole for cameras / Mast
- Junction box
- UPS

3.16.2. Networking and power cables and other related infrastructure

The indicative list of locations for the camera installation is mentioned in Annexure in the RFP document along with minimum technical requirements of associated hardware to implement a complete Surveillance system.

3.16.3. Supply & Installation of CCTV Surveillance Infrastructure

Based on detailed field survey as mentioned above, MSI shall be required to supply, install and commission the surveillance system at the identified locations and thereafter undertake necessary work towards its testing.

MSI shall use industry leading practices during the implementation phase w.r.t positioning and mounting the cameras, poles and junction boxes. Some of the check-points that need to be adhered to by the MSI while installing / commissioning cameras are as follows:

- 1) Ensure surveillance objective is met while positioning the camera such that the required field of view is being captured as finalized in field survey
- 2) Ensure camera is protected from the on-field challenges of weather, physical damage and theft.
- 3) Make proper adjustments to have the best possible image / video captured.
- 4) Ensure that the pole is well placed for vibration resistance adhering to the road safety norms.
- 5) Collusion preventive barriers around the junction box & pole foundation in case it's installed in collision prone place.

- 6) Appropriate branding or colour coding (Police/Purchaser Branding) of poles and junction boxes, to warn mischief mongers against tampering with the equipment at the junction.

3.16.4. Installation of Poles/Cantilevers/Gantry

- 1) MSI shall ensure that all installations are done as per satisfaction of Purchaser.
- 2) For installation of variable message system (VaMS), CCTV Cameras, PTZ Cameras, public address system, etc. MSI shall provide appropriate poles & cantilevers and any supporting equipment.
- 3) MSI shall be required to supply, install, configure and integrate surveillance cameras at the identified locations and thereafter undertake necessary work towards their commissioning.
- 4) MSI shall ensure that the poles erected to mount cameras are good, both qualitatively and aesthetically
- 5) MSI shall use the industry leading practices while positioning and mounting the cameras and ensure that the pole / mast implementation is vibration resistant. Arrangements for bird scare spikes on top of camera shall be made to prevent birds from sitting on top of camera box.
- 6) The poles shall be installed with base plate, pole door, pole distributor block and cover.
- 7) Base frames and screws shall be delivered along with poles and installed by the MSI.
- 8) In case the cameras need to be installed beside or above the signal heads, suitable stainless steel extensions for poles need to be provided and installed by the MSI so that there is clear line of sight.
- 9) MSI shall be responsible to undertake required structural analysis regarding the regulated load conditions and considering the respective wind load while installing the poles / cantilevers for Variable Messaging Sign boards
- 10) MSI shall provide structural calculations and drawings for the approval of Purchaser. The design shall match with common design standards as applicable under the jurisdiction of purchaser/authorized entity.
- 11) MSI shall coordinate with concerned authorities / municipalities for installation.
- 12) Poles and cabinet shall be so designed that all elements of the field equipment could be easily installed and removed.
- 13) MSI shall ensure that physical look of the installation area returns to neat & tidy conditions after installation of poles, cantilevers etc. The placement shall be designed keeping in mind the normal flow of vehicular traffic and pedestrian movement is not disturbed.

3.16.5. UPS for field locations

- 1) UPS shall serve as a backup for commercially available utility power at the intersections and shall ensure no-break functioning of all field components at each intersection in event of failure of utility power supply.
- 2) MSI shall carry out a study and identify locations to provide UPS backup, depending upon power situation across city, to meet the camera uptime requirements.
- 3) MSI shall install UPS at the identified intersections in secure, tamper-proof housing in corrosion resistant cabinets.
- 4) MSI shall ensure that the UPS is suitably protected against storms, power surges and lightning.

- 5) MSI shall provide UPS for efficient heat dissipation without air conditioning. It shall be able to withstand temperatures prevalent in Nagpur throughout the year.

3.16.6. Outdoor Cabinets / Junction Boxes

- 1) Each intersection shall be fitted with outdoor cabinets dimensioned to host all equipment necessary to operate enforcement systems and traffic surveillance systems as defined in this RFP.
- 2) MSI shall reserve additional room in the intersection controller cabinet to accommodate the future system requirements
- 3) The size of outdoor cabinet / Junction Boxes shall be sufficient to house all the system components, which may be installed at the intersection or nearby. Boxes shall be dustproof and impermeable to splash-water. They shall be suitable for Agra 's environmental conditions. They shall have separate lockable doors for:
 - a) Power cabinet: This cabinet shall house the electricity meter, online UPS system and the redundant power supply system
 - b) Control cabinet: This cabinet shall house the controllers for all the field components at that particular location e.g. ANPR, PTZ, RLVD, Fixed cameras etc.
- 4) Internal cabinet cabling shall be designed for an easy connection and disconnection of the equipment and power
- 5) The cabinets shall be of robust construction and shall include 3-point security-locking mechanisms to prevent unauthorized access to the field equipment
- 6) Temperature and Humidity Control: All enclosure compartments shall be equipped with a natural convection air circulation system via provision of air circulation filters that shall not require maintenance and shall allow free circulation of air inside the enclosures to prevent overheating as well as the build-up and effects of humidity and heat, without permitting the entry of elements that might endanger system operation.
- 7) MSI shall ensure that all the hardware is placed inside the junction boxes that could withstand temperatures prevalent in Agra City throughout the year.

3.16.7. Civil and Electrical Works

- 1) MSI shall be responsible for carrying out all the civil work required for setting up all the field components of the system including:
 - 2) Preparation of concrete foundation for MS-Poles & cantilevers
 - 3) Laying of GI Pipes (B Class) complete with GI fitting
 - 4) Hard soil deep digging and backfilling after cabling
 - 5) Soft soil deep digging and backfilling after cabling
 - 6) Chambers with metal cover at every junction box, pole and at road crossings
 - 7) Concrete foundation from the Ground for outdoor racks
- 8) MSI shall provide electricity to the cameras through the aggregation point. Since this component has dependency on approval from local authorities, it is recommended that SI plans this requirement well in advance & submits the application to the concerned electricity distribution agency with requisite fees, if applicable.

- 9) MSI shall carry out all the electrical work required for powering all the components of the system
- 10) Electrical installation and wiring shall conform to the electrical codes of India.
- 11) MSI shall make provisions for providing electricity to the cameras (ANPR, PTZ, and Fixed) via SJB (Surveillance Junction Box), housing the UPS/SMPS power supply, with minimum backup as defined in this RFP,
- 12) For the wired Box cameras, MSI shall provision for drawing power through PoE (Power over Ethernet), while PTZ cameras shall be powered through dedicated power cable laid separately along with STP/SFTP cable.
- 13) Registration of electrical connections at all field sites shall be done in the name of ASCL as agreed and finalized in the contract agreement.
- 14) MSI shall house the electricity meters inside the power cabinet as mentioned in the controller Cabinet section as above.

3.16.8. Earthing and Lightning Proof Measures

- 1) MSI shall comply with the technical specifications taking into account lightning-proof and anti-interference measures for system structure, equipment type selection, equipment earthing, power and signal cable laying. MSI shall describe the planned lightning-proof and anti-interference measures in their technical bid.
- 2) Corresponding lightning arrester shall be erected for the entrance cables of power line, video line, data transmission cables.
- 3) All interface board and function board, interfaces of equipment shall adopt high speed photoelectric isolation to reduce the damage to integrated circuit CMOS chip due to the surge suppression.
- 4) Install the earthing devices for the equipment, including lightning earthing, protection earthing and shielded earthing. All earthing shall meet the related industry standards.
- 5) The earthing cable shall be installed in a secure manner to prevent theft and shall be rust proof. Earthing down lead and the earthing electrode shall be galvanized

3.16.9. Miscellaneous

- 1) ASCL shall assist in obtaining all necessary go ahead, legal permissions, NOC (No Objection Certificate) from various departments to execute the project. MSI shall have to identify and obtain necessary legal / statutory clearances for erecting the poles and installing cameras, for provisioning of the required power, etc. MSI shall provide & manage all necessary paper work to pursue permission from respective authorities. No commercial/ legal fees shall be applicable to ASCL for obtaining the necessary permissions. These shall be provisioned for by MSI in their financial bid.
- 2) The MSI shall provide all material required for mounting of components such as cameras, VaMS and other field equipment. All mounting devices for installation of CCTV cameras to enable pan and tilt capabilities shall be included in the costs of the respective component. The same is also applicable to crossheads and cross arms, mounting brackets, stainless steel bands, screws and other accessories.
- 3) All the equipment, software and workmanship that form a part of the service are to be under warranty throughout the term of the service contract from the date of service acceptance and

commencement. The warranty shall require the SI to be responsible to bear all cost of parts, labour, field service, pick-up and delivery related to repairs, corrections during the Project Period or any and all such incidental expenses incurred during the warranty period.

- 4) MSI shall also get comprehensive insurance from reputed insurance company for the project duration for all the equipment / components installed under this project.
- 5) MSI shall ensure all the equipment's installed in the outdoor locations are vandal proof and in case the equipment get damaged /stolen for reasons whatsoever, it shall repair/replace the same in the specified time as per SLAs at no extra cost to the Purchaser. All such costs shall be factored in the comprehensive insurance of field equipment for the duration of the contract.
- 6) Preventive maintenance shall be carried out once in a quarter along with corrective maintenance and when calls are placed by ASCL or its designated agency.
- 7) MSI shall be responsible for operations and maintenance of all the supplied and installed equipment's during the entire O&M phase.
- 8) In addition to above, MSI shall be fully responsible for all maintenance activities for the period between installation of equipment and roll-out of the system.
- 9) During implementation, if observed that any camera / field equipment requires change in the field of view / orientation, it shall be done by SI without any extra cost.
- 10) In case of request for change in location of field equipment post installation, the same shall be borne by Purchaser at either a unit rate as per commercials or a mutually agreed cost.

3.16.10. Mounting structure

- 1) Should be cantilever mounted and shall have minimum 6 m height with appropriate vertical clearance under the system from the Road surface to ensure no obstruction to vehicular traffic.
- 2) Should be capable to withstand high wind speeds and for structural safety, the successful bidder has to provide structural safety certificate from qualified structural engineers approved/ certified by Govt. Agency.
- 3) Shall be painted with one coat of primer and two coats of PU paint. The equipment including poles, mountings should have an aesthetic feel keeping in mind the standards road Infrastructure (e.g. Poles, Navigation boards, etc.) currently installed at these locations. The equipment should look "one" with the surroundings of the location and not look out of place.
- 4) Rugged locking mechanism should be provided for onsite enclosures and cabinets.

3.17. Technical Functions

A. On site Local Processing Unit with communication & Electrical Interface (Junction Box)				
Sr. No.	Item	Minimum Requirement Description	Compliance (Yes / No)	Deviations / Remarks
LPU.00 1	Data Storage on site	System should be equipped with appropriate storage capacity for 24 x 7 recording, with overwriting capability. Images should be stored in tamper proof format only.		
LPU.00 1	Network Connectivity	Wired/GPRS based wireless technology with 3G upgradable to 4G capability.		

LPU.00 1	Communication port	Minimum 2(two) USB Port to support latest external mass storage devices and Ethernet (10/100) Port for possible networking. All logs of data transfer through the ports shall be maintained by the system.		
LPU.00 1	Operating range	ambient temperature range of -5°C to 60°C.		
LPU.00 1	Lightening arrester	shall be installed for safety of system (As per BIS standard IS 2309 of 1989).		
LPU.00 1	Housing	should be capable of withstanding vandalism, harsh weather conditions and should meet IP66, IK10 standards (certified).		
LPU.00 1	Violation Transmission and Security	Encrypted data, images and video pertaining to violations at the onsite processing unit should be transmitted to CCC electronically through wired or GPRS based wireless technology with 3G upgradable to 4G, in jpeg format.		
		Advanced Encryption Standard (AES) shall be followed for data encryption on site and CCC, and its access will be protected by a password.		
		Data from onsite local processing unit shall be transferred to CCC within one day.		
LPU.00 1	Video Recording	System should be capable of continuous video recording in base station for 7 days. System shall automatically overwrite data after 7 days. Any point of time, local storage at base station should have data of previous 7 days.		
		Direct extraction through any physical device like USB, Hard disk shall be possible		

B. Fixed Box Surveillance Camera (HD)				
Sr. No.	Item	Minimum Requirement Description	Compliance (Yes / No)	Deviations / Remarks
FBC.001	General Requirements	The camera should be manufacturer's official product line designed for commercial / industrial 24x365 use. The camera and camera firmware should be designed and developed by same OEM		
FBC.002	Image Sensor with WDR	1/3.2" with True WDR, Progressive CMOS Sensor or better		
FBC.003	Lens Specs	Compatible to image sensor, Focal length 8-50 mm or better, Full HD (1080P), Auto IRIS / P IRIS, Corrected IR, CS Mount with IR cut filter		
FBC.004	Resolution	Active Pixels 1920(w) x 1080(h)		
FBC.005	Minimum illumination	Colour: 0.3 lux or better, B/W: 0.05 lux or better		

FBC.006	Video Encoder	H.265 or H.264//Motion JPEG compression		
FBC.007	Frame Rate	min. 25 FPS or higher		
FBC.008	Local Storage	32 GB SD Card or higher		
FBC.009	Ethernet	10/100/ Base-T ports		
FBC.010	Image Compression	H.265 or H.264//Motion JPEG compression		
FBC.011	Protocols	Minimum of the following protocols to be supported RTSP, RTP/TCP, RTP/UDP, HTTP, HTTPS, DHCP		
FBC.012	Industry Standards	ONVIF Compliant		
FBC.013	Power Supply	POE IEE 802.3af compliant		
FBC.014	Operating Temperature	0° C to 50° C or better		
FBC.015	Operating Humidity	Humidity 10–100% RH (condensing)		
FBC.016	Enclosure	IP 66		
FBC.017	Certifications	UL, CE, FCC, ONVIF 2.x/S		

C. Fixed Box Surveillance Camera (HD)				
Sr. No.	Item	Minimum Requirement Description	Compliance (Yes / No)	Deviations / Remarks
FBC.018	Support	System should not be an end of life / end of service product.		
		Camera shall be able to setup and stream out minimum		
FBC.019	Streaming	two (2) stream profiles. Each stream profile should have its own compression, resolution, frame rate and quality independently.		
FBC.020	White Balance	Auto / Manual		
FBC.021	Back Light Compensation	Auto		
FBC.022	Security	Security Password protection		
FBC.023	Miscellaneous	Vandal and impact resistant housing, IK 10, IP66/ NEMA 4X		
FBC.024		Detection of camera tampering and Detection of Motion should be possible using either camera or VMS		

D. Surveillance Camera - PTZ (HD)				
Sr. No.	Item	Minimum Requirement Description	Compliance (Yes / No)	Deviations / Remarks

PTZ.001	General Requirements	Camera should be manufacturer's official product line designed for 24x365 use. Camera and camera firmware should be designed and developed by same OEM.		
PTZ.002	General Requirements	Camera should be based upon standard components and proven technology using open and published protocols		
PTZ.003	Image Sensor with WDR	1/3.2" with True WDR, Progressive CMOS Sensor or better		
PTZ.004	Resolution	Camera should be HD PTZ 1920 (w) x1080 (h)		
PTZ.005	lens specs	Compatible to image sensor, Focal length 30x, 4.3-129 or 4.7–141 mm or better, Auto Iris, Full HD (1080P), F/1.6, IR Corrected – Day / Night mode- Colour		
PTZ.006	Minimum illumination	Colour: 0.3 lux, B/W: 0.05 lux or better		
PTZ.007	Pre-set Positions	100 or better, Pre-set tour		
PTZ.008	Pan	360° endless, 300°/s		
PTZ.009	Tilt Range	Manual/programmable; speed: 300°/sec; angle :0-180° or proportional speed needs to be provided		
PTZ.010	Zoom	30x optical zoom and should support digital zoom feature		
PTZ.011	General	Camera shall be able to setup & stream out minimum two (2) stream profiles. Each stream profile shall have its own compression, resolution, frame rate and quality independently.		
PTZ.012	Outdoor Protection	Camera should be complete with IP 66 rated housing, Connectors, Camera Mounts, Power Supply and all Ancillary Equipment & all accessories.		
PTZ.013	Protocol	IPv4, TCP/IP, HTTPS, FTP, SMTP, SNMP, RTP, RTSP, DDNS, DHCP, DNS, NTP, UDP		
PTZ.014	Compression Capability	H.265 or H.264 /Motion JPEG compression @ 25fps		

E. Surveillance Camera - PTZ (HD)				
Sr. No.	Item	Minimum Requirement Description	Compliance (Yes / No)	Deviations / Remarks
PTZ.015	Certificate	FCC, CE, UL, ONVIF 2.x/S		
PTZ.016	Industry Standards	ONVIF Compliant		
PTZ.017	Miscellaneous	Compliance to Vandal and impact resistant housing – IP66 /		

	ous	NEMA 4X, IK10		
PTZ.018		Power Supply: External 12V /24V/48V DC/ POE		
PTZ.019		Connectors: 10Base-T/100Base-TX		
PTZ.020		Cable routing through base or rear of housing		
PTZ.021		Operating conditions unit: 0° C to 50° C or better, humidity Humidity 10–100% RH (condensing)		
PTZ.022		Tamper Proof		
PTZ.023		Detection of camera tampering and Detection of Motion should be possible using either camera or VMS		
PTZ.024	Support	The system should not be an end of life / end of service product.		
PTZ.025	Audio	Audio capture Capability		
PTZ.026	Local Storage	32GB or higher		
PTZ.027	Security	Password Protection		

F. IP Dome Camera				
Sr. No.	Item	Minimum Requirement Description	Compliance (Yes / No)	Deviations / Remarks
IPDC.001	Image Sensor with WDR	1/3.2" with True WDR, Progressive CMOS Sensor or better		
IPDC.002	Resolution	2 MP HD or higher		
IPDC.003	Minimum Illumination	0.3 lux in colour mode; 0.2 lux or better in B/W with IR		
IPDC.004	Lens	Min 3 to 10 mm fixed/vari-focal lens with Remote focus		
IPDC.005	Ethernet	10/100/ Base-T ports		
IPDC.006	Frame Rate	min 25fps or better		
IPDC.007	Image Compression	H.265 or H.264 /Motion JPEG compression		
IPDC.008	Protocols	Minimum of the following RTSP, RTP/TCP, RTP/UDP, HTTP, DHCP protocols to be supported		
IPDC.009	Operating Temperature	0°C to 50°C degrees or better		
IPDC.010	Power supply	POE IEE 802.3af compliant		
IPDC.011	Support	System should not be an end of life / end of service product.		
IPDC.012	Industry Standards	ONVIF Compliant		
IPDC.013	Certifications	UL, CE, FCC, ONVIF 2.X/S		
IPDC.014	Storage	32 GB or higher		
IPDC.015	White Balance	Auto / Manual		
IPDC.016	BLC	ON/OFF		

IPDC.017	Security	Password protection		
IPDC.018	Casing	IP 66 vandal resistant		
IPDC.019	Camera Tampering	Detection of camera tampering and Detection of Motion should be possible using camera. Functionality to be enabled vide VMS		
IPDC.020	Streaming	Camera shall be able to setup and stream out minimum two (2) stream profiles. Each stream profile shall have its own compression, resolution, frame rate and quality independently.		

G. Multi Sensor /Panoramic 360° Camera				
Sr. No.	Item	Minimum Requirement Description	Compliance (Yes / No)	Deviations / Remarks
MSC. 001	General Requirements	Camera should be manufacturer's official product line designed for commercial / industrial 24x365 use.		
MSC.002	General Requirements	Camera should be based upon standard components and proven technology using open and published protocols		
MSC.003	Image Sensor	Minimum 4 x 2MP, 1/3.2" CMOS - (Total) 8 MP or better		
MSC.004	Lens Specs	F2.0, IR Corrected; Options of 2.8/4/8/12/16 MM Lens		
MSC.005	Maximum Resolution	4 K Vision		
MSC.006	Minimum illumination	Colour: 0.6 lux or better, Monochrome: 0.05 Lux or better with IR		
MSC.007	Video Compression	H.265 and H.264/ Motion JPEG		
MSC.008	Frame Rate	15fps or better		
MSC.009	Wide Dynamic Range	100 dB or better		
MSC.010	Network Interface	100 Base-T ports		
MSC.011	Power Supply	POE IEE 802.3af compliant		
MSC.012	Industry Standards	ONVIF Compliant		
MSC.013	Certifications	UL, FCC		
MSC.014	Enclosure Type	IP66; IK 10 or NEMA 4X		
MSC.015	Operating Temperature	0° C to 50° C or better		
MSC.016	Operating Humidity	Humidity 10–100% RH (condensing)		
MSC.017	Supported Network	Minimum of the following RTSP, RTP/TCP, RTP/UDP, HTTP, DHCP protocols to be supported		

	protocols			
MSC.018	Support	System should not be an end of life / end of service product.		

H. IR Illuminator - Field Location				
Sr. No.	Item	Minimum Requirement Description	Compliance (Yes / No)	Deviations / Remarks
IRI.001	Range Distance	Minimum 80 m		
IRI.002	Angle	60 degrees minimum Adjustable		
IRI.003	Power	Input 100-240V AC, or 12/24 V AC/DC		
IRI.004	Casing	IP66 rated / NEMA 4X vandal resistance		
IRI.005	Operating Condition	0° to 50°C or better		
IRI.006	Certification	CE, FCC, ETL/UL, RoHS		
IRI.007	Lighting	High Definition LED's		
IRI.008	Required Accessories	Power Supply, Mounting Clamps, U-bracket		
IRI.009	Support	System should not be an end of life / end of service product.		

I. Variable Message Sign Board – VaMS				
Sr. No.	Item	Minimum Requirement Description	Compliance (Yes / No)	Deviations / Remarks
VaMS.001	Dimension Requirements	VaMS shall be full-matrix type (adjustable text size and allow both upper and lower case).		
VaMS.002	Display Requirements	Electronic-High Luminosity wide viewing angle oval LEDs (Only Nichia LED) for outdoor ambient light shall be used.		
VaMS.003	Display Requirements	Long life LEDs with minimum working of 1,00,000 hours to Half Life		
VaMS.004	Display Requirements	VMS shall automatically adjust their brightness under varying light conditions to maintain legibility		
VaMS.005	Display Requirements	Luminance of VaMS's should meet industry criteria for daytime and night time conditions		
VaMS.006	Display Requirements	VaMS unit shall have the provision to display online messages received from the command control centre for the duration specified by the user.		
VaMS.007	Display	Minimum vertical clearance between the finished		

	Requirements	road surface and the bottom of the support structure/bottom of the VaMS (whichever is lower) shall be 6.5 m.		
VaMS.008	Required Size for Surveillance	2.88 m x 0.96 m		
VaMS.009	Required Size	1.92 m x 0.96 m		
VaMS.010	Refresh Rate	Minimum 800 Hz		
VaMS.011	Temp Range	0 to +45 Degrees		
VaMS.012	Native Brightness	Minimum 5000 NITs		
VaMS.013	Contrast Ratio	Minimum 1200:1		
VaMS.014	Pixel Requirements	The pixel pitch shall be not more than 16 mm.		
VaMS.015	Pixel Density	Minimum 3096 pixel / m ²		
VaMS.016	LED Configuration	R/G/B 3 in 1 SMD		
VaMS.017	Power Input	100 ~ 240 VAC,		
VaMS.018	Max Power Consumption	≤ 1000 W/Tile		
VaMS.019	Dimming Capabilities	Minimum 64 Levels		
VaMS.020	Humidity	10% ~ 90%		
VaMS.021	IP Level	IP65 Front IP54 Rear		
VaMS.022	Image Processor for Each LED Wall Display	Signal Input – DVI; Signal Output - RJ - 45		
VaMS.023	Communication	The communication protocols supported shall be TCP/IP, RS 232		
VaMS.024	Communication	The signboard unit shall be able to communicate with central command centre computer using GSM data channel (GPRS) / Ethernet will be used to send online messages.		
VaMS.025	Communication	GPRS/ Ethernet port shall also be extended to ground level using necessary cables for local trouble shooting.		
VaMS.026	Communication	Each unit shall be provided with a unique identification number and shall communicate with the designated central command centre system and a local device loaded with relevant software		
VaMS.027	Communication	VMS shall have self-test diagnostics features to test the VMS for correct operation during power on.		
VaMS.028	Display Protection	The front of VaMS display board should be weather resistant IP 65 rated w.r.t various		

		climatic conditions		
VaMS.029	Power Requirements	230V AC + 15%, 50 Hz single phase power supply (Automatically re-start in the event of an electricity failure)		
VaMS.030	Power Requirements	Equipment components shall have adequate surge and lightning protection.		
VaMS.031	Power Requirements	Necessary earthing for electrical and lightning protection to be provisioned as per the industry standards		
VaMS.032	Power Requirements	Inverter of adequate power capacity having 2 hours of back up shall be provided by the vendor to counter any power failure.		
VaMS.033	Power Requirements	The enclosure for the inverter and battery should be pole mountable with IP65 protected housing and shall be lockable.		
VaMS.034	Component Requirement	Components should include SNMP Manageable VMS controller which can be controlled from remote, LEDs, LED matrix boards, pixel arrangements showing horizontal and vertical pitch and total number of pixels, power supply (including surge protection, inverter, back-up batteries), communication ports, cable termination, enclosure and mounting accessories.		
VaMS.035	Software for Layout Management	To be provided by respective OEM. LED Tiles, Image Processor & Software should be from same OEM to ensure compatibility and smooth after sale service support.		
VaMS.036	Power Distribution	Suitable Power Distribution Board to be provided for individual LED Wall		

J. Support Structure for Variable Message Signboards				
Sr. No.	Item	Minimum Requirement Description	Compliance (Yes / No)	Deviations / Remarks
SSVMS.001	General Requirement	Support structure for the VaMS shall be of MS IS: 2062 Gantry type		
SSVMS.002	General Requirement	Structure should be supported on the ground (shoulder/foot-path) on both the sides of the road through appropriate concrete foundation.		
SSVMS.003	General Requirement	Minimum vertical clearance between the finished road surface and the bottom of the support structure/bottom of the VaMS (whichever is lower) shall be 6.5 m as per NHA1		

		guidelines		
SSVMS.004	General Requirement	Support structure shall provide adequate support to the VMS from all four sides as well as top and bottom (at least six to eight connections for mounting the VMS)		
SSVMS.005	Load Requirement	Structure for display board mounting should withstand wind-speeds upto 150km/hr and support the weight of at least two VMS along with structure's self-weight. This should be certified by a structure engineer		
SSVMS.006	Load Requirement	Display board should be secured sufficiently with fasteners and fixtures to the support structure to withstand the mentioned loads.		
SSVMS.007	Painting	Structure shall be painted with one coat of primer and two coats of PU paint. Grey/silver paint or as described by Noida authority		
SSVMS.008	General Requirement	RCC foundation with M20 Grade Ready-mix RCC and required IRON bar structure to take load of Structure weight as well as VMS approved by Structure Engineer		
SSVMS.009	Access	All access panels shall be limited in size so they can be opened or closed by person shall be designed to prevent unauthorized access.		

K. Public Address System				
Sr. No.	Item	Minimum Requirement Description	Compliance (Yes / No)	Deviations / Remarks
PAS.001	PAS system	a) Should have the capability to control individual PAS i.e. to make announcement at select location (1:1) and all locations (1: many) simultaneously. b) The PAS should also support both Live and Recorded inputs.		
PAS.002	Speaker	Minimum 2 speakers, To be used for Public Address System		
PAS.003	Connectivity	IP Based		
PAS.004	Access Control	Access control mechanism would be also required to establish so that the usage is regulated.		
PAS.005	Integration	With VaMS and Command and Control Centre or any other component if required		
PAS.006	Construction	Cast Iron Foundation and M.S. Pole, Sturdy Body for equipment		
PAS.007	Battery	Internal Battery with different charging options (Solar/Mains)		
PAS.008	Power	Mains Power 230V AC and Backup 24VDC		

PAS.009	Casing	IP-55 rated for housing		
PAS.010	Operating conditions	0° to 55°C		
PAS.011	Central Server/Software	Redundant central application server/software		
PAS.012	Integration	Integration with command and control centre		
L. PAS - IP Amplifier				
S.No.	Description	Minimum specifications	Compliance (Yes / No)	Deviations / Remarks
PAS.013	Amplifier Type	Class D		
PAS.014	Amplifier output	250 Watts		
PAS.015	Connectivity	IP-Based, No conversion of Analogue amplifier to IP allowed		
PAS.016	Power	Mains Power 230V AC and Backup 24VDC		
PAS.017	Operating temperature	0°C and +55°C at a maximum relative ambient humidity of 95%.		
PAS.018	Certification	CE		
PAS.019	Monitoring functionality	Line monitoring		
PAS.020	Environment protection	IP 55 or better		
PAS.021	Audio transmission bandwidth	16 kHz		

M. Network Switch Ruggedized				
Sr. No.	Item	Minimum Requirement Description	Compliance (Yes / No)	Deviations / Remarks
NSR.001	General Requirement	The switch should be Industrial Grade ruggedized in nature that provides minimum 8 x 10/100/1000 BASETX access ports, additional 2 x 1000 Base-X SFP & 2x 1GE Uplink ports. One (1) ruggedized single mode SFP should be supplied with the switch.		
NSR.002	General Requirement	The switch should have non-blocking wire-speed architecture with support for both IPv4 & IPv6 from day one with wire-rate switching fabric of minimum 16 Gbps or more. Switch should have minimum 1GB RAM/DRAM & 1GB removable flash card.		

NSR.003	General Requirement	The switch should support backup storage drives, which will store the last known configuration of the switch, in the case of hardware failure and replacement. Reinserting the storage drive should restore the switch to original working condition without any manual intervention.		
NSR.004	Layer 2 Features	802.1Q VLAN on all ports with minimum 10k MAC address		
NSR.005	Layer 2 Features	Spanning Tree Protocol as per IEEE 802.1d, ring protection protocol like REP or equivalent		
NSR.006	Layer 2 Features	Should support Jumbo frames up to 9000 bytes & Link Aggregation Control Protocol (LACP) as per IEEE 802.3ad.		
NSR.007	Layer 2 Features	The switch should support IGMP v1/v2/v3 & up to 1000 IGMP groups as well as IGMP snooping & IGMP filtering. Should also support MLD v1/v2.		
NSR.008	Layer 3 Features	Static, Inter-VLAN routing must be enabled from day one		
NSR.009	Layer 3 Features	The switch should support Dynamic Routing – RIPv1/v2, OSPF for both IPv4 & IPv6, PBR, network address translation etc. protocol by enabling/upgrading the license as & when required		
NSR.010	Quality of Service (QoS)	Switch should support classification and scheduling as per IEEE 802.1P on all ports with minimum four egress queues per port		
NSR.011	Features	The switch should provide traffic shaping and rate limiting		

N. Pole for Cameras				
Sr. No.	Item	Minimum Requirement Description	Compliance (Yes / No)	Deviations / Remarks
POLE.001	General Requirement	Shall be minimum 6.5m height as per NHAI norms		
POLE.002	General Requirement	Hot dip galvanized pole with silver coating of 86 micron as per IS:2629 min 10 cm diameter pole and suitable bottom and top thick HT plate along with base plate		

		size 30x30x15 cms suitable for wind speed 50 m/sec with suitable arm bracket and with J type foundation bolts. Fabrication in accordance with IS 2713 (1980)		
POLE.003	Foundation	Pole would be fixed on an adequate and strong foundation to withstand city weather conditions and wind speed of 150 km/hr		
POLE.004	Foundation	Casting of civil foundation with foundation bolts to ensure vibration free (video feed quality should not be impacted due to wind in different climatic conditions) Expected foundation depth of minimum 100 cms or better		
POLE.005	Sign Board with number plate	Sign board depicting the area under surveillance and with serial number of pole		
POLE.006	Height	Height of the pole shall be as per requirement of the location varying from 6 m to 12/15 m.		
POLE.007	Electrical Connection	Electrical power requirement for the systems/devices installed on the pole should be available with metering and protection equipment		
POLE.008	Lightning Protection	Lighting arrestors with proper grounding		
POLE.009	Earthing	Pole should have proper earthing system		
POLE.010	Network Communication	All communication passive & active devices should be housed in enclosure of adequate standards and protection		

O. Pole for Cameras - Junction Box				
Sr. No.	Item	Minimum Requirement Description	Compliance (Yes / No)	Deviations / Remarks
POLJB.001	General Requirement	All the junction boxes shall be out door type with IP65 protection from rain, water. Provision for theft prevention. (Expected outdoor temperature 50C).		
POLJB.002	General Requirement	<ul style="list-style-type: none"> ▪ 1.5 mm steel sheet, profiled frame construction consisting of 9 folded rolled hollow sections punched on a 25 mm DIN Pitch pattern with load carrying capacity of 500 kgs. ▪ Front and rear 2 mm thick sheet steel door with PU Foamed Seal (Gasketing) with removable galvanized rectangular frame with holes on a 25 mm DIN pitch pattern with 3 point locking system. ▪ Hinges and retainers should be made of die cast, copper nickel chrome plated with SS hinge pins. 		

		<ul style="list-style-type: none"> ▪ Doors should be swapped to LH if required with door opening angle 130°C to VDI. ▪ Top panel made of 1.5 mm thick sheet steel with PU foamed (Gasketing) bolt able from inside. ▪ Bottom panel made of 1.5 mm thick sheet steel with PU foamed (Gasketing) with provision for fixing 4 nos of PG 29 glands. ▪ Side panels in double walled construction with air gap of minimum 20 mm between two walls with PU foamed(Gasketing) for IP 55 protection. Painting: Electro-phoretic dip coat priming to 20 Microns and then powder coated to RAL 7035 textured Pure Polyester (PP) to 80 to 120 Microns. powder coated with surface finishing nano coating, for the best possible surface protection and corrosion resistance. ▪ Side and Wall Panels shall be double wall constructed, with fixing bolts internal to the cabinet. 		
--	--	--	--	--

P. Pole for Cameras - Junction Box				
Sr. No.	Item	Minimum Requirement Description	Compliance (Yes / No)	Deviations / Remarks
POLJB.03	General Requirement	Should be outdoor type, Floor mounting with 3 point locking option, suitable to mount the switches and required UPS. Opening lever/handles shall be made of metal. Each Cabinet will be mounted on a raised height concrete Plinth, 600 -1000 mm high, as per site requirements.		
POLJB.04	General Requirement	Cabinet will be provided with a dimension of 800mmW x 1200mmH (24UH) x 800mmD with 19” mounting arrangement suitable for the mounting of associated network, power, UPS and Split Battery components securely and safely within the cabinet.		
POLJB.05	General Requirement	Junction box shall have floor mount type with required mounting accessories to provide a flexible solution for space constrained traffic applications.		
POLJB.06	General Requirement	2 x 5 way/15 Amp PDU’s will be provided to support the site equipment. 2 x thermostat controlled 230V AC Fans with 100% Duty Cycle with Filter and 2X Filter units with IP55 Rating with rain Canopy shall be fitted to front door of cabinet to provide ventilation to cool the equipment.		
POLJB.07	General Requirement	75 mm Rain canopy on Top with all around projection of the enclosure such that that rain water, water logging		

		shall not penetrate in the junction box and hamper working of the system, cable entry with glands.		
POLJB.008	General Requirement	Small Junction box for mounting Electrical Meter, Fuse and MCB with separate lock for utility power connection		
POLJB.009	General Requirement	Protection from ants, bugs and other small insects entering the enclosure		
POLJB.010	Standard and Support	Regulatory Standard Compliance: IP55 to EN60529/09.2000, ISO 9001, 14001, 18001 comply with EIA 310, DIN 41494 and IEC 297 standards. The system should not be an end of life / end of service product.		

Q. Automatic Number Plate Recognition (ANPR)

Sr. No.	Item	Minimum Requirement Description	Compliance (Yes / No)	Deviations / Remarks
ANPR.001	General Requirements	Cameras shall cover single lanes of 3.5 m each. For places where more than two lanes are to be monitored, lane cameras to be increased in proportion to the lane		
ANPR.002	General Requirements	System shall have IR illuminators to provide illumination for night-time scenario. Camera with IR illuminators should be deployed at heights between 20 feet to allow HMV (high motor vehicle) to pass underneath it, and to minimize occlusion.		
ANPR.003	General Requirements	System should have the facility to provide the live feed of the camera at the central command centre or as per user requirement.		
ANPR.004	General Requirements	System should be able to provide video clips of the transaction from the ANPR lane cameras as evidence		
ANPR.005	General Requirements	For each detected violation, the system would store 5 snapshots of both cameras, date and time, location, ANPR recognized license plate number, thumbnail of the license plate region		
ANPR.006	General Requirements	System should perform ANPR on all vehicles passing the site and send alert to central command centre on detection of any Hot-listed vehicles (whose numbers marked as Stolen, Wanted, etc. at the Central server).		
ANPR.007	General Requirements	With detected number plate text, picture should also be sent of hot listed vehicle. It is likely to misread similar alphabets like 7/1/L or 8/B		
ANPR.008	General Requirements	System should work 24 x 7 in both day and night conditions with good accuracy for the duration of the project		
ANPR.009	General Requirements	System should be able to detect and recognize the English alpha numeric License plate standard fonts and formats,		

		defined under CMVR 1989		
ANPR.0 10	General Requirements	System should have ANPR/ OCR to address the Alpha numerical character of irregular font sizes.		
ANPR.0 11	General Requirements	System should capture standard HSRP (high security registration plate, as per Govt of India notification) vehicle's number plates with an accuracy of at least 85% at day time and at least with an accuracy of 80% at night time. (On basis of number of vehicles)		
ANPR.0 12	General Requirements	System should have an option for the user to enter Hot-Listed vehicles at the Central Server and the same should be sent to all the sites automatically over the network.		
ANPR.0 13	General Requirements	Bidder to provide system with local processing unit at site and send only processed data		
ANPR.0 14	General Requirements	Local processing unit should be industrial grade capable of working up to 70° C		
ANPR.0 15	Vehicle detection by Colour	System shall have options to search historical records for post event analysis by vehicle colour or vehicle colour with license plate and date time combinations		
ANPR.0 16	Alert Generation	System should have option to input certain license plates according to hot listed categories like "Wanted", "Suspicious", "Stolen", etc. by authorized personnel.		
ANPR.0 17	Alert Generation	System should be able 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.		
ANPR.0 18	Logs	System shall enable easy and quick retrieval of snapshots, video and other data for post incident analysis and investigations.		
ANPR.0 19	Logs	System should be able to generate suitable MIS reports that will provide meaningful data to concerned authorities and facilitate optimum utilization of resources. A) Report of vehicle flow at each of the installed locations for Last Day, Last Week and Last Month. B) Report of vehicles in the detected categories at each of the installed locations for Last Day, Last Week and Last Month. C) Report of Vehicle Status change in different Vehicle Categories.		
ANPR.0 20	Logs	System shall have Search option to tune the reports based on license plate number, date and time, site location as per the need of the authorities. System shall have option to save custom reports for subsequent use.		
ANPR.0 21	Logs	System shall have option to export report being viewed to common format for use outside of the ANPRS or exporting into other systems.		
R. Red Light Violation Detection (RLVD)				

Sr. No.	Item	Minimum Requirement Description	Compliance (Yes / No)	Deviations / Remarks
RLVD.001	General Requirements	One single installation system should consist of cameras out of which one camera should be an overview camera providing evidence of the violation by capturing the offending vehicle and status of the traffic light in the same field of view		
RLVD.002	General Requirements	System should have the facility to provide the live feed of the camera at the central command centre as per user requirement.		
RLVD.003	General Requirements	System should generate Alarms at control room software if any signal is found not turning RED within a specific duration of time.		
RLVD.004	General Requirements	The system should be able to provide video clips of the transaction from the overview and lane cameras as evidence		
RLVD.005	General Requirements	For each detected violation, system Should store 5 snapshots of both cameras, date, time, location, ANPR recognized license plate number, thumbnail of license plate region, phase of light (red, amber), time since phase change (red, amber).		
RLVD.006	General Requirements	System should not use signal from traffic controller but use sensors instead. Should work without any lane based intuitive sensors like loops, piezo etc.		
RLVD.007	General Requirements	Should generate alarm if cameras get misaligned or dysfunctional including images- multiple images for pre and post infraction for red light over jumping, data, time, location, speed, with automatic number plate detection mechanism (to recognize vehicle automatically)		
RLVD.008	General Requirements	ANPR provided with RLVD should be capable of also searching for hot listed vehicles during green light. Accuracy of 85% in Day and 80% in Night for Standard HSRP plates.		
RLVD.009	General Requirements	Local processing unit should be industrial grade type (700 C)		
RLVD.010	General Requirements	local site should send transaction data for all violations and alerts of Hot listed vehicles to the central server. Alerts should be sent immediately, whereas violation data should be sent in batch mode as per available bandwidth		
RLVD.011	General Requirements	System should provide facility to search for the cases of violations occurred during any specific span of time, and provide a statistical analysis of the number of such incidences occurring during various days of the month, various months of the year in graphical forms. A report of all such incidences should be		

		available and transferable in hard copy during any selected span of time.		
RLVD.0 12	General Requirements	Additionally, the system should be able to store license plates numbers of at least 10,000 suspected vehicles at a time and should generate an Alert is any one of the vehicles is found crossing the stop line (irrespective whether the signal is GREEN or RED)		

S. Face Recognition System				
Sr. No.	Item	Minimum Requirement Description	Compliance (Yes / No)	Deviations / Remarks
FRS.001	General Requirements	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.		
FRS.002	General Requirements	The facial recognition system should be able to work on the server/ desktop OS as recommended by OEM and provided by the System Integrator		
FRS.003	General Requirements	The user interface of the facial recognition system should have a report management tool 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.		
FRS.004	General Requirements	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.		
FRS.005	General Requirements	System should have ability to handle initial real-time watch list of 100,000 Faces (should be scalable to at least 1 Million faces) and 50 Camera Feeds simultaneously and generate face matching alerts.		
FRS.006	General Requirements	The algorithm for facial recognition or the forensic tool should be able to recognise partial faces with varying angles		
FRS.007	General	System should be able to detect multiple faces from live single		

	Require ments	video feed		
FRS.008	General Require ments	System should have combination of eye-zone extraction and facial recognition		
FRS.009	General Require ments	System should have short processing time and high recognition rate		
FRS.010	General Require ments	System should be able to recognize faces regardless of vantage point and any facial accessories/ hair (glasses, beard, expressions)		
FRS.011	General Require ments	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 of GPU technology instead of Traditional CPUs, to greatly improve the computational performance in crowded environments.		
FRS.012	General Require ments	System should be able to identify and authenticate based on individual facial features		
FRS.013	General Require ments	System should be compatible with the video management system being proposed by the system integrator		
FRS.014	General Require ments	System should have capability for 1:1 verification and 1:N identification matching		
FRS.015	General Require ments	The system should be able to integrate with other systems in the future such as 'Automatic fingerprint identification system (AFIS)' etc.		
FRS.016	General Require ments	The system should be able to support diverse industry standard graphic and video formats as well as live cameras		
FRS.017	General Require ments	The system should be able to match faces from recorded media.		
FRS.018	General Require ments	The system should be able to detect a face from a group photo		
FRS.019	General Require ments	The system should be able to detect a face from stored videos of any format		
FRS.020	General Require ments	The system should have bulk process of adding faces in the system		
FRS.021	General	The system should be an independent system, with capability		

	Requirements	to integrate with industry standard Video Management Systems (VMS) for alert viewing.		
FRS.022	General Requirements	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.		
FRS.023	General Requirements	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.		
FRS.024	General Requirements	The system shall be able to detect faces in different environmental changes like rain, wind, fog and poor light.		
FRS.025	General Requirements	The system should have the facility to categorize the images like "Remember this person" or "hit-list" or "wanted".		
FRS.026	General Requirements	The OEM should have deployed the solution in India		

T. E Challan Handheld device:				
Sr. No.	Item	Minimum Requirement Description	Compliance (Yes / No)	Deviations / Remarks
ECHH.001	Operating System	Latest Windows or Android OS or iOS		
ECHH.002	Processor	Min 1.2GHz Quad Core		
ECHH.003	Memory (Flash ROM)	Minimum 8 MB		
ECHH.004	RAM	1GB Min		
ECHH.005	Extend Slot	Micro SD 32 GB		
ECHH.006	Display	Min 3.5 inch TFT LCD (Trans reflective screen VGA/QVGA)		
ECHH.007	Touch Screen	Yes		
ECHH.008	Form Factor	Any		
ECHH.009	GPS	Yes		
ECHH.010	Bluetooth	Yes		
ECHH.011	Wi-Fi	Wi-Fi (802.11 b/g/n)		
ECHH.012	Thermal Printer	Direct thermal line printing 3 inch		
ECHH.013	Barcode scanner	1D and 2 Scanner		
ECHH.014	External Interface	USB HOST/RS232(Customized)		
ECHH.015	Drop resistance	1.5m		

	level			
ECHH.016	Camera	3 MP Min		
ECHH.017	Camera- Video	Support still image and video capture		
ECHH.018	Keypad Front	QWERTY 42 Keys / touch screen keypads		
ECHH.019	Mini-USB Connector	USB2.0 connection		
ECHH.020	Credit/Debit Card Slot	Yes		
ECHH.021	SIM card slot	Yes		
ECHH.022	TF card slot	Yes		
ECHH.023	Power jack	Yes		
ECHH.024	Audio Jack	Yes		
ECHH.025	Battery Type	rechargeable Li-ion battery 3000mAh		
ECHH.026	Operating temperature	0 deg C to 50 deg C		
ECHH.027	Storage temperature	0 deg C to 60 deg C		
ECHH.028	Operating humidity	10%--80%		
ECHH.029	Storage humidity	10%--90%		
ECHH.030	Payment PINPAD	Device should have/be supplied with (in case of wireless bluetooth printer) IPCI, EMV certified PINPAD as per RBI guideline for accepting payment through Credit / Debit card		

U. Camera Specification for Police VAN with NVR

S. No.	Features	Description	Compliance (Yes/No)
1.	Camera Type	Mobile Speed PTZ	
2.	Standard	ONVIF Profile S Compliant	
3.	Certification	UL,CE/BIS ,FCC and RoHS	
4.	Image Sensor	1/2.8" CMOS or better	
5.	Resolution	2MP (Min.1920 x 1080) at 25 FPS or better	
6.	Max. Mbps CVBR	5	
7.	Compression	H.264 and H.265	
8.	Streaming	Min. Dual compressed stream (Individually Configurable)	
9.	Encryption	HTTP(SSl/TLS)/HTTPS	
10.	Video Authentication	For video authentication, digital signature must be embedded in Video Stream along with name, time, date stamped which cannot be tampered	
11.	Physical Layer	10/100 base Tx Ethernet	

12.	Protocol	Minimum TCP, HTTP, RTP, RTSP, SNMP, IPV4, IPv6,FTP, NTP,DHCP, RTP, SMTP, UDP, UPnP, ICMP, IGMP, SSL, QoS, 802.1x, DNS,DDNS, HTTPS	
13.	IP Support	Static/dynamic or both	
14.	Remote Administration	Remote configuration and status using web based tool	
15.	System Update	Remote system update over Network using web client	
16.	PC Client	PC application client with a channel recording feature support	
17.	Web Client	Viewer through HTTP(min.) System Configuration Setting / Streaming	
18.	Simultaneous Connection	5 users or more	
19.	Lens Type	4.7 – 94mm, 20x motorized, Autofocus, Autoiris, Varifocal	
20.	Dynamic Noise Reduction	3D	
21.	Auto Exposure	Automatic Level Control/Electronic Level Control	
22.	Intelligent Defog	Yes	
23.	Illumination	Color: 0.05 lux, F1.6 B/W: 0.01 lux, F1.6 At 30 IRE Inbuilt IR (60 mtrs. or better)	
24.	Signal Process	Digital Signal Process	
25.	Auto Gain Control	Yes	
26.	Back Light Compensation	Yes	
27.	High Light Compensation	Yes	
28.	Electronic Shutter	1/10000s to 1 s or better	
29.	White Balance	Yes	
30.	Wide Dynamic Range	min 120 db (Sensor based)	
31.	Day and Night	Yes, (ICR)	
32.	Operating Temperature	0 °C to 60 °C Humidity 20–80% RH (non-condensing)	
33.	Power Source	Suitable adaptor shall be supplied to make the equipment work on 230V \pm 10%, 50Hz and Power over Ethernet (POE 802.3 at) or 12 V DC through NVR	
34.	Internet protocol Support	IPv4 and IPv6	
35.	Housing	Poly Carbonate/ Aluminum Construction with IP-66 Including pole mount/wall	

		mount accessories, Power and data cables	
36.	Presets	100 presets or higher	
37.	Edge based video content Analytics	Video motion detection and Active tampering alarm	
38.	Accessories	All required accessories at site for installation of camera to be provided like Pole Mount, Corner brackets, Connector kit, screws etc.	
V. Display			
1.	Display	7inch/ 10 inch display/tablet to be provided along with all necessary cables for connecting with NVR/Camera for display and power adapter etc.	
2.	Accessories	All required accessories for installation of Display in PCR VAN to be provided like brackets, Connector kit, screws etc.	
3.	Warranty	5 Years Comprehensive OEM Warranty	

W. Body Worn Camera			
S. No.	Features	Feature Description	Compliance (Yes/No)
1	Display	Shall have inbuilt min 2.0" TFT LCD with 16:9/4:3 aspect ratio for viewing camera video and Configuration of the device. Must be Visible under sun light.	
2	CCTV camera	Shall be embedded with wide angle CMOS image sensor of min. 16 MP	
3	Compression technique	H.264/H.265	
4	Resolution	Shall support capture at min. 16MP with .jpg format and recording up to 2MP resolution with .mp4 format H.264/H.265	
5	Recording Frame rate	Min.1920 x 1080 at 25 FPS or better	
6	ICR	Shall support auto IR switch function	
7	Night View	white LED, IR LED, Min. 10M Infrared Distance	
8	Network Support	3G (WCDMA, TD-SCDMA, EVDO) and 4G (FDD-LTE, TD-LTE)	
9	Satellite positioning	Built in GPS/GPSS module	
10	Transmission	Shall transfer real time video/audio to management system via Wi-fi 802.11a/b/g/n module and 4G module	
11	Storage	Inbuilt Min. 128 GB	

12	Audio i/o	Shall support 2 way audio communication, shall also have built in mic and speaker provision	
13	Interface	Min. One USB 2.0/USB 3.0 port to backup stored files and charging battery	
14	Battery Capacity	min 2700mAh	
15	Accessories	Battery Charger to be provided	
16	Alarm button	SOS button, in case of danger or emergency, should send alarm signal using this button	
17	Physical button	Button for IP based, Power On/Off, Video recording, Audio recording, Snapshot, Event tag	
18	Protection	Waterproof with IP66 protection	
19	Shock Absorption	upto 2 meters drop	
20	Weight	Should not be more than 220 gm	

4. COMPONENT 4 : ICT Enabled Solid Waste Management

4.1. Overview

Agra Municipal Corporation is responsible for collection, segregation, transportation, dumping and processing of the city waste from door to door.

Waste is transferred from primary collection vehicles into secondary collection vehicles for dumping at Waste Processing plant. AMC has field staff responsible for street sweeping and collection of street waste and dumping to the nearest bins.

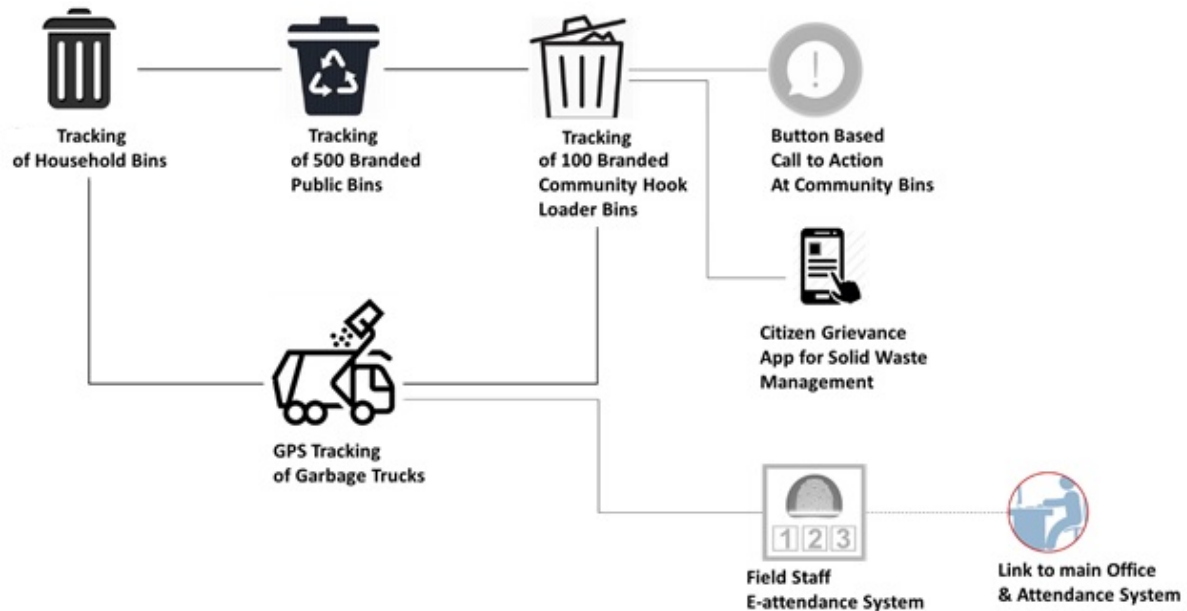
Currently, managing people responsible for the activity and proper utilization of assets/resources assigned to them has become a complex job for AMC. The main problems of existing solid waste collection process are:

- 1) Lack of information about collection time and area.
- 2) Lack of proper system for monitoring, tracking collection & transportation vehicles
- 3) Physical visit required to verify employee performance
- 4) Transfer of waste from primary collection to secondary collection is vehicle transfer and improper co-ordination leads to missed trips and garbage piling.
- 5) Lack of quick response to urgent cases like truck accident, breakdown, long time idling, etc.

ASCL intends to implement a RF/QR Code based and GPS enabled Solid Waste Management System practices within the existing landscape to:

- 1) Door to door collection tracking and monitoring
- 2) GIS Mapping of Commercial Establishment with Entity Type
- 3) RFID Tags/QR Code for door to door, waste tracking and monitoring. Primary objective of the project is to track location of waste pickup at each house-hold/commercial establishments and tipper vehicles movement .
- 4) Option to capture pictorial evidence with GPS Location and issue notification for each pickup.
- 5) Placing RFID tags/QR Code on each house-hold/Commercial Establishment/Dustbins from where waste need to be picked up.
- 6) Option for Route Creation over the Map
- 7) Route assignment/roaster management for route scheduling and assignment
- 8) Manage routes and vehicles dynamically through an automated system.
- 9) Route optimization which shall help in reduction of trip time, fuel saving and serving more locations
- 10) Reduce human intervention in monitoring process
- 11) Determine the Route Violation if any
- 12) Record & maintain history of vehicle routes, attended sites/missed sites/bins and other details
- 13) Reporting of vehicles, garbage collected and other SWM details to higher authorities from any location at any time
- 14) Monitor and track activities of field staff on daily basis
- 15) Real time management of missed garbage collection points

- 16) Ensure complete coverage of door to door and community collections
- 17) Option to send verification SMS/notification to registered mobile number for each household and collect response.



4.2. Project Intent

The ICT enabled solid waste management component will provide a transparent and comprehensive mechanism to monitor & manage the solid waste management process across all the wards in the city. Under this component, existing vehicles deployed for collection of solid waste will be fitted with GPS devices for vehicle tracking and RFID readers/Smart Phones to read the RFID/QR Code tagged community bins. RFID/QR Code tags will be installed on community bins. RFID tags/QR Code will be installed at each house and commercial establishment in the city and all the field staff collecting the solid waste will be provided with GPRS Based RFID readers/Smart phones. Handheld devices like GPRS based RFID Reader/Smart Phones or POS Device will be deployed to manage the workforce deployed for solid waste collection.

The field staff collecting the solid waste should capture evidence of pickup and notify the user on Mobile App/SMS and the end customer should be able to track daily/monthly collection status/report thorough Mobile App. It should also be possible for the end customer to request for the collection report though a missed call or SMS on a predefined number.

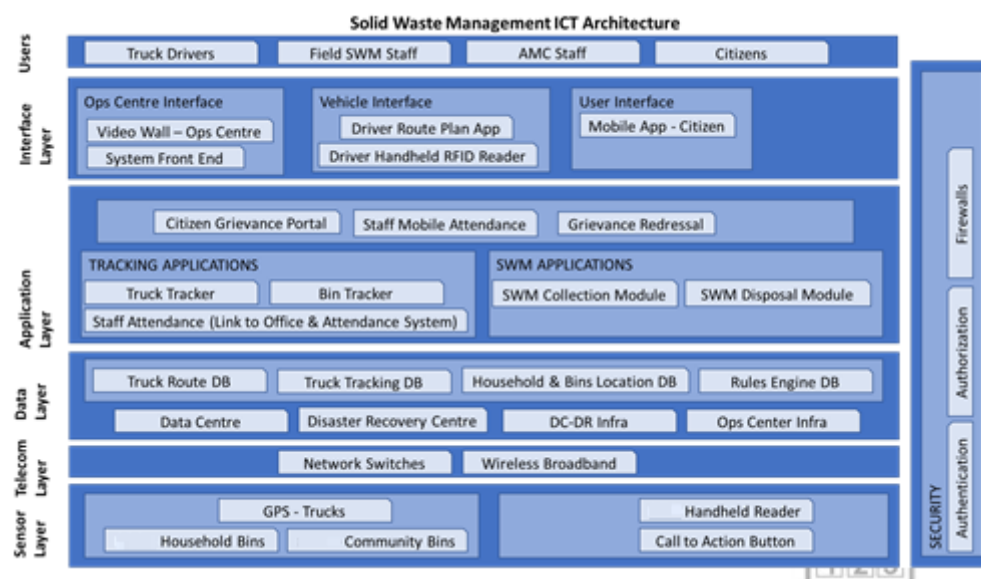
4.3. Scope of Work

Solution should use latest GPS, RFID Tag/QR Code, Biometric system and sensor based technology for real time tracking and monitoring of operational vehicles at garbage collection process throughout city. It should enable ease and transparency in operation of collection municipal solid waste.

Provide end-to-end ICT solution to implement and provide support services & maintenance.

- 1) Implementation of “Door to Door Collection Monitoring System”
 - i. Supply and installation RFID tags/QR Code and GPRS Based RFID readers/Smart Phones.
 - ii. Design and integrate Door to Door Tracking and Monitoring System
 - iii. Registration of Each House Hold/Floor/Commercial Establishment for Master Data
- 2) MSI should provide Automatic Vehicle Locator solution to vehicles to track the complete traverse path round the clock with any state of movement or non-movement
- 3) MSI should provide GPS and Pictorial based attendance management system to the staff
- 4) MSI should install surveillance cameras at bulk waste generation/ collection points.
- 5) MSI shall provide an MIS system which shall be capable of recording details of daily waste collection, waste processed and waste disposed in terms of tonnage. Solution shall be automated with a computerized weigh bridge. Data from the weigh bridge shall be transmitted online to OCC.
- 6) Integrating data feed from waste disposal site (data feed access would be provided by BSCL/BMC) like feeds from CCTV camera and Data from Weigh Bridge
- 7) Sizing of hardware, software and network devices required in DC/DR for using the Integrated SWM.
- 8) Supply & Installation of hardware (servers), software and network devices required in DC/DR for using the Integrated SWM.
- 9) Design, Development, Supply, and Deployment & Implementation of Web Based Application software integrated with GPS, RFID devices, QR Codes & Vehicle Tracking Management System (VTMS) and complaint management modules.
- 10) Mobile Apps for both Android & iOS for Citizens for complaint and Door to Door Solution and also integrate with Meragra Citizen App or other available SWM Solution
- 11) Maintenance of RFID devices and other provided hardware and after warranty period including the replacement of devices in case of damage, new vehicle or any other change.
- 12) Maintenance of web based application/mobile apps for Integrated SWM, during and after warranty for a period of 5 years.
- 13) Real time management of missed garbage transfer
- 14) Daily report of Door-Door Collection efficiency combined with complaints raised by Public
- 15) Monitoring & Reporting Application - reports of vehicles, garbage collection status, bin status etc.

- 16) Provide resources for support, maintenance and administration of the system.
- 17) Integration of ISWM with City Operation Command Centre
- 18) Provide training to ASCL resources for operating the SWM system.



4.4. Mandatory H/W for Real time monitoring of Solid Waste Collection Process

- 1) All garbage collecting & transferring vehicles need to be fitted with GPS devices and RFID Reader/QR Code Reader/Smart Phones and GPS device must be capable to accept the data from such readers and transfer on command center/servers
- 2) All the vehicles will also be fitted with RFID Tag/QR Code as well
- 3) RFID tags/QR Code Tags on Door to Door Collection Points/Bins and on Commercial Establishment
- 4) All Community Bins / Container Bins need to be fitted with Level Sensors and communication module for data transfer.
- 5) RFID Readers at strategic location such as Key Entry/Exit Points, Parking Areas, Waste Transfer Stations, Regional/Zonal Offices, Weighbridges, Dump Site and Waste Recycling Plants
- 6) Automated Weighing Scales needs to be fitted and integrated with RFID Readers
- 7) Biometric attendance devices have to be given to supervisor staff.
- 8) Premise GPRS based biometric attendance devices needs to be fitted at office location.
- 9) All STP and road sweeping vehicle should have GPS device fitted into it.
- 10) Central control center should have facility of audio- discussion and display unit.

4.5. Functional Specifications

4.5.1. Automated Vehicle Tracking Management System

- 1) GPS tracking of waste pick up vehicle for real time tracking
- 2) System should help in co-ordination between primary and secondary collection vehicles for transferring dump
- 3) Route Optimization will help in reduction of trip time, fuel saving and serving more locations
- 4) System should ensure that complete coverage of door to door and community collections served by vehicles

- 5) Record history of vehicle routes, attended sites and other details
- 6) Monitoring & Reporting Application - reports of vehicles.
- 7) Ensure complete coverage of door to door and community collections served by vehicles
- 8) Alert / Alarm management for Ignition/Over speed/Power Cut and tempering
- 9) Solution should be integrated into the GIS map

4.5.2. Mobile GPS based Staff Attendance Management System

GPS based device like smart phone or any hand held terminal having biometric capture function shall enable AMC's field staff to register their attendance/presence throughout the day. System shall periodically track location (with time stamping) of staff through their GPS based mobile device and shall map it in the system with pre-defined area coordinates. Device shall feed data through GPRS/GSM network to the city operation command centre central application for reporting generation and alerts. The system should provide:

- 1) Mobile device/Smart Phones shall be provided to Staff who are doing activities like door-door collection via Pushcarts / Tricycle / street sweeping
- 2) Provide ability to the staff to update job completion reports along with pictures.
- 3) Pictures should be stored on historical mode in the GIS Map for a period of 1 Month.
- 4) Solution should be integrated into the GIS map
- 5) Solution should be able to mark route attended by staff along with allocated route

4.5.3. Mobile Application for Customers

MSI should integrate with Meragra Application or other available solid waste management solution to be provided to the citizens/public which will help them raise complaint for following:

- 1) Garbage Pile on the roads
- 2) Missed Garbage Collection at residential, commercial, industrial and other areas
- 3) Crowd sourcing application for compliant registration and grievances
- 4) Request for Garbage Collection
- 5) Other issues like Street Sweeping and Blocked Nala/nali etc

4.5.4. Unified Dashboard View for Solid Waste Management

- 1) A unified view should show the primary and secondary collection.
- 2) Included all vehicles tracked via AVL or Mobile based.
- 3) Collection Percentage achieved daily – co-relating with the final dumping process
- 4) Co-relation with the complaints raised / Area, along with photographic evidence
- 5) System should be capable of providing missed collection
- 6) System should be capable of marking areas where waste is generated or high to low basis
- 7) System should be capable of showing only a single selected process for a particular area
- 8) System should be capable of showing complaints raised by citizen tagged to a particular location.

- 9) System should be capable of showing CCTV footages from bulk waste generation points and inside the waste treatment plant on the GIS map
- 10) Unified view should be capable of being integrated with other departments
- 11) Unified View goal will be to improve waste collection efficiency using the field infrastructure deployed
- 12) Any other reports aiding to perform the same shall be in scope of MSI.

4.5.5. Infrastructure Solution - Field Devices

MSI shall be responsible for the supply, installation & commissioning of following field equipment's as per technical specifications mentioned in the RFP document:

- 1) GPS Tracking System with all fittings & fixtures in all the vehicles
- 2) GPS based mobile attendance management.
- 3) CCTV Cameras at Waste Processing Site and at bulk waste generation points
- 4) RFID tags/QR Code at households /RFID tags/QR Code on collection vehicles
- 5) Automated Weigh bridge

Sr. No.	Type of Vehicle/ Staff	Field Devices
1	Auto Tipper (Primary Collection)	GPS Tracking System
2	Push Carts + Tricycle (Primary Collection)	Tracking via GPS Based Attendance System
3	Twin Dumpers (Secondary Collection)	GPS Tracking System
4	Tipper (Secondary Collection)	GPS Tracking System
5	Tractor (Secondary Collection)	GPS Tracking System
6	Field Staff – Collecting Waste	Tracking via GPS based Attendance System
7	Field Staff Sweeping Roads	Tracking via GPS based Attendance System

The solution should have below mentioned indicative functional requirements. However detailed functional requirement will have to be prepared by MSI after award of project by carrying out a detail requirement gathering with AMC and other line departments.

Common Functional Requirements
Dashboard:
Dashboard Module should give a quick and easy view to know overall fleet status on real time basis. It should display status information of all vehicles i.e. Running, Idle or Standby. Dashboard view should provide following information: <ul style="list-style-type: none"> ▪ For each department, separate authentication based vehicle tracking module. ▪ Within department section, there shall be an aggregated view of all department specific vehicles, its location, movement and other real-time details shall be available. ▪ There should be a facility to club area specific and category specific vehicles in groups.

<ul style="list-style-type: none"> ▪ Zone name, Ward Name, Vehicle No, Vehicle Type, Current Location & Last Updated Date & Time of each vehicle. ▪ It should give alert message if GPS device gets disconnected from a vehicle. ▪ Dashboard should have search parameter where different searches i.e. Vehicle Number wise, Zone & Ward wise, running / idle / standby vehicle wise and “No communication” wise searches can be done. ▪ Running Km and Idle KM Related parameters also required on daily basis ▪ It should also give an indication regarding running speed of vehicle i.e. Normal speed, Alarming speed and above Alarming speed. ▪ There should be a provision to see route followed by a vehicle on a GIS map. 	
Map Based Analysis:	
Integration with: <ul style="list-style-type: none"> ▪ GIS ▪ Vehicle Tracking System 	Functionality: <ul style="list-style-type: none"> ▪ Creating buffers along emergency site & working site. ▪ Creating & sending alerts in case SUB's reach particular level for vehicle movement, which can be shown on the map
Functional Requirements – SWM:	
Area Details:	
<ul style="list-style-type: none"> ▪ Area information (Zone / Ward / Colony / Society) ▪ Population details ▪ Volume of Solid waste which includes Wet & Dry waste (recycled & non-recycled) ▪ Resources required ▪ Collection procedure (i.e. Primary: House to House & Secondary: Community Bin to Garbage transport centre or mix) 	
Garbage Collection Scheduling:	
Integration with: <ul style="list-style-type: none"> ▪ GIS ▪ Vehicle Tracking System 	Functionality: <ul style="list-style-type: none"> ▪ Assign SWM Vehicles to pick-up Garbage. Category wise assignment like A: Highly in demand, B: Medium, C: Low Demand. ▪ Assignment of dynamic routes using vehicle initial route and bins attended. ▪ Location-wise assignment of Sanitation Staff ▪ Scheduling of garbage collection and cleaning activities with the objective of maximizing citizen friendliness and optimum use of resources.
Primary Garbage Collection & Disposal:	
Integration with: <ul style="list-style-type: none"> ▪ Weigh Bridge 	Functionality: Record volume of garbage collected/disposed on daily basis.
Integration with: <ul style="list-style-type: none"> ▪ Vehicle Tracking System 	Functionality: Keeping certain Checks as per environmental regulations, like minimum frequency of lifting garbage etc
Management Information System (MIS):	
<ul style="list-style-type: none"> ▪ Monitor deployment of pickup trucks & personnel based on schedule originally drawn. ▪ Info on use of Transfer Stations / Quantity of garbage received 	

- Door to door collection, ward wise / Dashboard for all activities
- Reports of Ward Wise Weight Reports. / Any other custom report as per department

4.6. Technical Specifications

A. GPS Device Unit				
Sr. No.	Item	Minimum Requirement Description	Compliance (Yes/No)	Deviations / Remarks
GPS.001	GPS Receiver	Minimum 16 channels		
GPS.002	GPS re-acquisition functionality	Cold start <= 42 Sec, Warm Start < 35 sec, Hot Start <= 2 Sec		
GPS.003	GPS Tracking Sensitivity	-165 dBm		
GPS.004	GPS Velocity Accuracy	< 0.01 m/sec		
GPS.005	GPS Navigation Sensitivity	-148 dBm		
GPS.006	GPS Navigation Update	1 Second		
GPS.007	GPS Data Format	Support WGS – 84		
GPS.008	GSM/GPRS Band	GSM/GPRS SMT quad band and UMTS (3G)		
GPS.009	GSM/GPRS Network Support	Support all GSM Network		
GPS.010	Data Acquisition and Transmission	Data packets shall have configurable fields - Unit ID, Latitude, Longitude, Speed, Time Stamp, Orientation, GPS fix, Alert Status.		
GPS.011	Data Acquisition and Transmission	Shall be configurable for Data Transmission at varying minimum time intervals of few seconds and minutes to a central computer application		
GPS.012	Data Acquisition and Transmission	Shall support GPS data storage up to 10000 logs (based on string size) during non GPRS coverage area and forward the same when GPRS coverage is available. Shall be capable of storing 150 or more route geofences with facility to update route geofence master in the device over the air		
GPS.013	Data Acquisition and	Shall transmit data in SMS mode when GPRS is not available		

	Transmission			
GPS.01 4	Micro Controller Module support for Interface	16 bit RISC architecture based Micro Controller system for interface with various sub systems		
GPS.01 5	Antennas	Built -in GPS and GSM Antenna.		
GPS.01 6	Audio Interface	16 Watts Audio Amplifiers 4 Loud Speaker (4 Watts each)		
GPS.01 7	Power Supply	Power Supply input support 7 V to 32 V DC battery and shall be powered by vehicle battery and not ignition		
GPS.01 8	Internal Battery Back Up	6-8 hours backup		
GPS.01 9	Environment	Shall be heat resistant, dust resistant and water / rain splash resistant, dustproof, shock proof and tamper proof. Shall have at least IP65 or higher protection classification Operate between 0°C to +55 °C		
GPS.02 0	Status LEDs	Power, GPS, GSM, VMU Status		
GPS.02 1	Alerts & Notifications	Shall be programmed to provide Alerts on power supply disconnect, speed violation, device tampering etc.		
GPS.02 2	Configuration	Shall support Over The Air (OTA) firmware upgrade and shall be remotely configured for the required GSM Service Provider, Server IP connection, GPS data Update Interval etc.		
GPS.02 3	Packaging & Accessories	Dimensions: 121mm (L) x 102mm (W) x 30mm (H) with power supply cable		
GPS.02 4	Rating	22 tracking / 66 acquisition minimum		
GPS.02 5	General Requirement	GPS tracking device should have adequate intelligence and programmability to run custom edge applications and analytics on the edge device.		
GPS.02 6	General Requirement	GPS tracking device should have embedded storage and compute and should offer SDK/API for custom tools and application portability into the same.		
GPS.02 7	Device I/O	GPS tracking device should have minimum 3 digital input and One Analog input and One input for SOS		

B. RFID Reader

Sr. No.	Item	Minimum Requirement Description	Compliance (Yes/No)	Deviations / Remarks
RFIDR.01	Protocol	ISO18000-6C EPC GEN2		

RFIDR.002	Configuration	Shall support Over The Air (OTA) firmware upgrade Shall be configurable for mixed or single tag-type operation		
RFIDR.003	Frequency Range	Standard ISM 902 928MHz or 915 MHz (US FCC), 865 MHz (ETSI 302-208), and 869 MHz (ETSI 300-220)		
RFIDR.004	Operation Mode	FHSS		
RFIDR.005	RF Power	0~30dBm, software adjustable		
RFIDR.006	Reading Speed	Software Programmable Average Reading per 64Bits <6ms		
RFIDR.007	Reading Mode	Timing or Touch, Software Programmable (reading shall be such that the reader does reads two tags at a time)		
RFIDR.008	Communication Mode	TCP/IP and GPRS/GSM/2G or higher		
RFIDR.009	Data Input Port	Trigger input one time		
RFIDR.010	Reading Range	Max 12 m (able to calibrate)		
RFIDR.011	Communication Interface	RS232		
RFIDR.012	Accessories	Vehicle-mount DC power cable kit Antennas, and antenna cables		
RFIDR.013	Environmental Rating	IP68		
RFIDR.014	Humidity	10% to 90%		
RFIDR.015	Shock and Vibration Protection	Withstands standard material handling vehicle environments. Meets or exceeds MIL STD 810F		
RFIDR.016	Operating Temperature:	0°C to 55°C		
RFIDR.017	Storage Temperature:	0°C to 65°C		
RFIDR.018	Power Supply	Vehicle DC power 12 to 60V, 4.5 A maximum		

C. RFID TAG

Sr. No.	Item	Minimum Requirement Description	Compliance (Yes/No)	Deviations / Remarks
RFIDTAG.	Type	ABS, High Quality Engineering Plastic		

001				
RFIDTAG.002	Supported Transponders	ISO18000-6C EPC Class 1 GEN2		
RFIDTAG.003	Frequency Range	ISM 865~928 MHz		
RFIDTAG.004	Operation Mode	Fixed Frequency or FHSS Software Programmable		
RFIDTAG.005	Memory capacity	Tag shall support ISO18000-6C protocol standard 2K Bits storage capacity, 1728 Bits (216bytes) writable user area; MR6730B metal supports EPC C1 GEN2 (ISO18000-6C), with 96Bits writable EPC Code area, 512Bits writable user area, and 32Bits password area, EPC 128 bit user 512 bit TID 96 bits.		
RFIDTAG.006	Reading Rate	Software Programmable, Average Reading per 64 Bits < 10ms		
RFIDTAG.007	Tags material	Metal material		
RFIDTAG.008	Reading Range	Shall be able to be calibrated (to be kept as 4 - 6 m max) based on the site visit		
RFIDTAG.009	Operation Temp	0°C to 60°C		
RFIDTAG.010	IP Classification	IP 68		
RFIDTAG.011	Weather	Heat, dust proof, UV resistant & sea water resistant		
RFIDTAG.012	Chemical Resistance	No physical or performance changes in -168 hour Motor oil exposure 168 hour Salt water exposure (salinity 10%) 5 hrs Sulfuric acid (10 %Ph 2) 1 h Naoh (10 % Ph 14) exposure		

D. Automated Vehicle Locator System - AVLS

Sr. No.	Item	Minimum Requirement Description	Compliance (Yes/No)	Deviations / Remarks
AVLS.001	General Requirement	Each vehicle, using the GPS vehicle tracking (VTS) device, shall determine its precise location through GIS based GPS System and transmit the same to the City Operation Centre at defined intervals of time. The location shall be displayed on GIS based route maps at City Operation centre		
AVLS.0	General	AVLS shall be able to give ETA at next bus stops in real time		

02	Requirement	based on speed and distance measured. System shall update ETA at each bus stop on all PIS accordingly.		
AVLS.003	General Requirement	System shall be able to compare the actual location of the vehicle / bus, at any given time, with its scheduled location		
AVLS.004	General Requirement	System at the control rooms shall be able to calculate the time for the vehicle / bus to reach all subsequent stops along the route, factoring in the current vehicle / bus and any deviations from the schedule and reported traffic congestion enroute		
AVLS.005	General Requirement	Shall provide inputs/feeds to Passenger Information System (PIS) with the real-time data to be displayed at various display units and announcement systems		
AVLS.006	General Requirement	Information elements that need to be captured and transmitted to City Operation Centre at the minimum include longitude, latitude, and physical location enroute with date and time stamps, vehicle / bus number, route number, and Driver ID, etc.		
AVLS.007	General Requirement	Shall provide these data on real time basis at pre-determined and configurable intervals (10 seconds) over GPRS/GSM network		
AVLS.008	General Requirement	Tracking of vehicle / buses that deviate from the scheduled route based on definition of permitted geographic regions of operation		
AVLS.009	General Requirement	Vehicle Fleet Summary Dashboard – Quick view on vehicle fleet performance		
AVLS.010	General Requirement	Register a vehicle / bus on unscheduled route from backend on real time basis		
AVLS.011	General Requirement	Application must have the functioning for planning/scheduling/Rostering/Dispatching of any Bus using Software		
AVLS.012	General Requirement	Option should be there on Driver Console to accept the route assigned by dispatch manager at which bus has to ply		
AVLS.013	General Requirement	Real Time ETA based Trip Management showing trips in progress/completed trips and scheduled trip and Missed Stoppage Details etc		
AVLS.014	General Requirement	Fare Collection Summary for Each Bus and Stoppage wise for the day		
AVLS.015	General Requirement	Exception Recording/ Actions (Over-Speeding, Harsh Acceleration, Harsh Braking, Off-route Detection, unscheduled stoppage, Non-Stoppage at Bus stops/collection points, Trip		

		Cancellation).		
AVLS.0 16	General Require ment	Real-time Running Trip Line diagram of vehicle / buses on a particular route, for headway detection.		
AVLS.0 17	General Require ment	Auto headway detection and notification.		
AVLS.0 18	General Require ment	Applications Software shall have a facility to define the Masters.		
AVLS.0 19	General Require ment	New routes shall be created in the application.		
AVLS.0 20	General Require ment	Business rules engine for fare stages, fare structures, various routes etc. shall be configurable.		
AVLS.0 21	General Require ment	Facility shall be provided to collate the transactional data received from Depots and Bus Stations. The transaction data shall be uploaded once every day for the previous day.		
AVLS.0 22	General Require ment	Officials shall be able to access the application as per the pre-defined roles and responsibilities		
AVLS.0 23	General Require ment	Application shall provide facility to query the data and generate the customized reports as per the requirements.		
AVLS.0 24	General Require ment	System shall display the contact details of the bus driver / conductor so that the operation centre staff can communicate with them directly.		
AVLS.0 25	General Require ment	Operation Centre operator shall be able to drill down to the exact location of the event by clicking on the alert and see the position of event drawn over the map along with driver, vehicle and standard description of event details related to the business rule.		
AVLS.R EQ.026	General Require ment	The system be able to integrate with the City IOP/City Operations Platform with all the available data like Location, route information, Vehicle telemetry information, Speed etc.		
AVLS.R EQ.027	General Require ment	The system should allow programmability, allowing actions to be triggered based on events. e.g. speed metric can trigger API call to GIS Maps pulling speed limit on the road based on GPS or GTFS location.		
AVLS.R EQ.028	General Require ment	The platform should offer an Application builder for developing custom Applications as needed and should support an Interactive Development Environment that can facilitate in-house expertise to develop widgets and create API extensions		

E. Mobile Device for Biometric Attendance				
Sr. No.	Item	Minimum Requirement Description	Compliance (Yes/No)	Deviations / Remarks
MDT.001	Processor	At least Dual core, 1 GHz or more		
MDT.002	Memory	RAM at least 1 GB or better		
MDT.003	Storage	At least 8 GB or higher		
MDT.004	Operating System	Android v 4.1 and above		
MDT.005	Network	2G bands: GSM 900 / 1800 / 1900 3G bands: HSDPA 900 / 2100 Speed: HSPA 14.4/5.76 Mbps GPRS: Yes EDGE: Yes SIM: Single or dual sim		
MDT.006	Display	Capacitive touchscreen, 16M colours Resolution: 480 x 800 pixels (~217 ppi pixel density)		
MDT.007	Generation	2G and 3G support		
MDT.009	GSM	Yes		
MDT.REQ.010	Screen size	minimum 4" with touch support		
MDT. 011	Camera & Video	at least 3MP Front & 5 MP rear with LED Flash (integrated) Geo-tagging, face/smile detection Video: Yes		
MDT. 012	Feature	Should work as Location Tracker device for Attendance Management System		
MDT. 013	Screen luminosity	Daylight readable		
MDT.014	Speakerphone	Hands free Support		
MDT. 015	Keyboard	Virtual on Screen		
MDT. 016	Communication	GPS: Yes with GLONASS, WLAN: Wi-Fi 802.11 b/g/n, Wi-Fi Direct, hotspot, DLNA, Bluetooth: v4.0, A2DP, apt-X, USB: microUSB v2.0		
MDT. 017	Audio Playing Format	With 3.5 mm Jack MP3, wav files format etc.		
MDT. 018	Ports	Micro USB * 1 version 2.0 and above and same for charging and Headset port etc.		
MDT. 019	Power Supply	230V, 50 Hz AC Supply		
MDT. 020	Bluetooth	Yes		
MDT. 021	Battery	minimum 1500 mAh and above		
MDT. 022	Charger	Suitable charger shall be supplied, Built-in rechargeable battery pack/battery. USB Charger		

MDT. 023	Mobile Device Monitoring	Should support the ability to disable access to public App Stores based on a policy configuration		
MDT.REQ.0 24	Mobile Device Monitoring	Should have configuration Policies to allow individual Components of the mobile device to be enabled or disabled.		

F. Quick Response Code (QR Code)

Sr. No.	Item	Minimum Requirement Description	Compliance (Yes/No)	Deviations / Remarks
QR.001	Video Compression & Resolution	Encode up to 7,089 numerals with its maximum version being 40 (177 x 177 modules).		

G. Pan Tilt and Zoom CCTV Cameras for SWM:

Sr. No.	Item	Minimum Requirement Description	Compliance (Yes/No)	Deviations / Remarks
PTZCA.001	Video Compression & Resolution	H.264 or better & 1920 X 1080		
PTZCA.002	Frame rate	Min. 25 fps		
PTZCA.003	Image Sensor & Lens	1/3" OR ¼" Progressive Scan CCD / CMOS & Auto-focus, 4.7 – 84.6 mm		
PTZCA.004	Minimum Illumination	Colour: 0.5 lux, B/W: 0.1 lux (at 30 IRE)		
PTZCA.005	Day/Night Mode	Colour, Mono, Auto		
PTZCA.006	S/N Ratio	≥ 50dB		
PTZCA.007	PTZ	Pan: 360° endless/continuous, 0.2 to 300°/s (auto), 0.2 to 100°/s (Manual) Tilt: 90°, 0.2 to 100°/s (Auto), 0.2 to 40°/s (Manual) 18 x optical & 10 x digital zoom, 16 pre-set positions, Auto-Tracking, Pre-set tour		
PTZCA.008	Auto adjustment &	Colour, brightness, sharpness, contrast, white balance, exposure control, backlight compensation, Gain Control, Wide Dynamic Range		

	Remote Control			
PTZCA.009	Protocol	HTTP, HTTPS, FTP, RTSP, RTP, TCP, UDP, RTCP, DHCP, SNMP		
PTZCA.010	Security	Password Protection, IP Address filtering, User Access Log, HTTPS encryption		
PTZCA.011	Operating conditions	0 to 50°C		
PTZCA.012	Casing	NEMA 4X / IP-66 rated		
PTZCA.013	Certification	UL / CE / FCC / EN		
PTZCA.014	Auto Detection & Configuration	Camera should be automatically discovered & configured when connected to VMS or Network Switch, to set right network parameters for video stream on the network		
PTZCA.015	Activity detection	Camera should support User- definable alerts with configurable sensitivities and thresholds, email alert, HTTP notifications. Camera should support for IEEE 802.1X authentication		

5. Component 5 : City and Enterprise GIS Solution

5.1. Project Objective

The broad objective of the work is to develop a comprehensive Instigated Enterprise GIS Application for Corporation for planning, management and governance in context of entire functioning of the organization. The major activities of the departments to be supported by the system shall be as follows:

- 1) Creation and Updating of Geospatial Data – ABD Area
- 2) Supply of Enterprise GIS Platform Suit – Pan City
- 3) Design Develop Enterprise Web GIS Municipal Application for all ASCL Departments - Pan City
- 4) Design and Develop Geo-enabled Mobile Application for ASCL Pan City
- 5) AMC for 5 Year

5.2. Expected Benefit of the Project

5.2.1. Decision Support System

- 1) Central Command and Control Centre - GIS is Back Bone Infrastructure for Smart City Decision Support System and Command Control Centre
- 2) Dissemination of Geospatial Data at Enterprise Level and to ASCL official and Citizens

5.2.2. Revenue Management

- 1) Better Monitoring of the Recovery of Property, Water & other taxes
- 2) Improve the efficiency of tax authorities and better tracking of defaulters

5.3. Analysis, Planning, Operation and Maintenance

- 1) GIS is used by various department as basic tool for Analysis, Planning, Operation and Maintenance in their day to day functions i.e. Building permission., building Certificate, Town Planning, Property Tax, Land and estate Management, Education Planning, Citizen complain Management, Park and Garden Monitoring, Land Encroachment, Disaster Management, Utility Planning, Operation and Maintenance, Smart Grid, Traffic Planning and VTMS etc.

5.4. Municipal Department Utility Asset Management and Maintenance

- 1) Secured updating of spatial and attribute information for all Assets and Network lying on the ground
- 2) Provide GIS based decision support system for ANN officials to undertake well informed and faster decisions to identification problem and response
- 3) Up-to-date & user friendly maintenance of ASCL assets
- 4) Efficient maintenance of Public utilities like Roads, Street Light, Water Supply Network, Sewerage Network, Petrol Pumps, Dispensary, Hospitals, Fire Stations, Schools, etc.

- 5) Customized GIS Application (to integrate spatial information with the future e governance software solution)

5.5. Dash Board for Project Planning, Implementation and Monitoring

- 1) Visualize Proposed Utility Schema Plan on GIS like road, Sewerage street Light, also other project like Park, School etc
- 2) Support to decide whether need to take the project or Drop
- 3) Support overlay of Final Plan on map.
- 4) Support day to day Updating of project progress on map and Pictures
- 5) Plan and Actual gap Analysis
- 6) Integrate Project Milestone with payment validation

5.6. Scope of Work Overview

Various services that are imperative to achieve the proposed GIS solution and which need to be delivered by bidder include:

5.6.1. Base Map Creation – Pan City

- 1) Procure and supply .5 m or better Resolution, Ortho rectified, Geo
- 2) Referenced Satellite Image
- 3) DGPS Survey
- 4) Image Processing for digitization
- 5) Digitization of Base Map
- 6) Survey - Base Map validation and Verification

5.6.2. Data Updating and Data Creation for ABD Area

- 1) Updating and Creation of Base map
- 2) Creation of Utility Data for New Area Using CAD Drawings approx. 9 SqKm
- 3) Geo-referencing and spatially adjusting the existing town planning sheets with available with ASCL and creating new digital TP sheets for the remaining number of physical and non geo reference TP sheets
- 4) Integration of the readily available data with ASCL to the proposed application/system
- 5) Property/Consumer Survey

5.6.3. Provide GIS Software – Pan City

1. GI and Image Processing Desktop Software
2. Supply, installation, training and maintenance of Enterprise GIS Platform 16 core License

5.6.4. Implementation of Enterprise GIS Suite – Pan City

- 1) Maximum No. of users on Intranet simultaneously viewing spatial data - 500
- 2) Maximum No. of users on Intranet simultaneously editing spatial data - 30

- 3) Maximum No. of users on Internet simultaneously viewing spatial data through ASCL Citizen web portal – 30000
- 4) Desktop GIS User Clients - 4
- 5) Design and Develop Enterprise Web GIS Smart City Application on GIS Platform for ASCL Departments approx. 12 Modules
- 6) Training on Enterprise GIS Software to departmental Users
- 7) Development of GIS based Mobile Application for municipal Survey and Services with comprehensive features for ASCL

5.6.5. Integration GIS with existing, proposed system and Future Systems

Bidder need to Integrate GIS Platform with existing components and utilities, new implemented smart City Components and proposed in future.

5.7. Detail Scope of Work

5.7.1. Geospatial Data Creation and Updating Base Map for PAN Area

The bidder have to create GIS Base map using satellite imagery and utility Layers and update the existing base map and Utility data and also create new data.

5.7.2. Data Collection

Selected Bidder will collect the available maps and secondary data (if any) from ASCL (soft copy and or hard copy) namely; municipal boundary, Zone boundary, Town survey maps, Field measurement book (if available), ward boundary maps, slum related data, sanitation, and basic infra-structural facilities and land marks, details of Town Planning Schemes to be incorporated superimposed / synchronized and corrected suitably to match current field data;

- 1) Existing Base map
- 2) Town Planning Schemes showing proposed land use zoning, transport network and sites designated for various public purposes.
- 3) Maps showing administrative boundaries ward boundaries, census boundaries, slum boundaries.
- 4) Revenue Maps showing Cadastral Boundaries.
- 5) Soft copy Maps / drawings of utilities like water supply, sewerage, storm, water drainage, solid waste disposal, roads and street lights along with the data available with other Concerned Department.
- 6) Location of State and Central Government offices, railways and highways, police stations, primary & high schools, colleges, universities, primary health centers, hospitals, banks, theatres etc. also need to be located on the maps through field verification.
- 7) All the details that ASCL desires to include.

5.7.3. Data validation and gap analysis

Selected Bidder will conduct QA, QC and check the Qty , Quality, Accuracy, source and reliability of the collected data from ASCL, whether the data (spatial or non-spatial) is recent or accurate enough to be used and not obsolete.

5.7.4. Positional Accuracy

Selected Bidder will check whether the positional accuracy of the existing data available (if any) with ASCL is in sync with the Satellite Imagery provided by ASCL. Selected Bidder will prepare base map using the available and fetched data and validation of the same will be carried out by the authorized officials of ASCL. In case of Field Measurement Books, they are to be built and super imposed on the Base Maps.

- 1) **Accuracy Requirement:** The 10% of GCPs will be randomly selected as sample for the accuracy of .3m. On the data and see whether data fits on the projection of basemap in case data doesn't fit ASCL will provide data which can be used.
- 2) **Reliability:** Selected Bidder will check from the available legacy data with ASCL, whether the data (spatial or non-spatial) is recent or accurate enough to be used and not obsolete. In case data is rejected bidder will be responsible to rectify data.
- 3) **Attribute Validity:** Selected Bidder will validate attribute data accuracy, whether the data accurate enough to be used and not obsolete.

5.7.5. Procurement of High Resolution Satellite Imagery – Pan Area

The selected bidders have to procure and supply ortho rectified having 5m or better resolution latest satellite imagery. Only procured imagery shall be used for the preparation of Base Maps, data from alternative online sources such as Google Earth / Google Maps is strictly prohibited as this is strictly against the usage policies of the respective services.

ASCL will provide necessary NOC/Approvals for procurement of Satellite Imagery to the successful bidder. Cost of the Satellite Imagery would be quoted in the Price Bid. Bidder will provide the details of Satellite Imagery proposed in the Technical Solution.

5.7.6. Geo referencing and Post Processing of Satellite Imagery – PAN area

Geo-referencing is the process of assigning real-world coordinates to each pixel of the raster. It is the process of scaling, rotating and translating the image to match a particular size and position.

For Geo-referencing the Bidder needs to take the Ground Control Points (GCPs). GCPs are basically taken as a road intersection points, Building Corners, Permanent Locations etc. Bidder shall generate the Grid of 1 x 1 Sq. km. on the Satellite Image and collect GCPs per Sq. km. GCPs need to be collected using DGPS. The locations identified on the image and real ground should be verified with the Authorized Representative appointed by the Corporation. The data should have following:

- 1) Projection: Universal Transverse Mercator (UTM), Spheroid: WGS 84, Zone: 43N. Observation time for DGPS instruments has to be minimum 12 (Twelve) Hours at Base Station and minimum 30 Min Thirty Minutes at each GCP using DGPS.
- 2) The horizontal accuracy of GCPs should be 0.1-0.3 meters. 5% of GCPs would be randomly selected as sample for the accuracy. If the incorrectness in accuracy found in any sample, the entire work shall be rejected and shall be required to rework.
- 3) To correct various geometric anomalies in raw satellite imagery, Ground Control Points (GCP) collected through Differential Global Positioning System (DGPS) survey will be used for Geo referencing of the imagery

5.7.7. Data Modelling Pan Area

Data Model for storing the spatial & Non-Spatial data shall be decided by the ASCL in consultation with the successful Bidder/SI in accordance with the National Large Scale mapping Policy. "Bidder will modify the data model and update the same with the help of detailed round of discussion with each concerned ASCL department officials. Bidder will understand existing data model of ASCL and will use proper tools to create the data model like CASE tools and UML etc. The final data model will be approved by the ASCL and before proceeding further the data model will be finalized. Once the data model is finalized, bidder will give the details of the data model diagram (ER Diagram) to ASCL for future references or for any modifications in future.

5.7.8. Digitization of Satellite Imagery, Updating and capturing of various layers

Bidder will create / update all geographical features class required as per RFP/SRS by digitizing from satellite imagery of PAN area.

The Satellite Image / scanned map will be digitized using the suitable COTS software. This process includes Creation of standard Template Initially; a standard template will be created & inserted into each Digitized Map. In this template the layer name, line type and color for each feature present on the map will be standardized. This system helps when a number of sheets and village maps are to be mosaicked. This process maintains uniformity in all the maps, which will be digitized.

Post the processing of the satellite imagery by removing the geometric anomalies (if any), the bidder will prepare a Grid of 1Km x 1Km for positioning bidder with respect to its Geographic Location. These grids then further will be divided into 250m x 250m scenes for future usage like Map Book creations, Smart Asset ID creation etc. and future analysis. All the grids and scenes will have unique IDs.

Bidder will then take sufficient number of Ground Control Points (GCPs) collected through Differential Global Positioning System (DGPS) survey. Bidder will prepare an

up-to-date large-scale base map (Scale 1:2000) of all the wards/zones of Agra City using satellite imageries and then will prepare a new Database using the existing Database available with Agra Municipal corporation, as unified Geo-spatial Data with infrastructure details.

Bidder will carry out mapping on the rectified satellite data using heads up digitization process. The features that would be taken for mapping includes Buildings, Vacant Plots, Roads, Bridges, Railway Tracks, Parks, Gardens, Stadiums, Slums, Traffic Squares, Water Bodies (River, Lake, Pond, Drainage, Canal etc), Over Head Tanks, etc. While doing the digitization, a special care of data correctness to be taken like no overshoots / undershoots, proper layering, proper symbology etc.

5.7.9. Property Survey and Property Tagging – ABD Area

ASCL is already in process of property assessment Survey bidder have tag this property survey data to GIS and for this bidder may have to do field survey, the field teams will visit door to door to cover all properties in the area of interest. The teams will contact the occupant/ owner or any other responsible person in the family. And identify the property data and tag it with GIS property maps using mobile / tablet/ handheld application.

5.7.10. Final Base Map preparation – PAN Area

Bidder will integrate information of Utilities features such as Street lighting, Water supply line, Sewerage network, Wastewater, Storm water drain, sanitation facility (Household/public/private), Solid Waste management and unauthorized properties as provided by ASCL as layers with base map.

The layer list would be exhaustive taking into consideration of the features to be captured, the attributes will added etc., The layer list and the database layers would be created using programs, appropriately. All the data captured would be checked and validated using custom built routines for its accuracy and logical correctness. The rigorous QC process of bidder would help in achieving accurate feature capturing, required accuracy in coding and classification.

Final base maps will be prepared at 1:2000 Scale incorporating the data collected, processed and digitized after survey process. The base maps will be prepared in various layers as defined by ASCL.

5.7.11. Tentative GIS Data Layers require for Geospatial Smart City Project

Satellite Imagery

- 1) Latest High resolution Ortho rectified, Geo Referenced Satellite Image of .5m or Better Resolution

Administrative Boundaries

- | | |
|--|--|
| 1) State Boundary | 9) SLUM Boundaries |
| 2) District Boundary | 10) Gamtal/Village Boundaries lying in MC Area |
| 3) Metropolitan Regional Development Authority | 11) Police Thana Jurisdiction Boundaries. |
| 4) Municipal corporation Boundary | 12) Heritage Boundaries / Corridor |
| 5) All Zone Boundaries | 13) Area of Interest Boundaries |
| 6) All Ward Boundaries (Old and New) | 14) TP Boundaries |
| 7) MP Constituency Boundaries | 15) Non TP Boundaries |
| 8) MLA Constituency Boundaries | |

Town Planning Schemes (TP Sheets)

- | | |
|---|--|
| 1) TP Scheme Georeferenced with Total Station Survey done | 6) F Form & B Form Softcopy in XLS Format |
| 2) TP Scheme Total Surveyed done but not georeferenced | 7) Survey Plots , Original Plots and Final Plots |
| 3) TP Scheme Digitized | 8) TP Reservation Plots |
| | 9) Town Planning Sheets |
| 4) Hard copy and No digital | 10) Zone type R3/ R2 etc |
| | 11) Town Planning Survey data |
| 5) Survey Maps for TP Scheme | 12) Field Measurement Books |

Development Plan (DP)

- 1) Development Plans (Latest approved for 10 years)
 - a. Land Use
 - b. Cadastral Map
 - c. Revenue
- 2) Historic DP

Important Features

Road

- | | |
|--|---------------------|
| 1) National High Way | 6) Road Divider |
| 2) State High Way | 7) Road Center line |
| 3) Street and Society Road | 8) Foot Path |
| 4) BRTS Corridor | 9) Traffic Square |
| 5) TAR Road / Cement Road/ Other Road type | 10) Traffic Signals |
| | 11) BRTS Station |

Railway

- | | |
|-----------------------------------|--------------------|
| 1) Railway Property Boundary | 4) Railway Station |
| 2) Railway Track Meter Gauge Line | 5) Metro Line |
| 3) Railway Track Broad Gauge Line | 6) Metro Station |

Bridges

- 1) Flyover
- 2) Under Bridge
- 3) Railway Bridge
- 4) Culvert
- 5) Foot over bridge

Building

- | | |
|-----------------------|------------------|
| 1) Building Boundary | 9) Multi story |
| 2) Building Footprint | 10) Single Story |
| 3) Building Type | 11) Commercial |
| 4) Tenement | 12) Residential |
| 5) Flat | 13) High Rise |
| 6) Bungalow | 14) Low Rise |
| 7) Slum | 15) Govt |
| 8) Society | 16) Private |

Water Bodies

- 1) River
- 2) Lake
- 3) Ponds
- 4) Canal
- 5) Open Sewerage / Drainage

Garden/Parks

- 1) Pvt
- 2) UDA
- 3) MC
- 4) Forest

Stadium, Swimming Pool and Play Grounds

- 1) MC
- 2) UDA
- 3) PVT

Parking

- 1) MC
- 2) UDA
- 3) PVT
- 4) Pay Parking
- 5) Free Parking

Entertainment/Worship Places

- | | |
|-------------|-----------------------------------|
| 1) Theaters | 5) Shopping Malls& Shopping enter |
| 2) Temples | 6) Market |
| 3) Mosque | 7) Water Park |
| 4) Church | 8) Clubs |

Important features

- | | |
|----------------|-----------------|
| 1) Petrol Pump | 6) Hotel |
| 2) Hospital | 7) Restaurants |
| 3) Clinics | 8) Fire Station |
| 4) ATM | 9) Govt Offices |
| 5) Banks | 10) MC Office |

- | | |
|--------------------------|-----------------------------|
| 11) PMRDA office | 17) Vetnary Hospital/Clinic |
| 12) City Civic Centers | 18) Police Station |
| 13) College | 19) Police Chowky |
| 14) School | 20) CCTV Camera |
| 15) Recreational centers | 21) Taxi stands |
| 16) Training centers | 22) Rickshaw Stands |

Utilities

- 1) Power
 - a. HT Line
 - b. Towers
 - c. Street Light
 - i. Poles Locations
 - ii. Fixtures
 - iii. Transformer
 - d. Power Stations
 - e. GIS/ CAD /Paper drawings
- 2) Water Supply Network

<ol style="list-style-type: none"> a. Mains b. Distribution line c. Wells d. Over Head Tanks e. Water supply pipeline f. Waste water supply g. Public taps 	<ol style="list-style-type: none"> h. Storage i. Street Taps, j. GLSR ground level dump reservoir, k. Direction of flow l. Meters m. GIS / CAD /Paper drawings
---	--
- 3) Storm Water Drain Network
 - a. Manholes
 - b. Flow direction,
 - c. Network up to tank if available with MC including all component
 - d. Construction type whether permanent or temporary
 - e. Place of disposal and distance
 - f. Location of culvert and condition
 - g. location and alignment of drain/channels
 - h. Invert level L section of the drain, channel indicating slope
 - i. GIS /CAD /Paper drawings
- 4) Sewerages Network
 - a. Septik Tanks
 - b. House Hold connection
 - c. Pit
 - d. Manhole
 - e. Open Drainage
 - f. Derivation line of underground pipe using manhole and well locations

- g. connectivity house hold network and flow direction to be taken up to STP including all components
 - h. Disposal Sites
 - i. GIS / CAD /Paper drawings
- 5) Sanitation
- a. Material, size, length, and condition of sewage line
 - b. Connectivity to town wide sewerage system
 - c. Septic tank, condition and point of disposal
 - d. Community/Public toilets
 - e. GIS/ CAD /Paper drawings
- 6) Solid Waste Management
- a. Bin of all categories
 - b. Yard
 - c. GIS / CAD /Paper drawings

5.8. Data Migration

Bidder will migrate updated Base Map and Utility Data at ASCL into centrally located Enterprise GIS database.

5.8.1. Supply of Desktop GIS and Image Processing Software

Bidder will provide three licenses of Desktop GIS and Image Processing Software

#	Functional Description	Compliance Status
A. General Functions		
1	Multiple Document Interface (MDI)	
2	Project, View and Layer Management	
3	Geo-Linked Multiple Views	
4	Well known Raster, Vector and Tabular file formats support	
5	On the Fly Map Projection Transformation	
6	Large set of Library for Projection & Geographic Coordinate System	
7	Advance Map Navigation and Visualization	
8	Seamless data handling using ORDBMS	
9	Identification and Measurement Tools	
10	Customizable GUI	
11	Extensive Map Composition Tool	
12	Raster and Vector Catalogue	
13	GIS Software should be able to operate on Windows	
14	The proposed software should have functions of GIS and Image Processing along with advance functions such as network analysis, terrain analysis, 3D analysis, change analysis, etc.	
15	The proposed GIS software could be any Industry standard COTS GIS platform and should be easy to handle, operate, maintain & also train the authority staff/end users.	

16	The customized software for authority should have simple user interface both for departmental users as well as for citizens with easy navigation and querying facility.	
17	On-line help shall be provided at all functions and tools.	
18	The proposed software should be OGC compliant and follow the interoperability.	
19	The software should support all types of raster formats and services like ERDAS IMAGINE, ENVI, PIX, DTED, DEM, CEOS, JPEG, JP2, PNG, GeoTIFF,	
B. GIS Functions		
1	Advance Drawing and Editing	
2	Topology Creation	
3	Edge Matching and Rubber Sheeting	
4	Geometric Correction	
5	Database Management	
6	Query Builder for Simple and Complex Query	
7	Legend Creator for thematic mapping	
8	A large library of symbols	
9	Rule Based Labelling and Annotation	
10	Geo-processing and Overlay Analysis	
11	Vector to Raster	
12	Advanced Report Generation with wizard	
13	The proposed software should support multiple document interface (MDI), User should be able to create multiple views in single project.	
14	The application framework of the software should be such that it should have Dockable/Floating Toolbars, Dockable and Auto Hiding Windows, Unicode	
15	Support for Multilanguage Attributes, Drag and Drop to Rearrange Tools/Toolbars, Create New Toolbars or Menus without Programming, Extend the Applications with Add-ins built with .NET, Java, or Python, Build New GIS Components with .NET or Java or other development platforms.	
16	The proposed software should have capability to create layer as per the data model defined by the authority. User should be able create table structure as per the requirement.	
17	The software should have provision for definition of map projection system and geodetic datum to set all the maps in a common projection and scale.	
18	It should have facility to create custom projection using 3 to 7 parameters.	
19	It should have the facility to display multiple projection coordinates on map click.	
20	The software should provide facility to click on any feature of the map and return a select set of attributes for feature i.e. Identify tool along	

	with pop-up.	
21	Software should have rich geo-processing functions such buffer generation, clip, erase, intersection, dissolve, union, polyline to polygon, etc. It should have facility to perform the spatial intersection analysis like plot area with buffer zone to calculate road-widening impact on adjacent land.	
22	The Software should be able to import / export data from / to various formats like .dwg, .dxf, .dgn, .shp (shape files), coverage file, .mif (MapInfo), .mdb (GeoMedia), .gml, .kml, .gpx, Geo PDF GeoJSON, interlis, GeorSS, SQLite etc.	
23	The proposed software should have function to import / export tabular data such as .xlsx, .csv, .dbf, etc.	
24	Support of IFC object for BIM applications.	
25	Integrated GPS module for desktop and mobile GIS.	
26	Support of Coordinate Geometry (COGO) description for GIS objects creation and store in GIS database.	
27	Facility to define joins between the two tables (graphic / non-graphic) of the database to get integrated information in the table and perform GIS analysis.	
28	The system should provide facility to exchange the GIS Data with other platform applications like Microsoft Word, and Excel to use GIS data and generate reports like graph and charts.	
29	Software should have rich display and navigation tools. It should have zoom in, zoom out, fixed zoom in, fixed zoom out, pan, real time pan, bookmark, Geo link multiple views, swipe, flicker, search by location, cross hair, cursor location value, numeric dump, query cursor etc. It should have support of continuous panning i.e. real time pan.	
30	Software should allow the user to perform undo / redo operations during edits.	
31	The software should have module for geo-referencing of vector and raster data.	
32	Facility to capture the geometry from the layout maps, Building maps by maintaining the coincident geometry i.e. when a new polygon is captured simply by selecting an existing polygon to digitize the common boundary thereby ensuring no slivers or gaps between adjacent area features like parcels.	
33	The software should provide a complete set of drawing & editing tools in order to enable the user to Draw & Modify any or parts of various geographical objects (point, line and polygon) on the map.	
34	The software should have topology creation tool to remove the topological errors from vector data.	
35	The software should have the ability to add data from internet or intranet users to the existing map data so that data from other	

	sources.	
36	The software should allow user to create layers or shortcuts to geographic data that store symbology for displaying features.	
37	A rich legend creation tool should be required in proposed application for thematic mapping. User should apply color and symbology using the attribute attached with the layer based on single, quantile and unique values functions.	
38	A rich annotation tool should be available such as add label, edit label, move label, rotate label, remove all label, etc.	
39	The software should have module of Dynamic Labeling and Rule based Labeling.	
40	The software should have a provision of hyper linking the GIS feature as well as its attribute fields with existing documents, URLs, Images, drawing files or scanned maps related to that feature.	
41	Software should have versioning capability for history tracking.	
42	Query builder tool should be available with the software to perform simple and complex queries.	
43	The customized application should provide the user facility to make dynamic queries on GIS GUI. The application should allow users to store and retrieve standard queries used by them in day to day operation.	
44	Software should have various query tools for queries based on attributes, location, etc.	
45	Software should have map composition / layout tool for printing spatial data at different scales and at adjustable print quality.	
46	Software should allow users to export results to various file formats like EMF, BMP, TIFF, JPEG, PDF, etc.	
C. Image Processing Functions		
1	Image Enhancement and Filtering	
2	Image Analysis Tools	
3	Image Geo-referencing	
4	Image Extraction and Mosaicking	
5	Atmospheric and Radiometric Correction	
6	Image Transformation	
7	Image Classification	
8	Advance Segmentation	
9	Advanced Change Detection	
10	Raster To Vector	
11	The proposed software should support HRSI (High Resolution Satellite Imagery) and low resolution satellite images (panchromatic & multispectral) such as IKONOS, Quick bird, Geoeye, Worldview, CARTOSAT, EROS, LISS-IV, LISS-III, AWIFS, RISAT-1, KALPANA-1, INSAT3A, INSAT3D, PROVA-V, etc..	

12	The software should have capability to process optical satellite data as well as microwave image data.	
13	The software should be capable to process and visualize the stereo pair data. It should be able to create DEM from stereo pair and perform ortho-rectification.	
14	The software should support images with More than 8 bits, 11 bit, 16 bits, and 24 bits per band.	
15	The software should support image format such .tif, geotiff, .img, .pix, .hdr, .h4, .h5, DTED, DEM, CEOS, .bmp, .jpeg, etc.	
16	The software should be also support LiDAR data file format such as *.las, *.isd, *.pcg etc...	
17	The software should have projection transformation tool to reproject the image from one projection to other projection system.	
18	Image extraction module should be available in the proposed software which can be performed by defining the extent, inquire box and polygon layer.	
19	The software should have module for image mosaicing and splitting.	
20	Geometric Correction and atmospheric correct module should be available to remove the geometric distortion in the image and atmospheric anomalies such as haze.	
21	It should have Layer stacking to create composite image from a number of band of the satellite imageries.	
22	The software should have image enhancement module to enhance the imageries. It should have enhancement algorithm such as	
23	Linear, Logarithmic, Histogram Equilize, Histogram Matching, Density Slice, Gaussian, Squire root, Tone Balancing	
24	The software should have Image filtering algorithm such as Convolution, Texture, Adaptive, Crisp, Laplacian, Statistical, FFT, etc.	
25	The software should have image transformation module such Vegetation Index, Principal Component Analysis (PCA), Inverse PCA, Pan sharpening, Wavelet fusion, etc.	
26	The software should have Natural Color image generation module using NIR, Red and Green band of high resolution multispectral image data. This module should have capability to stretch the natural color image into 8 bit.	
27	Proposed software should have image classification modules such as supervised and unsupervised classification along with image segmentation.	
28	The software should be capable to process the temporal or time series image data. The software should provide change detection module such as: Basic Change Detection, Advance Change Detection Auto Change Detection and Site Monitoring	

33	The advance change detection module should be capable to ingest multiple input images to find the change. It also handles the multi resolution satellite image along with mis-registration. It should supports various methods of advance change detection such as single band differencing, cross correlation, Image regression, Image ratioing, PCA, Change Vector Analysis (CVA), Magnitude Differencing, Vegetation Index Differencing, Tasseled Cap, Chi-Square, Unsupervised Change Detection, etc.	
34	The change detection module should have capability of Object Library Creation for Object Identification and Automatic Feature Extraction (AFE).	
35	The software should have functions like Linear Algebraic Combination, Change resolution, Bit Conversion, proximity analysis, etc.	
36	The software should have function called Dynamic threshold for analyzing change detection using image. This function is used to categorize the pixels in input image based on the threshold value.	
37	The software should have raster catalog and vector catalog tool for raster and vector data management.	
38	The software should have network analysis module to find the shortest and Optimum path using the topologically corrected road network.	
39	The software should have tools for terrain analysis and 3D analysis. The module should be able to create slope/aspect, hillshade, elevation profile, topographic normalize, line of sight, viewshed analysis.	
40	The software should have algorithm for surface generation such as Linear, IDW and Krigging.	
41	Software should support fully automatic and semi-automatic raster to vector conversion tools.	
D. Advanced Modules		
	Network Analysis	
1	Defining Network Rules	
2	Add Network Location	
3	Remove Network Location	
4	Find Shortest and Optimum Path	
5	Location Analysis	
6	Multi Location Analysis	
7	Service Area	
8	Dynamic Segmentation	
E. 3D Modelling		
1	Terrain Extraction	
2	Flythrough & Walkthrough Creation	
3	Drape Raster, Vector and 3D Object	
4	Line of Sight and Radio Line of Sight	
5	View Shed Analysis	
6	Stereo Viewing	

7	Environmental Effect Like Fog, Fire, Cloud, Sun, etc	
8	Particle emitter	
9	Save Image & Animation [*.avi]	
F.	Raster GIS Analysis	
1	Spatial Analysis	
2	Distance Tools:	
3	Math Tools	
4	Conditional Tools	
5	Extraction Tools	
6	Local	
7	Generalization	
8	Multivariate	
9	Neighbourhood	
10	Weighted Overlay	
G.	Terrain Analysis	
1	DEM to Contour and DEM from Point and Contour Line	
2	Slope and Aspect	
3	Hill Shade and Topographic Normalize	
4	Cut & Fill Analysis	
5	View Shed, Route Indivisibility and Line of Sight	
6	Best Path	
7	Area/Volume Calculation	
8	Hypsometry	
9	Semi Variance	
10	Surface Specification Points	
11	Anaglyph	
H.	Global Positioning System	
1	Interface with GPS device	
2	GPS Tracking and Navigation	
3	Extract feature using GPS	
4	Simulate GPS file	
5	GPS data validation	
6	GPS error correction	
7	Satellite sky-view	
8	Speed and Bearing Indication	
9	Way-Path generation and storing	
10	Geo-fencing	
11	Different File formats support	
12	Export to KML/KMZ	
I.	Tracking Analysis	
1	Simulate and analyse time-based data	
2	Report on patterns related to time and defined rules.	
3	Monitoring of mobile resources	

4	Analyse patterns of movement	
J.	Neural Network Classification	
1	Supervised	
2	Unsupervised	

5.9. Supply of COTS Enterprise GIS Software

Bidder will supply Enterprise GIS platform which will be installed on 16 Core Hardware Server (Hardware server will be provided by ASCL for installation).

5.9.1. Detail Specification of Enterprise GIS Platform

#	Functional Description	Compliance Status
General Functions		
1	OGC Certified	
2	User Management Tools	
3	Main Page Login, Registration, Forgot Password	
4	Map Tools	
	Vector and Raster Data Support (Display)	
	Zoom In	
	Zoom Out	
	Zoom to Extent	
	Previous View	
	Next View	
	Pan	
	Zoom to box	
	Book Mark	
Layer Visibility on/off		
5	Data Management Tool	
	Data Import and Export	
6	Measure Tool	
	Measure Distance	
	Measure Area	
7	Advanced Tools	
	Select Tool	
	Unselect	
	Identification	
	Buffer	
	Get XY coordinates	
	Find XY coordinates	
Labelling		
8	Query Tools	
	Basic Query	

	Feature Query (Spatial and Non Spatial)	
	Advance Query	
9	Spatial Editing Tools	
	Feature Creation	
	Add Feature	
	Edit Feature	
	Delete feature	
10	Non Spatial Editing Tools	
	Attribute Information Editing	
11	Printing Tool	
12	Report Generation Tool	
13	Should support std DBMS like SQL, Oracle, Postgres	
14	Geo-processing	
15	Versioning	
16	Network Analysis	
17	Developer SDK	
18	Data Publishing	
19	Real Time Data Support	
20	Should support WMS, WFS, WCS	
21	Seamless Data Handling	
22	Online Spatial Data Creation and Updation Support	
23	Should support internet, intranet, cloud	
24	Multiuser data editing	
25	The GIS server should be based on a Services Oriented Architecture (SOA).	
26	Should support Java /VB Script, .Net etc. and other latest technologies.	
27	OGC certification and capability to serve and consume OGC complied web services including WMS, WFS, WCS, CSW, INSPIRE, etc.	
28	Should be based on 64 bit architecture or better.	
29	Should support Windows/Linux platform.	
30	Should be able to support broad range of clients including Interoperability and browsers, desktops, Mobile Handsets.	
31	The application should be highly interoperable with the ability to import and export to a wide range of industry standard formats including CAD (DGN, DXF,DWG), ArcGIS geo databases, Geo Media Warehouse, MapInfo, GML(GEOGRAPHY MARKUP LANGUAGE) , XML, SHP, ArcInfo Coverage, ESRI Arc Info Export (EOO), Micro Station V7/V8, Geo PDF GeoJSON, interlis, GeorSS, SqlLite etc.	
32	Should support unlimited number of Editing and viewing clients. It should also allow multiuser editing with Advanced Editing Functionalities.	

33	Should support standard Web server/application server like IIS, Apache, Tomcat, Oracle HTTP server, etc.	
34	Should supports unlimited Desktop client connection. Desktop GIS applications with the capability to consume WMS/ WFS services should be able to connect and use data from the server.	
35	Should support multiple DBMS for database storage including Oracle, DB2, SQL Server, Postgre SQL, Informix, Windows Azure SQL Database, IBM Netezza, Tera data.	
36	Should be capable of maintaining data history, version management and conflict detection / resolution.	
37	Should have geo-processing framework, geo-processing core analysis functionalities, spatial and statistics analysis functionalities.	
38	Should have capability of centrally managed data, models, tools, maps and applications.	
39	Should have the capability to link documents like Adobe pdf, word/power-point JPEG, GIF, PNG, DTED and TIFF files etc to map features.	
40	Should support database check in-check out/replication functionalities hence maintaining the parent child relationship of Master Database.	
41	Should have open access to extensive GIS capabilities so as to enable organizations to publish and share geographic data(2D&3D),maps, analysis tools, Manipulate data, 3D models etc.	
42	The publisher should have capability to publish the project/data on GIS server and enable OGC services such as WMS, WFS, WCS and CSW in the data layer.	
43	All the Geo-processing and Image processing function such as buffer creation, clip, erase, image enhancement, image filtering, Vegetation Indices Calculation, Linear Algebraic Combination, Band Math, change detection, image extraction, mosaicing, etc should be performed at server end by sending the request using the web client and should enable the WMS service to display the processed data on web.	
44	Application Server must support Time aware data for Trends / Time Series Analysis. Application Server must support network and perform Routing analysis, Service Area Analysis, and Tracking Analysis.	
45	Should support for GML, RSS (Real Simple Syndication) and KML/KMZ (Keyhole Markup Language).	
46	The server should have in built map caching capability.	
47	It should provide imagery access quickly after acquisition with dynamic mosaicing and on- the-fly processing.	
48	Should support standard Web server/application server	

49	Should have Web Application Functionalities like pan, zoom, identifying features on a map, feature based hyperlink, measure distance, overview window, find place, query attribute, search attribute, editing and geo processing task.	
50	The software should allow visualization of data in 2D, 3D in web as well as desktop application.	
51	The application should support LDAP (Light weight Directory Access Protocol) or Active directory based authentication.	
52	Control user access and credentials to data by assigning roles.	
53	Hide data completely, prevent manipulation, or allow editing, based on role Compartmentalize data based on accessibility.	
54	Define which groups of users can view and access data through Discretionary Access Control (DAC).	
55	Logging records all transactions including log-ins, searches, downloads, uploads, edits, and deletions.	
56	Should support Single sign-on, authentication module.	
57	Should support SSL and signed certificates to ensure complete security from browser to server.	
58	Should enable a secure, private sharing of confidential data that can be deployed on private network to promote collaboration on maps and applications within the organization.	
59	Support to Connect securely Operate the Web application over a Hypertext Transfer Protocol Secure (HTTPS) Connection. Optional Lockdown mode to remove anonymous access and require all users to log in.	
60	Should provide a web publishing wizard so that registered users can publish websites without coding/programming.	
61	Should be able to create and manage groups to control publishing the data and its services on Data store/workspaces.	
62	Should have the facility of customizable reports and map layout as per the requirements.	
63	Print server application for online printing in different formats with desired GIS Map scale and customized templates.	
64	Platform for GIS Application Software should be able to operate on Windows	

65	The proposed software should have functions of GIS and Image Processing along with advance functions such as network analysis, terrain analysis, 3D analysis, change analysis, etc.	
66	GIS Software must allow authority to implement a centrally managed GIS providing the advantage of lower cost of ownership through single, centrally managed, focused GIS applications (such as a Web application) that can be scalable to support multiple users and saves the cost of installing and administering desktop applications on each user's machine.	
67	Proposed customized GIS Application Software should be able to integrate with the eGovernance Solution being developed at authority.	
68	The web based GIS software shall be usable for viewing the GIS data over internet/ intranet and shall be functional with all type of standard browser like Internet Explorer®, Apple® Safari, Google™ Chrome, Mozilla® Firefox®, etc. The database shall be developed on any standard RDBMS.	
69	ODBC compliance enabling interface with RDBMS like Oracle, SQL server, Access etc. should be available.	
70	GUI shall be highly user friendly, self-explanatory and eye catching. It shall provide the sample example wherever it seeks user input and also preserve the history of the inputs. GUI can be made good looking and beautiful by making use of good color scheme and putting functions indicative image (drawing) on button.	
71	The proposed GIS software could be any Industry standard COTS GIS platform and should be easy to handle, operate, maintain & also train the authority staff/end users.	
72	The customized software for authority should have simple user interface both for departmental users as well as for citizens with easy navigation and querying facility.	
73	On-line help shall be provided at all functions and tools.	
74	The proposed software should be OGC compliant and follow the interoperability.	
75	The software should support OGC Services such as WMS, WFS, WCS, CSW, INSPIRE, etc along with GML, KML, etc.	

76	The software should support all types of raster formats and services like ERDAS IMAGINE, ENVI, PIX, DTED, DEM, CEOS, JPEG, JP2, PNG, GeoTIFF, & Web Coverage Service (WCS, OGC standard), Web Map Service (WMS), OGC standard.	
77	Should be able to support broad range of clients including browsers, desktops, Mobile Handsets, Palmtops, Tough books, etc.	
78	Data Preparation Image Processing	
79	Create Blank Image	
80	Reproject	
81	Image Statistics	
82	Subset Image	
83	Subset Image using Vector Polygon	
84	Split Image	
85	Mosaicking	
86	Layer Stacking	
87	Fill Area Using Vector Polygon	
88	Data Analysis	
89	Look up Table Update	
90	Image Enhancement	
91	Linear	
92	Gaussian	
93	Logarithmic	
94	Density slice	
95	Square Root	
96	Histogram Equalize	
97	Histogram Matching	
98	Tone Balancing	
99	Image Filtering	
100	Texture	
101	Adaptive	
102	Crisp	
103	Statistical	
104	Convolution	
105	Image Classification	
106	Unsupervised Classification	
107	Supervised Classification	
108	Threshold	
109	Generate Statistics of ROI/ Create Signature File	
110	Post Classification Smoothing	
111	Contingency Matrix	
112	Signature Reparability	

113	PCT Edit	
114	Scatter Plot	
115	Class Information	
116	Fuzzy Classification	
117	Fuzzy Convolution	
118	Segmentation	
119	Change Detection	
120	Cut and Fill Analysis	
121	Conversion	
122	Raster To Vector	
123	Vector To Raster	
124	Raster GIS Analysis	
125	Spatial Analysis	
126	Distance Tools	
127	Generalization	
128	Neighbourhood	
129	Weighted Overlay	
130	Zonal Tools	
131	Record by Vector	
132	Locate DEM Position	

5.10. Design and Development of Enterprise Web GIS Smart City Department Application

Bidder will Design and Develop web GIS application for ASCL using Enterprise GIS platform. This application will cater to the viewing, analysing, & utilizing the Geographic Information needs of the different departments of ASCL. And will also play a role of decision support system and Backbone for Smart City Command Control System

The required features to be developed for web GIS application is as follows:-

- 1) Will be based on Enterprise GIS Platform
- 2) OGC Open Geospatial data standards compliant
- 3) Existing Server, Client, Web, Mobile / Tablets to be supported
- 4) Application will be open to integrate additional functionalities in future
- 5) Visualization of data e.g. Land Parcel Data DEM on Satellite Image
- 6) will support multiple relational database connections
- 7) Shall have query based results
- 8) Application will have facility of Historical data analysis for Land parcel information, property tax information, building information using time series
- 9) Will support distributed transaction. This allows multiple users to edit the map data at a same time
- 10) Application will support DBMS spatial index and R- tree index for better system performance
- 11) Creation of server clusters with load balancing and fail-over functionality will be supported

- 12) Application will support data compression and asynchronous map view, static & dynamic cache
- 13) Application will have facility to configure additional menus for future functionality
- 14) User authorization and authentication should be GUI based
- 15) Application will have the facility to monitor application operations and status: Logged in user status, server load, data access status
- 16) Application will have the facility to create custom GUI without business customization through designated application the selected bidder is expected to follow the complete SDLC for the development of the GIS application
- 17) Proposed/Developed GIS Application software will follow National Spatial Data Infrastructure (NSDI) Meta standards and should be compatible with National Urban Information System (NUIS) Scheme. Tightly integrate the spatial data with the existing system at ASCL.

The Smart City Application should have following Modules

	Department Modules
1)	GIS Module for Estate Management
2)	GIS Module for Parks and Gardens
3)	GIS Module for Water Supply
4)	GIS Module for Sewerage Operation
5)	GIS Module for Road and Traffic
6)	GIS Module for Storm Water Drainage
7)	GIS Module for Street Light Management
8)	GIS Module for Education
9)	GIS Module for Health Services
10)	GIS Module for Advertisement and Hoardings
11)	GIS Module for Disaster Fire & Emergency Services Management
12)	GIS Module for Capital Project Monitoring and Control

5.10.1. Modules and Sub Modules of Land and Estate Management System

Map Handling Module: User can view municipal plot details along with plot dimensions, details of heritage structure with buffer analysis and ward, village and election boundaries. He/She can also view and assess the area under slum and location of ULB owned vacant lands. Upload GIS / CAD Drawing on the system for Permission

Municipal Service Query Module: Query module will support users to access details about the Plan and Gap analysis. Query system will also support user to see information based on plinth area, floor wise details.

Spatial Query Module: This will support user to analyze area under slum and the zone, ward and other information regarding location of vacant land of ULB.

Reports: Reports will be generated Building Permission / Building Use Certificate

5.10.2. Estate Management

This solution will help ASCL officials to manage the estate related information along with analysis of slum area and ULB owned vacate land.

Modules and Sub Modules of Land and Estate Management System:

Map Handling Module: User can view municipal plot details along with plot dimensions, details of heritage structure with buffer analysis and ward, village and election boundaries. He/She can also view and asses the area under slum and location of ULB owned vacant lands.

Municipal Service Query Module: Query module will support users to access details about encroachment and legal information of plots. Query system will also support user to see information based on plinth area, floor wise details.

Spatial Query Module: This will support user to analyze area under slum and the zone, ward and other information regarding location of vacant land of ULB.

Reports: Reports will be generated queries results based on city survey number, built-up area, plinth area, floor details, date of possession, details of encroachment, slum details, ward boundaries etc.

5.10.3. Disaster Fire & Emergency Services Management

This system will enable user to do the advance planning of all possible disasters to control the situation effectively and rapidly locating the incident location which requires immediate rescue and administrative support.

Map Handling Module: In map viewer user can view all required spatial features such as road plan including lanes and by lanes, position of water hydrants, high rise buildings, and location of fire stations along with other relevant layers.

Incident Locating & Tracking: To track incident location in a faster manner this module will provide intelligent location search by implementing fuzzy logic to search the location input by user without matching the exact words system will show the possible matches as per input given by user. User can relate the information and zoom to the location as required.

Query Module: This module will help user to access information about necessary emergency services such as nearby fire stations, police stations, hospitals and other related information.

User can also get information about facilities available in hospitals such as no of beds etc. Query module will also provide information current project status.

Spatial Query Module: Spatial query module will enable user to perform nearest neighbour analysis to find out closest facility available from incident site, also spatial routing will enable users to find out shortest path to display transportation routes for responding equipment's with commutable roads.

Reports: Reports will be generated on queries based on location of numbers of nearest health care centres, hospitals; those are nearest to the incident occurred.

5.10.4. Park and Gardens Management System

This solution will enable ASCL officials for effective management of development sheet with the garden department. It will provide detail information about the garden and parks available in the city such as location detail, garden area number of trees etc.

Map Handling Module: In this module Map viewer will show garden and parks, stadium location and plot boundaries which can be measured with the help of measuring tool on the map interface. User can also view other associated information such as number of trees, services availability, water bodies inside the garden, and shopping area details.

Query Module: Query module is designed to provide maximum information associated with garden and parks, user can locate all parks and garden and open spaces through query search and then zoom the exact location of selected garden and park on the map viewer. He / She can extract information about number of taps provided in park/ garden.

Spatial Query Module: This module will enable user to perform buffer analysis to get information around park /garden as well as services availability such as water connection, sewerage facility, telephone etc.

Reports: This module will allow the users to generate report on query results based Number of public taps provided, Lease period/ adoption period with expiry date of Lease or adoption of individual Park/Garden.

5.10.5. Water Management System

It will enable user to identify, isolate, and map areas of concern during a leak or outage. He / She can also trace the network to identify customers who are downstream of a main break, complete valve isolation traces, create leak reports, and reroute resources in an outage with detection of spots where leakage in the pipe have occurred. Through GIS system user can communicate leak or outage information with customers and related agencies such as public works and water companies. System will create all city water pipe line networks along with diameter and valves information to calculate flow and pressure at junction.

Map Handling Module: Map viewer will show entire water pipeline network along with valves in legends user can view information related to diameter, length, and depth of a particular water line segment. User can also view different water bodies such as Lake, open wells, bore wells etc. User can click on the water pipeline segment to know the material and condition of pipe.

Routing and Utility Network: Routing will enable user to find out shortest route from source to the particular pump station.

Query Module: User can extract data through queries base on diameter of pipelines and resultant can further be select to see position of valves on the select water pipe line. Depth of pipeline from road level and inverted level can also be fetch through queries. He / She can locate all water bodies and valves throughout the municipal area along with details like maintenance history, repair and replacement of water pipeline and type of material of construction.

Spatial Query Module: This sub module will allow user to get population statistics of the selected area and generate buffer along with water pipeline to analyze nearby other utilities in the area.

Reports: This will allow the users to generate report on query results based on numbers of Leakage spots, pipe having more numbers of leakage spots etc. and also will allow Selection of the diameter of pipeline based on the, population statistics of the area, Lines of diameter and above/ below, Lines of diameter and above/ below, depth of pipeline from road level and invert level, repairs/replacement history, types of material, location of valves with select material of construction etc.

5.10.6. Sewerage Operation

This system will support ASCL officials to manage collection treatment and disposal of sewerage effectively by using GIS application. User can plan and track maintenance schedule of sewerage lines, calculate flow capacity based on diameter of sewage pipeline along with overall capacity of sewer line.

Map Handling Module: On map viewer user can view entire network of sewerage pipeline, he/she can also run network trace and could view the output on the viewer part of the application. Position of manholes will also be shown as point location on the map.

Query Module: User can execute queries base on diameter of pipeline, material of construction, slippage in maintenance schedule flow capacity and status of pumping mains, shutdown status, present capacity of sewer line, locations of landfill, transfer stations and waste handling facilities etc.

Spatial Query Module: With spatial query user can get the details of bypass line direction of flow, position details of ventilation column, User can also run sewerage line network trace between two points and view result on map viewer.

Reports: Reports will be generated on queries on type manholes including depth and size, slippages in Maintenance schedule, flow, capacity and Current status of pumping mains, status of shutdown in attribute attached etc.

5.10.7. Road and Traffic Management

It will enable ASCL users to planning and tracking of maintenance of all roads with in the municipal limits including all types of bus stands, taxi stands, and petrol pumps. The application system will enable users to identify position of road divider, position of U-turn boards and speed breakers, number of speed breakers in a stretch, and road partition along with road street light information.

Map Handling Module: Map viewer will show all the roads within the municipal limits of ASCL with footpath surface as well as it will show traffic lights as point location. User can identify bus stand, bus route, and petrol pumps location on map.

Query Module: With queries user can identify position of road divider, U-turn boards, and speed breaker, road partition for light and heavy vehicles, number of street lights, and number of speed breakers on stretch of a road. User can also query bus stand, bus routes, location of petrol pumps.

Routing & Network: Routing will enable user to find out alternative route in case of Jam, emergency or certain festivals, user can also user routing for identifying routes of all petrol filling vehicle.

Spatial Query Module: Spatial analysis will enable user to get information of speed breaker, number of street lights and other relevant features based on selected area.

Reports: It will be generated on query results based on getting numbers of street lights per km in a road, number of speed breakers on a stretch of road, Identifying roads with number of street lights less than per km.

5.10.8. Storm Water Drainage Management System

This solution will enable users to perform effective management of storm water drains.

Map Handling Module: Map viewer will show main town level drains with thematic view based on their type such as “Nalla” or “Outfall” along with cross sections.

Query Module: User can perform queries based on size, slope, and materials of drains. Maintenance schedule data can also be extracted for effective tracking of De-silting achievements.

Spatial Query Module: Through spatial queries user can locate cross section of all drains with details like width and depth levels.

Reports: Reports will be generated based on the queries on details of cross-section of all drains with clear width and depth levels, and information about type of drain.

5.10.9. Street Light Management System

It will enable ASCL users to planning and tracking of maintenance of all street lights with in the municipal limits including all types of street lights, traffic signals, high mast lights, installation policy and Failure Statistics . The application system will enable users to identify position and numbers of street lights, high mast light, traffic signals on road and partition along with road street light information.

Map Handling Module: Map viewer will show all the roads within the municipal limits of ASCL with high mast lights, street lights it will also show traffic lights as point location.

Query Module: With queries user can identify position and numbers of street lights per km in a road, Identifying roads with number of street lights less than per km, traffic signals, and high mast lights on stretch of a road. User can also query Failure Statistics, installation policy etc.

Spatial Query Module: Spatial analysis will enable user to get information of traffic signals, number of street lights, within the buffer area or within the ward boundaries of the municipal limits and other relevant features based on selected area.

Reports: It will be generated on query results based on getting numbers of street lights per km in a road, number of traffic signals on a stretch of road, Identifying roads with number of street lights less than per km and failure statistics analysis based on user input to the GIS application.

5.10.10. Capital Project Monitoring and Control

This module will capture request coming for development project in SMC like Road repair, New Road Constructing, Building Construction, Flyover Construction, Toilet Construction, Park / Garden Construction, Laying of sewerage Line, Laying of water Line , Laying of Strom Water Drainage etc

Request for all development projects can compile and a proper GIS view will be provided to do analysis on exiting geo location and requested project so that decision can be taken looking at GIS View for suitability of the project.

Once its decided that project is feasible, approved for Implementation the same project can be monitored and controlled through application by incorporating GIS / project Work in Progress through GPS base Tagging and GPS enabled Photos etc. and Functions for analysis like Buffer, Measurement, Vector over lay, Colour Symbology. With following sub modules:

- 1) Project Analysis and Decision support System for project as request
- 2) Project Analysis and Decision support System for project as plan

- 3) Project Analysis and Decision support System for project work in progress
- 4) Project Analysis and Decision support System for Final

5.11. Integration GIS with existing and proposed/future Smart Systems

- 1 Video Surveillance System
- 2 Smart Lighting
- 3 CT Enabled Solid Waste Management
- 4 Intelligent Transportation System
- 5 Smart Education
- 6 Smart Water Supply System
- 7 Smart Health Management System
- 8 BRTS/MRTS and City Bus Services
- 9 Public Bike Sharing
- 10 Central Command Control Centre
- 11 Smart Parking Management System
- 12 Environmental Sensors
- 13 Enterprise Project Management
- 14 Any other Municipal e-Governance Application
- 15 Incident – response management

6. Component 6 : Environmental Sensors

6.1. Project Intent

Smart environment sensors will gather data about pollution, ambient conditions (light, noise, temperature, humidity and barometric pressure), weather conditions (rain), levels of gases in the city (pollution) and any other events on an hourly and subsequently daily basis. It is for information of citizens and administration to further take appropriate actions during the daily course/cause of any event.

6.2. Functional Specifications

- 1) The environment sensors should have the following capabilities:
 - I. They should be ruggedized enough to be deployed in open air areas, on streets, roads, coastal areas, parks etc.
 - II. They should be able to read and report at least the following parameters: Air-Quality, Sun Light, Noise, Weather conditions etc.
- 2) Smart environment sensors will notify and allow citizens and administrators to keep a check on their activities which impact the environment and enable the city to take remedial action if required.
- 3) These environmental sensors can be connected via 3G/4G wireless network or Wi-Fi/LORA networks based on connection availability.
- 4) The data should be collected on a data analytics cloud application. In addition, the data should be integrated in third party CCC (Command and Control Centre) Software. Various environment sensors shall sense the 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. The platform must include intelligent analytical engines that make information meaningful to all stakeholders and helps ease decision making.
- 5) The environmental data should be submitted in a print ready PDF report format on daily, weekly and monthly basis to at least 5 designated email of the authorities of various departments.
- 6) In a situation where environmental deterioration crosses a threshold limit set by the concerned authorities in the software system, the system should be able to notify the concerned authorities of various departments by means of SMS and E-mails.
- 7) MSI can also make use of the Nearby Variable Messaging Displays wherever possible (need to be finalized post detailed survey of locations).
- 8) The sensor management platform should allow the configuration of the sensor to the network and also location details etc.
- 9) The sensors should be able to be managed remotely. This includes sensors being updated with calibration parameters and software upgrades.
- 10) Apart from information provision, the sensors must ensure data is transmitted securely and have security measures from sensors to the software platform. It must also ensure tamper alerts are provided in cases of vandalism, security breaches, etc.

6.3. Technical Specifications

Sr. No.	Parameter	Specification
1	Measurement parameters and range (must measure required ranges)	PM 2.5: 0 to 600 micrograms / m ³ PM 10: 0 to 900 micrograms / m ³ NO ₂ : 0 - 10 ppm (minimum detection 10 ppb) SO ₂ : 0 - 10 ppm (minimum detection 10 ppb) O ₃ : 0 - 5 ppm (minimum detection 10 ppb) CO: 0 - 500 ppm (minimum detection 100 ppb) Light: up to 50,000 Lux UV Radiation: up to 50,000 uW/cm ² Noise: up to 135 dB (A) Rainfall Monitoring : in inch/mm of rain per day (Upto 40 inch)
2	Temperature, Humidity and Atmospheric Pressure Sensors	Real-time Temperature Range: outdoor -10°C ~ 70°C Real-time in Air Humidity Level 0-100% RH Real-Time Atmospheric Pressure (in Bars or millibars)
3	Connectivity (Minimum)	GPRS (2G) / GSM (3G) / LTE (4G) / Wi-Fi / LORA Sensors shall have provision to interchange between GSM and LORA.
4	Power	The sensor should be consuming power as low as 3 Watt and fully operated using Solar Power with minimum of 24 Hours of Battery Backup.
5	Data Frequency	Each environmental sensor should be sending data every 120 to 600 seconds. The data frequency should be changeable from sensor management platform.
6	Measurement Principle	The sensors should be measuring air-quality and noise parameters from downward (ground) direction to capture vehicular pollution and noise. The sensors should be measuring light parameters from top direction to capture maximum sunlight. The sensors should be measuring particulates from the sideward direction to avoid the effect of gravity on the measurement.

7	Measurement Flow-rate	<p>The system should have a suction based air measurement system.</p> <p>For Particulate monitoring should be having 1 Liter / Min as the minimum required flow rate. Where for Gas monitoring should be having 100 ml/min as the minimum required flow rate.</p>
8	System backup	<p>The system should have an internal memory for the data backup for minimum 7 days in case of network failure or system maintenance cycles</p>
9	Sensor Configuration and Geo-tagging	<p>Smart environmental sensors should be centrally configurable and updated from Command and Control Center Software.</p> <p>Geo location tagging of each environmental sensor should be done from Command and Control Center Software.</p>
10	Weather Protection	<p>The mechanical enclosure should be weather resistant with IP65 grade protection.</p>
11	Mechanical Enclosure	<p>Smart Environment Sensor System should be inside a single enclosure (keeping only necessary parts outside for measurement constraints) without exceeding exterior dimensions 400mm X 400mm X 250mm for better aesthetic value.</p> <p>Mechanical Enclosure should be made of tamper proof material preferably engineering metal.</p>
12	Data Validation (OPTIONAL)	<p>Every sensor data should be validated by Nationally accredited environmental laboratory with certification and test-report before installation.</p>
13	Quality Certification	<p>The Hardware manufacturer should be having Quality standards with ISO-9001-2015 and Environmental Standards with ISO-14001-2015.</p>

7. Component 7 : Data Centre (DC) and Disaster Recovery (DR) Centre

7.1. Introduction

The 'Data Center' (DC) infrastructure catering to all the Components & features of the Agra Smart City – ICT Solutions, will be co-housed in the building identified by ASCL which will be provided to MSI with requisite space and electric power depending on the requirement as per the proposed solution of MSI. The MSI shall be required to undertake a detailed assessment of the requirements at the identified location and commission all the necessary ICT and non-ICT infrastructure which also add civil/ electrical work as required.

The Data Centre wherein all the ICT infrastructure along with the network infrastructure are installed. The data center will host all the software applications for various smart city components. The Data Centre shall provide the private cloud like functionalities which allows agility, seamless expansion which is non-disruptive and help infuse the new technologies into the existing landscape as and when available. The data center to have adequate provision for data security through implementation of firewall, IPDS, antivirus system, etc. the Physical access to the data center shall be managed through a biometric access system.

The Disaster Recovery Centre is a mirror image of all the application hosted at the data center & will be 50% of the Compute however the data of video feeds is to be 100% available in case of Disaster. In case of non-availability of data center, the DR center should be able to operate all the applications for the smart city components. The DR center will have all the functionality and infrastructure similar to the data center.

Disaster Recovery Centre will be 50% of Data Centre Site, it is mandatory to have two separate physical location and distance itself through Seismic Zones.

7.2. Design, Configuration, Installation and Commissioning of DC and DR

1. MSI shall be responsible for detail designing and Solutions architecture of required Infrastructure, setup, applications of ASCL and premise shall be software defined data center which has zero dependency on the proprietary hardware.
2. Understanding the existing Infrastructure, setup, software, applications of ASCL and planning for DC-DR solution
3. MSI must ensure that virtual machine is into separate network tenant and virtual LAN. Also, Micro segmentation shall be part of solution architecture which enables the fine grained security policies to be assigned to data center applications down to workload level.
4. MSI must ensure that virtual machines are having private IP network assigned to VM.
5. MSI must ensure that all the managed hosted VMs are in same network segment (VLAN) even if they are spread across DC-DR
6. In case of scalability like horizontal scalability, the MSI should ensure that additional require network is provisioned automatically of same network segment.
7. MSI must ensure that ASCL gets ability to map private IP address of VM to public IP address as require from portal

8. MSI must ensure that public IP address of VMs remains same even if VM gets migrated to another datacenter due to any incident.
9. MSI must ensure that public IP address of VMs remains same even if VM network is being served from DC-DR
10. MSI must ensure that the public network provisioned for VMs is redundant at every points.
11. MSI must ensure that VMs are accessible from ASCL private network if private links P2P/MPLS is used.
12. MSI must ensure that there is access to VMs if there is a requirement to access it using IPSEC/SSL or any other type of VPN.
13. MSI should ensure that VM network is IPv4 and IPV6 compatible with segregated ports.
14. MSI should have provision of dedicated virtual links for data replication between their multiple datacenter in order to provide secure data replication for DR services.
15. MSI should ensure use of appropriate load balancers for network request distribution across multiple VMs.
16. MSI shall propose the system which has the capacity planning built into the system which provides ASCL the transparent view of the system resources used and required for future expansion.
17. MSI shall provide the capabilities to assign role based access and ability to templatelize the VM, Application based on the workload.
18. MSI shall propose the system which has ability to define redundancy level for each workload across the cluster.
19. Reduction in data center footprint over traditional siloes architecture for power, cooling and space savings.
20. MSI shall require while architecting the solution which works on the software defined data center conceptualization inside the firewall & further workloads which cannot be virtualized on bare metal or physical server that shall be used for the software defined storage pool.
21. MSI is required to locate all hardware/software and related items as per design offered for smart city infrastructure including SLA monitoring and Help desk management, in above data Centre complying with standard guidelines as per Telecommunications Infrastructure UPTIME/TIA-942.
22. Data Centre shall be available for 24 x 365 operation.
23. Smart city infrastructure shall have built in redundancy and high availability in computing and storage to ensure that there is no single point of failure.
24. MSI shall submit to ASCL adequate documentation/ evidences in support of the choice of the data Centre to meet the project requirements.
25. Minimum Guiding factors for selection of Data Centre: Following are benchmark requirements which should act as guiding factors for MSI to select and propose locations for Data Centre
 - I. There should be dedicated rack space available in the Data Centre for entire smart city solutions / infrastructure.
 - II. Access to Data Centre Space where the Smart City Project Infrastructure is proposed to be hosted should be demarcated and physical access to the place would be given only to the authorized personnel
 - III. Racks to be caged.

- IV. Smart City Data Centre should be as per Telecommunications Infrastructure Standard for Data Centre and should be 27001 Certified. The required certification to be enclosed along with the technical bid response.
 - V. It should have access control system implemented for secured access.
 - VI. Indoor CCTV Cameras would be required to be installed to monitor the physical access of the system from remote location
 - VII. If required, it should be possible to depute police personnel for physical security of the premises.
26. Video feeds shall be stored for 30 days online/real-time and shall be securely archived for 1 year which is flagged or is registered in evidence. The transaction data for minimum 1 year shall also be stored within the Data Centre infrastructure.
27. In case the Data Centre services are to go down due to any unforeseen circumstance, the Command Centre should have access to video feeds of previous 30 days and transaction data for min 1 year from this data backup facility.
28. Access logs to be stored for entire duration of contract and handed over to ASCL upon termination/expiry of the contract.
29. MSI must provision for storage and availability of archived/flagged video data of incidents and events on an archival server at the Police Control Room. Admin/Operator in the Police Control room should have access to this data through client workstations or web enabled clients.
30. The operator should be able to export archived video directly from the archival server and produce the same when needed in court of law or for other requirements.

DC Minimum characteristic:

- 1) Data Centre Availability: The availability of data from the hardware at a location must be guaranteed to 99.982% availability.
- 2) Redundancy and concurrent maintainability. It requires at least n+1 redundancy as well as concurrent maintainability for all power and cooling components and distribution systems. Any such component's lack of availability due to failure (or maintenance) should not affect the infrastructure's normal functioning.
- 3) No more than 1.6 Hours of downtime per year
- 4) N+1 fault tolerant providing at least 72-hour power outage protection
- 5) All IT equipment should be dual-powered and fully compatible within the topology of site architecture.

Data Centre shall primarily be divided into two zones:

- 1) Server Infrastructure Zone: This zone shall host servers, server racks, storage racks and networking components like routers, switches to passive components. All the Data Centre LAN connections shall be provided through switches placed in this area. Access to this zone, where the surveillance project IT infrastructure is hosted, shall be demarcated and

physical access to the place shall be given only to authorized personnel. Indoor CCTV Cameras shall be installed to monitor physical access of the system from remote location.

- 2) UPS and Electrical Zone: This zone shall house all the Un-Interrupted Power Supply units, Main Power Distribution Units (PDUs) to feed the components such as PAC, UPS, lighting, fixtures etc. This shall also house all the batteries accompanying the UPS components. As these generate good amount of radiation, it is advised to house these components in a room separate from server infrastructure zone.

7.3. DR Plan and Implementation

Disaster Recovery as a Service

1. MSI shall avail hosting services from MEITY Empanelled Cloud Service Provider to host DR site in addition to implement and manage the architecture accordingly.
2. MSI is responsible for Disaster Recovery Services so as to ensure continuity of operations in the event of failure of primary data center meet the RPO (Recovery Point Objective) and RTO (Recovery Time Objective) requirements.
3. RPO should be less than or equal to 1 hour i.e. the replication cycle should run at maximum 1 hour that needs to be reconsidered as it will be dependent on application to application.
4. RTO shall be less than or equal to 4 hours.
5. During the change from Primary DC to DR or vice-versa (regular planned changes), there should not be any data loss.
6. Support for synchronous and asynchronous data replication.
7. Automated site to site failover and failback.
8. Support for non-identical server and storage configurations at the remote site.
9. The Primary Managed hosted DC-DR should be in different seismic zones.
10. MSI should provision VM's for both DC and DR.
11. During normal operations, the Primary Data Centre will serve the requests. The Disaster Recovery Site shall will not be performing any work but will remain on standby.
12. During this period, the compute environment for the application in DR shall be available on demand basis for a functional DR and minimum compute if required, as per the solution offered. The application environment shall be installed and ready for use.
13. DC Data shall be replicated on an ongoing basis at DR, as per designed RTO/RPO and replication strategy, data consistency and integrity should be maintained
14. Database should be in Active mode at DC and Passive mode at DR, data consistency and integrity should be maintained.
15. In the event of a site failover or switchover, DR site will take over the active role, and all the requests will be routed through that site. Application data and application states will be replicated between data centers so that when an outage occurs, failover to the surviving data center can be accomplished within the specified RTO. This is the period during which the Compute environment for the application shall be equivalent to DC. The installed application instance and the database shall be usable and the same SLAs as DC shall be provided. The use of this Full Compute DR environment can be for specific periods during a

- year for the purposes of DC failure or DR Drills or DC maintenance or DC Major Software Upgrades or DC High Peak Load Support.
16. Self-remediating security implementation which allows systems to revert back to approved security state at designated interval.
 17. Website and live application (both external and internal) should be routed seamlessly from MHDC site to MHDR site.
 18. The MSI shall conduct DR drill one in every six months, of operation wherein the Primary DC has to be deactivated and complete operations shall be carried out from the DR Site. However, during the change from DC to DR or vice-versa (or regular planned changes), there should not be any data loss.
 19. The MSI shall clearly define the procedure for announcing DR based on the proposed DR solution. The MSI shall also clearly specify the situations in which disaster shall be announced along with the implications of disaster and the time frame required for migrating to DR. The MSI shall plan all the activities to be carried out during the Disaster Drill and issue a notice to the Department at least 15 working days before such drill.
 20. RPO monitoring, Reporting and Events Analytics for the Disaster recovery solutions should be offered as part of the offering. Any lag in data replication should be clearly visible in dashboard and alerts of same should be sent to respective authorities.
 21. Training should be provided to the staff members and System Administrator on DR.
 22. Services provider should provide the solution document of DR.
 23. Selected bidder should have proper escalation procedure and emergency response in case of failure/disaster at DC.
 24. Selected bidder shall provide support for all server maintenance activities. This would include periodic health check, on-demand troubleshooting, etc. from certified vendors. ITIL processes named problem, change, incident & configuration will be followed by selected bidder at DR site.
 25. Selected bidder shall provide Disaster Recovery services during the event of Disaster.
 26. The Selected bidder shall configure all the components and sub-components for end-to end user access to all Windows applications/services.
 27. The Selected bidder will have to demonstrate the DR site to run on thirty percent capacity for proving successful implementation of the DR site.
 28. ASCL reserves the right, on its own or via a third-party auditor, to conduct overall testing at any point of time for the services delivered by the selected bidder.
 29. The selected bidder shall make provisioning of requisite software licenses, Database licenses and other required monitoring software, tools for IT setup at DR site
 30. The selected bidder shall undertake installation and configuration of operating systems, databases, and storage solution and replication mechanism for all in-scope business application systems.
 31. The selected bidder shall undertake installation and configuration of any other specialized applications/ software solution/Hardware solution required for the Disaster Recovery Setup.
 32. The selected bidder would be solely responsible for implementation of all applications at DR site. All costs including licenses for application, OS, replication tools or databases if any shall be borne by the selected bidder
 33. Automated switchover/ failover facilities (during DC failure & DR Drills) to be provided and ensured by selected bidder. The switchback mechanism shall also be automated. The

- selected bidder shall also provide a tool/ mechanism for ASCL DC to trigger DR switchover (MHSP to deliver Switch Over and Switch back)
34. Selected bidder shall provide support for the development of detailed activity plans for recovery for all systems.
 35. Selected bidder shall provide support for the development of a detailed disaster recovery plan. This plan document will contain steps/procedures to switch over services to DR site in the event of invocation of disaster at DC site. Selected bidder shall also document steps for restoring services from DR site to DC site.
 36. Selected bidder shall provide support with the development of detailed operating manuals for the implemented replication solution from system administrator's perspective.

7.4. Testing and Validation

Following resource deployment/provisioning, the testing of the same at DC DR site becomes very important. Therefore, the service provider must perform following testing:

- 1) Infrastructure testing - The bidder should perform various testing procedures listed below on infrastructure (server, storage and network infrastructure) provided at Managed hosted site. Indicative list of test parameters are as follows
 - I. VM testing
 - II. Storage / Disk IO testing.
 - III. Network throughput and latency testing
 - IV. CPU and RAM benchmarking testing
 - V. Read/Write latency testing
 - VI. Data Replication Testing
 - VII. Firewall policy and configuration testing
- 2) Data Integrity Testing, Reverse Replication Testing and Switch over testing: The MH service provider will facilitate the application vendor of ASCL to carry out these/ such testing, whenever required.

7.5. Post Implementation Maintenance & Support

The service provider shall maintain and manage the system for the entire period of the contract and shall be fully responsible for ensuring adequate CPU processing power, memory, storage, network, internet bandwidth and monitoring of the MH services for optimum performance of the entire Managed hosted solution conforming to SLAs as per the Contract. The successful bidder has to provide post implementation support to maintain SLAs. During the O&M period (defined as period of 5 years), if the successful bidder is unable to comply with the support terms as mention in later section, the bidder will have to pay a Penalty as specified under the SLA of this project. Post implementation support would also include support during scheduled DR drills (once every 6 months, which shall be monitored by ASCL), during regular operations while only replication is taking place, in disaster scenario when DR is active and operational, and during switchover and switchback.

7.6. Security Audit

The service provider shall conduct vulnerability and penetration test (to be conducted by a third party testing agency which should be CERT-IN empanelled and which is approved by ASCL) on the proposed Managed hosted solution in every one year and reports should be submitted to ASCL. Corrective action should be taken by the service provider within 3 months from the date of submission of the report. Compliance review should be done within 4 months from the date of submission of the report. Any non-compliance in the reports may lead to penalty clauses. The service provider needs to update the system in response to any adverse findings in the report. ASCL may also depute auditors to conduct security check/ vulnerability test / penetration test.

7.6.1. Datacenter Specification

1. The primary datacenter location should not cause a latency of more than 15 millisecond (roundtrip) of access time from the ASCL ICC.
2. The access network to the primary hosting location should be redundant, resilient and sufficiently provisioned to ensure a near real time operational response with no single point of failure.
3. The primary site must have a redundant architecture for all applications and ensure no single point of failure.
4. The hosting locations for primary and DR site should be spread across different geolocation in different seismic zones within India.
5. The MHSP datacenters should have adequate physical security in place.
6. The MHSP datacenters should comply/certified Tier III datacenter norms.
7. The Data Center should conform to at least Tier III standard (preferably certified under TIA 942 or Uptime Institute certifications by a 3rd party) and implement tool-based processes based on ITIL standards.

7.7. IT Infrastructure at Data Centre/ Disaster Recovery Centre

Scope of work for Design, Supply and Deployment of IT Infrastructure for DC & DR:

1) Hardware and Network Provisioning:

MSI shall be responsible for following but not limited to:

- I. Appropriate initial sizing and provisioning of IT infrastructure like servers/storage, network devices (like routers/switches, etc.), security equipment including firewalls, etc. with the required components/modules considering redundancy and load balancing in line with minimum technical requirements.
- II. After deployment the MSI shall have capacity planning tool which provides the complete picture of resources used and resources required for future expansion.
- III. Warranty for all IT hardware assets procured to comply with the requirements as defined in this RFP.
- IV. Size the bandwidth requirements across all locations considering the application performance, replication, data transfer, internet connectivity for DC & DR and other requirements.
- V. Furnish a schedule of delivery of all IT Infrastructure items

- VI. Ensure all hardware requirements of application suite (including third party applications), databases, OS and other software are met.
- VII. ASCL may at its sole discretion evaluate the hardware sizing. The MSI needs to provide necessary explanation for sizing to ASCL
- VIII. Ensure that the servers should accommodate newer versions of processors, memory, etc. that support enhanced capability (e.g. lower power footprint, higher working temperature, smaller process architecture, higher frequency, etc.) of operation if required, whenever they are available. To further clarify, motherboard, controllers, etc. provided shall be of latest architecture available that supports such newer version. MSI shall substantiate with proof; preferably with an undertaking to replace the processors as and when such processors of highest level of frequency are supported.
- IX. Server models wherever applicable shall be Blade Mount servers with key board, monitor, etc. shared to minimize the requirement of rack space in DC & DR considering any space constraints.
- X. Broad range of different server footprint supporting high density configurations and high performance/ large capacity/ storage only configurations.
- XI. Qualified hardware from more than 1 server vendor.

2) Provisioning Switches:

- XII. MSI shall size and propose requisite switch at DC & DR with the required components/modules considering redundancy and load balancing.
- XIII. MSI shall size and propose other switches required for interconnecting various segments, operations centre, work area, etc.

3) IP Address Schema:

- XIV. MSI shall design suitable IP Schema for entire Local Area Network including DC & DR and interfaces to external systems/network. MSI shall ensure efficient traffic routing irrespective of link medium.
- XV. MSI shall maintain the IP Schema with required modifications from time to time during the project period.
- XVI. MSI should provide unique identity schema similar to addressing schema for all hardware components.

4) Sub-Networks & Management of Network operation

- XVII. Architecture of DC & DR shall be divided into different sub-networks. These networks shall be separated from other networks through switches and firewalls. Logical separations of these sub-networks shall be done using VLAN.
- XVIII. Separate VLAN shall be created to manage the entire network. This network shall have systems to monitor, manage routers, switches, Firewalls, etc. The MSI shall provide necessary hardware / server for loading the monitoring software if required.

5) Provisioning Storage

- XIX. Storage requirements for the application suite shall have to be assessed by MSI and the storage solution shall be sized and procured accordingly. MSI shall propose appropriate storage mechanism to accommodate proposed application suite requirement of ASCL.

- XX. Proposed storage shall be configured with appropriate redundancy to maintain business continuity based on the application & workload.

6) Network Equipment level redundancy

- XXI. MSI shall provide real-time redundancy at the network equipment level in Data Centre, and there shall not be any single point of failure.
- XXII. All equipment shall be provided with dual power supply modules. Each of the two supply modules shall be connected to alternate power strips of the network rack (two power strips to be provided in each network rack).
- XXIII. Network Equipment redundancy stipulations wherever prescribed are minimum requirements that MSI needs to consider. However, MSI needs to estimate and plan actual requirements considering service level requirements specified in this RFP.

7) Provisioning IT Security Equipment

- XXIV. MSI shall size & propose firewalls with required components/modules for DC/DR.
- XXV. Necessary IDS/ IPS shall be provided for monitoring traffic of all VLANs at DC/DR.
- XXVI. Necessary devices for log capture from servers, network equipment and other devices shall to be provisioned.
- XXVII. MSI shall implement DNS server so that the URL can be used instead of accessing web server using IP address directly. The required Hardware and Software for DNS server at DC & DR shall be provisioned by MSI.
- XXVIII. MSI shall implement management systems and procedures that adhere to ASCL's security policies.
- XXIX. MSI shall secure network resources against unauthorized access from internal or external sources.
- XXX. MSI shall also provide a mechanism for tracking security incidents and identifying patterns, if any. The tracking mechanism shall, at a minimum, track the number of security incident occurrences resulting in a user losing data, loss of data integrity, denial of service, loss of confidentiality or any incident that renders the user unproductive for a period of time
- XXXI. MSI shall ensure that all firewall devices are staged and comprehensively tested prior to deployment. In addition, SI shall conduct a vulnerability scan and analysis of the network to ensure that the optimal policies are instituted on the firewall.
- XXXII. MSI shall ensure that all firewall management is initiated from a segregated management rail on the network.
- XXXIII. MSI shall provide intrusion management services to protect ASCL's resources from internal and external threats.
- XXXIV. MSI shall provide ASCL with the necessary hardware/software required for efficient intrusion management.

Both DC and DR site shall have built in redundancy and high availability in compute and storage to ensure that there is no single point of failure. There shall be no loss of video recording in a CCC in case of failure of any single server and storage component.

MSI shall establish dedicated connectivity between DC & DR Site for replication & failover. MSI shall design the DC and DR solution with the necessary load balancing, replication and recovery solution that provide 1 hour RPO (Recovery Point Objective) and RTO (Recovery Time Objective) of 4 Hours.

DC and DR site shall be periodically audited, updated and mock drills shall be performed along with the findings and improvement /corrective steps to be taken to concern ASCL.

MSI shall submit the detailed solution document for DC and DR Site solution with justification for the proposed design meeting the requirements along with the bid.

7.7.1. Back Up Solution

- 1) Backup solution shall have same GUI across heterogeneous platform to ensure easy administration and available on various OS platforms such as Windows, Linux and UNIX platforms and be capable of supporting backup/ restores from various supported platforms.
- 2) Backup Solution should have ability to backup data from one server platform and restore it to another server platform to eliminate dependence on a particular machine and for disaster recovery purposes.
- 3) Backup Solution should support various level of backups including full, incremental, and user driven backup along with various retention period.
- 4) Backup clients should be updated automatically using the client push feature
- 5) Backup should support agentless backup for virtualization platform with non-staged granular recovery.
- 6) Backup Software should support intelligent policy for virtualization.
- 7) Backup Software must provide Source (Client & Media Server) & Target base data deduplication capabilities.
- 8) Backup Solution should Integrate with third party VTL, NAS, SAN which has data deduplication capabilities and Robotic/automated Tape library
- 9) Backup Solution must have Wizard-driven configuration and modifications for backup, restoration and devices.
- 10) Backup solution shall have in-built frequency and calendar based scheduling system.
- 11) Backup Solution must have Optimized way for data movement from client to disk target.
- 12) Backup Solution should support (inflight & at rest) encryption and Data Encryption from more than three algorithm.
- 13) Backup solution shall support tape mirroring of the same job running concurrently with primary backup.
- 14) Backup solution shall allow creating tape clone facility after the backup process.
- 15) Backup Solution should have Capability to do trend analysis for capacity planning of backup environment.
- 16) Backup Solution must offer user/capacity-based licensing. License should be for the front-end capacity rather than back-end. There should be no incremental cost associated with longer retention periods.

- 17) Backup solution should not require purchase of additional licenses for DR sites (copies of original data), also should not require purchase of additional licenses for replication to DR sites.
- 18) Software license should be independent of hardware so replacing hardware should not incur new software license cost.
- 19) Backup solution must include Agent/Modules for online backup of files, applications and databases natively for PostgreSQL, MS SQL, Oracle, DB2, Sybase, Exchange, SharePoint and File share backup(SMB)
- 20) Backup solution should provide recovery from physical servers to Virtual and image level recovery.
- 21) Backup solution should have DC/DR plug-ins for backup data replication.
- 22) Backup Solution should have Inbuilt feature for extensive alerting and reporting with pre-configured and customizable formats.
- 23) Backup Replication at DR site, DC/DR. Replication license should be included as part of solutions.
- 24) Backup software should support multiplexing and multi streaming and shall support the capability to write up to Min 32 data streams.
- 25) Backup Solutions should have capabilities to tape/disk out backup catalogue and deduplication catalogue.
- 26) Backup solution should have integrated data de-duplication engine with multi-vendor storage support to save de-duplication data. De-duplication engine should also facilitate IP base replication of de-dupe data; without any extra charge.
- 27) Backup solution must have built in capability to protect the backed up disk volumes from malware.

7.8. Enterprise Management System (EMS)

To ensure 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:

- 1) Network Monitoring System
- 2) Server Monitoring System
- 3) Helpdesk System

The solution should provide a unified web based console which allows role based access to the users.

7.8.1. Network Management System

Solution should provide fault & performance management of server side infrastructure and should monitor IP\SNMP enabled devices like Routers, Switches, PA System, Emergency Call Boxes, Sensors, etc. Proposed Network Management shall also help monitor key KPI metrics like availability to measure SLA's. Following are key functionalities that are required which will assist administrators to monitor network faults & performance degradations to reduce

downtimes, increase availability and take proactive actions to remediate & restore network services.

- 1) Proposed solution must automatically discover manageable elements connected to the infrastructure and map the connectivity between them. Solution should provide centralized monitoring console displaying network topology map.
- 2) Proposed solution should provide customizable reporting interface to create custom reports for collected data.
- 3) System must use advanced root-cause analysis techniques and policy-based condition correlation technology for comprehensive analysis of infrastructure faults.
- 4) System should be able to clearly identify configuration changes and administrators should receive an alert in such cases.
- 5) Tool must be able to track all network flow (including NetFlow v1-v9, Jflow, Sflow and IPFix) of traffic on the network and identify malicious behavior with all IP to IP and IP to Application conversations

Tool must provide high availability, simple backup and restore options in disaster recovery situations

7.8.2. Server Performance Monitoring System

- 1) Tool should integrate with network performance management system and support operating system monitoring for various platforms supplied as part of this Project.
- 2) Tool must provide information about availability and performance for target server nodes.
- 3) Tool should be able to monitor various operating system parameters such as processors, memory, files, processes, file systems, etc. where applicable.
- 4) Tool must support SNMP v1-3, WMI, PowerShell, SSH, JDBC, HTTP, JMX, collectd agents, Rest API based monitoring interface for monitoring various type of devices and systems
- 5) Tool must provide application monitoring capabilities to monitor application response time and usage behavior
- 6) Tool must support logs collected from commercial and proprietary applications. For assets not natively supported, the solution should provide the collection of logs through customization of connectors or similar integration
- 7) Tool must provide the ability to store/ retain both normalized and the original raw format of the log data for the period of 3 months and allow to extend it to further without any disruption to the ongoing data collection
- 8) Tool must provide SDK/Rest API for North bound and South Bound Integrations e.g. Forwarding specific metric data to third party database, Notifications to third party systems

7.8.3. Centralized Help Desk System

- 1) Proposed helpdesk solution must provide flexibility of logging, viewing, updating and closing incident manually via web interface for issues related to surveillance project.
- 2) Helpdesk system should provide incident management, problem management templates along with helpdesk SLA system for tracking SLA's pertaining to incident resolution time for priority / non-priority incidents.

- 3) Helpdesk system shall support ITIL processes like request management, problem management, Knowledge base management and change order management with out-of-the-box templates for various ITIL service support processes
- 4) 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) Solution should provide a clustered view of recurring themes hidden in the huge quantities of data for spotting service desk trends easily
- 6) Helpdesk should have capability to automatically categorize, understand the impact, and assign the service desk ticket to relevant helpdesk team members
- 7) Centralized Help Desk System should have integration with Network / Server Monitoring Systems so that the Help Desk Operators can to associate alarms with Service Desk tickets to help surveillance operators that for what alarms corresponding helpdesk tickets got logged.
- 8) The proposed solution should tightly integrate with monitoring system to provide two way integration - E.g. when system down alarm created, it should automatically create ticket and assign it to technician, in case system comes up before ticket is resolved by technician, it should automatically close the ticket to minimize human efforts Helpdesk should have an integrated CMDB to automatically collect and manage accurate and current business service definitions, associated infrastructure relationships and detailed information on the assets
- 9) It must be a centralized monitoring solution for all IT assets (including servers, field level infrastructure etc.)
- 10) Solution should provide inventory of all the discovered devices. Out of box inventory fields should be available and it should have provision to add additional fields as required
- 11) SLA & Contract Management module of helpdesk should be able to capture all the System based SLAs defined in this RFP and then calculate quarterly (or for any duration) penalty automatically. Measuring service performance requires incorporation of a wide variety of data sources. SLA solution should support the collection data from various sources in order to calculate Uptime / Performance / Security SLAs.
- 12) Helpdesk must have integrated dashboard providing view of non-performing components / issues with related to service on any active components
- 13) Solution must support Service Level Agreements version control and audit Trail to ensure accountability for the project.
- 14) Solution should support requirements of the auditors requiring technical audit of the whole system.
- 15) Solution most have an integrated dashboard, view of Contract Parties & current SLA delivery levels and view of Services & current SLA performance
- 16) Solution should support SLA Alerts escalation and approval process.
- 17) A general process flow for the helpdesk management is depicted in the flow chart given as follows. Systems Integrator shall prepare a detailed Helpdesk Policy in consultation with ASCL prior to Go Live date.

7.8.4. Reporting

- 1) Solution should provide historical and concurrent service level reports to ensure accountability of the service provider's performance
- 2) Automatic Report creation, execution and Scheduling, must support variety of export formats including Microsoft Word, Adobe PDF etc.
- 3) Support real-time reports (like at-a-glance status) as well as historical analysis reports (like Trend, TopN, Capacity planning reports etc.)
- 4) Solution must support security for drill-down capabilities in dashboard reports ensuring visibility for only relevant personnel of the surveillance project
- 5) Resource utilization exceeding or below customer-defined limits
- 6) Resource utilization exceeding or below predefined threshold limits
- 7) Network Management function should be able to do traffic analysis. Traffic Analysis must include Bandwidth Utilization patterns by protocol/source/destination, Network Response time patterns for various applications over the network. It should help with out of the box analysis reports to understand top bandwidth consumers by application, source, or destination. It should help with advanced reporting features to provide various reports that help understand capacity needs of the network bandwidth based on current utilization and response time trends.
- 8) Solution should be able to also provide a threshold and profile capability on the KPIs monitored on the network to understand the impact of failures and degradations which eventually results in revenue loss.
- 9) Should support automatic base lining on historical data, and thresholds that can be adjusted as required, based on data collected
- 10) Solution should offer off-the-shelf Reports for KPIs such as Availability, Uptime, and Resource

7.8.5. Centralised Antivirus Solution

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

- 1) Ability to scan through all file types and various compression formats. Ability to scan for HTML, VBScript Viruses, malicious applets and ActiveX controls.
- 2) Must update itself over internet for virus definitions, program updates etc. (periodically as well as in push-updates in case of outbreaks)
- 3) Able to perform different scan Actions based on the virus type (Trojan/ Worm, Joke, Hoax, Virus, other)
- 4) Shall provide Real-time product Performance Monitor and Built-in Debug and Diagnostic tools, and context- sensitive help.
- 5) The solution must provide protection to multiple remote clients
- 6) Shall provide for virus notification options for Virus Outbreak Alert and other configurable Conditional Notification.
- 7) Should be capable of providing multiple layers of defense
- 8) Shall have facility to clean, delete and quarantine the virus affected files.
- 9) Should support online update, where by most product updates and patches can be performed without bringing messaging server off-line.
- 10) Should support in-memory scanning so as to minimize Disk IO.

- 11) Should support Multi-threaded scanning
- 12) Should support scanning of nested compressed files
- 13) Should support heuristic scanning to allow rule-based detection of unknown viruses
- 14) All binaries from the vendor that are downloaded and distributed must be signed and the signature verified during runtime for enhanced security.

7.9. Central Identity Management Service

This service will handle user life cycle management and governance that will enable all smart cities to manage the lifespan of the user account from its initial stage of provisioning to the end stage of de-provisioning. Typically user provisioning and de-provisioning is workflow driven that will require approval. The Solution should cover user role discovery and entitlement. Similarly, it should be capable of integrating with privileged user account. User management service will cover user administrative functionalities like creation, propagation and maintenance of user identity and privileges.

Self Service feature will allow end users (e.g. members) to maintain their user identity account including self-password reset which will significantly reduce helpdesk/admin effort to handle password reset requests.

The central user repository will store the user identity data and deliver it to other services (e.g. central authentication service) for credential verification. Adherence to LDAP v3 standard has been the dominant standard for central user repository. Enforce a robust and strong password policies that will allow users to change/reset password with password expiry and account lockout features, define and implement complex password rules and session timeout policies.

7.10. 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 -

- 1) Establish groups of users based on similar functions and similar access privilege.
- 2) Identify the owner of each group
- 3) Establish the degree of access to be provided to each group

7.11. Physical DC/DR Technical Specification

A. Data Centre Specification:				
Sr. No.	Item	Minimum Requirement Description	Compliance (Yes / No)	Deviations / Remarks
DC.001	Data availability	99.982%		
DC.002	Receiving Power	Commercial power substation next to DC		
DC.003	UPS	UPS system with N+N redundancy		
DC.004	Generator	Gen-set with N+1 redundancy		
DC.005	Power Provision	Dual power feed, PDU sources to each rack, Power supply to a rack as per requirement		

DC.006	Cooling Features	<ul style="list-style-type: none"> System: Air-cooling system with N+2 redundancy, Management of temperature and humidity Blow-out Type: Raised flooring air conditioning system, Down-blow below raised floor and drawn into ceiling		
DC.007	Fire Protection:	High Sensitive Smoke Detectors, Fire Suppression System		
DC.008	Security	CCTV surveillance cameras, 24x7 on-site security presence, building Access (Photo ID Card must) along with biometric authentication		

B. Hyper Converged Infrastructure

Sr. No.	Item	Minimum Requirement Description	Compliance (Yes / No)	Deviations / Remarks
HCI.001	General Requirement	The proposed HCI solution should be software defined and should not use any hardware based RAID, Compression or De-duplication		
HCI.002		The proposed solution independently scale storage and compute as and when needed without any downtime. HCI should support storage expansion and compute expansion to extend storage/compute capacity as and when needed.		
HCI.003		The proposed HCI solution must have metadata distributed within a cluster i.e. cluster should carry information about data lying in the cluster		
HCI.004		The proposed solution must have capability to support nodes with same/different CPU & Memory configurations in the same cluster		
HCI.005		The proposed solution must have capability to support SSD & SAS/SATA		
HCI.006		Thin provisioning of both storage entities and virtual machine hard disks		
HCI.007		The solution should provide automatic failover for hardware failure		
HCI.008		The proposed HCI should support File Services or block storage any of these industry protocols over NFS/CIFS/SMB/iSCSI and should support applications across clusters and Data Centers		
HCI.009		Shall support automated chassis redundancy and survive the failure of entire chassis containing multiple nodes. In a multi-chassis configuration the infrastructure must intelligently distribute data across chassis so no redundant copies of data exist on the same		

	chassis or node.		
HCI.010	Shall support minimum 8 nodes or higher in a same cluster.		
HCI.011	The solution support for automated upgrades of storage controllers through management GUI with no downtime and major impact on production		
HCI.012	Support for layer-2 VLAN for networking and integrated VM IP's Management capabilities		
HCI.013	Shall distribute data intelligently across all nodes and capacity utilization across all nodes has to be uniform at all times.		
HCI.014	Shall be capable of adding additional combined server and storage components with high performance GPU capabilities, seamlessly, with no downtime, to scale performance and capacity on demand		
HCI.015	Native storage level snapshots with no impact to guest performance or using any additional storage capacity		
HCI.016	The solution should support data replication with disk space optimization		
HCI.017	The platform should have support for rack /chassis awareness to support redundant data should go to different rack/chassis nodes		
HCI.018	The proposed HCI should support native File Services over NFS/CIFS/SMB and file replication across clusters and data centers		
HCI.019	The proposed HCI solution must provide operations management and provide performance, storage, CPU utilization per VM		
HCI.020	Platform must provide management through a web based HTML 5 console. Must provide storage, compute & hypervisor metrics on a per VM level as well as health and monitoring of entire platform. Platform should support LDAP Active Directory integration		
HCI.021	Platform must support monitoring via SNMPv3 and email alerting via SMTP		
HCI.022	Shall be capable of creating instant snapshots of virtual machines and maintaining multiple copies of snapshots & clones		
HCI.023	Proposed HCI solution should support fault tolerance of at least two nodes failure within a cluster		

HCI.024		Solution must support native VM level replication for installed Hypervisor		
HCI.025		The solution should have call home capability for remote log collection and proactive support for predictive failure hardware component		
HCI.026		Proposed HCI solution should have inline deduplication and compression for the proposed capacity		
HCI.027		The proposed solution should provide a minimum of 200TB of usable storage. Any additional storage required for successful solution deployment should be considered and provided by the bidder.		
C. Server for Non Virtualize / Non HCI environment				
S.001		Minimum 1 numbers of Intel(R) Xeon(R) 64Bit Processor upgradable to 2 Processors on the same system, each with minimum of 8 cores, 2.10GHz Speed, 20M Cache or above. Latest Intel Chipset supporting above Process Graphics integrated with chipset		
S.002		Minimum 256 GB Memory with 32/64GB /DDR4 2133 MHz or above Memory modules, should be scalable up to 768 GB per server		
S.003		Minimum 4 PCI-e (Express) slots in which minimum 2 x PCI-e8Xslots SAS/SATA/SSD Raid controller capable of providing RAID 0, 1, 5 configurations. Min 3 x USB 2.0, 1 x Management port, 1 x VGA and 4X network ports		
S.004		Minimum 2 x 600GB SFF 15K RPM, 6Gbps SAS HDD / SSD Hot Pluggable Hard Drive with min 1 TB usable space. The server should support SAS, SATA and SSD hard disk drives		
S.005		The Server to support Microsoft Windows Server, Redhat Enterprise Linux, SuSE Linux Enterprise Server and other major industry standard operating systems		
S.006		Minimum 4 X 10 GbE Ethernet Ports and use of proprietary interconnects leading to vendor lock-in is unacceptable.		
S.007		Redundant hot pluggable Fans and Power supplies		

S.008		Server should be either blade enclosure or Rack mountable systems		
D. Minimum recommended Technical Specifications for Node / Server for HCI environment				
T.001		Minimum 2 numbers of Intel(R) Xeon(R) 64Bit Processor each with minimum of 8 cores, 2.10GHz Speed, 20M Cache or above. Latest Intel Chipset supporting above Process Bare metal Virtualization Hypervisor		
T.002		Minimum 256 GB Memory with 32/64GB /DDR4 2133 MHz or above Memory modules, should be scalable up to 1 TB per server		
T.003		The total physical core and memory comprising all the physical nodes in Converged / Hyper Converged Environment should be basis the applications , workload performance and availability requirements to be architected by MSI Min 200 TB Usable space across, excluding the OS partition and cache, if any.		
T.004		Minimum 4 PCI-e (Express) slots in which minimum 2 x PCI-e8Xslots SAS/SATA/SSD Raid controller capable of providing RAID 0, 1, 5 configurations. Min 2 x USB 2.0, 1 x Management port, 1 x VGA and 4X network ports		
T.005		Minimum of 2 SSD drives per server. Each server should support SATA/NL-SAS and SSD hard disk drives. multiple levels of data block level replication across node / controllers to prevent multi node / controller failures. Single logical unit of storage should be shared across nodes / controllers at the same time within a given cluster. It should support thin provisioning, Clone volumes.		
T.006		The Server to support Microsoft Windows Server, Redhat Enterprise Linux, SuSE Linux Enterprise Server and other major industry standard operating systems		
T.007		Minimum 4 X 10 GbE Ethernet Ports and use of proprietary interconnects leading to vendor lock-in is unacceptable.		
T.008		The system should be managed with a GUI based management software tool with storage monitoring tool integrated in the toolset, locally		

		and remotely. The management software should provide real time monitoring, and historical analysis of storage performance and capacity such as total no. of IOPS, read/write %, CPU Utilization, Network Utilization and throughput etc. for analysing the performance of the system. should have audit log for recording all service/maintenance and host log actions on the storage.		
T.009		Redundant hot pluggable Fans and Power supplies		
T.010		Rack space max up to 2 U per enclosure		

E. SAN Storage Minimum Specifications:				
Sr. No.	Item	Description	Compliance (Y/N)	Deviation/R emarks
SAN.0 01	Capacity	The Usable capacity of min 650 TB of each SAN Storage should be proposed using RAID 6 (10+2) or better for NL-SAS Disk using 6 TB or 10TB Capacity Disk along with 8 Nos. of 1.6 TB SSD Disk in RAIDS.		
SAN.0 02		The storage capacity should be scalable to double the capacity by adding the disk. No Controller hardware upgrades shall be done required		
SAN.0 03	Fault Tolerant	The Disk controller offered should have minimum support for RAID 0,1,5,6,10 levels.		
SAN.0 04		The offered Storage controller should have minimum 6 GB cache per controller and support cache backup mechanism to protect the data on cache to SSD in case of power failure.		
SAN.0 05		The Disk controller or expansion units should have redundant power supplies. Fan and controller should be redundant and hot swappable		
SAN.0 06	Supported Disk Types	The offered disk controller shall support for SSD, SAS and NL-SAS disk types of maximum capacity available.		
SAN.0 07	Host Interface	The offered storage shall support for minimum 8 no. of 16Gbps Fiber channel host interfaces.		
SAN.0 08		The host interface module shall be interchangeable or support 10Gbit or iSCSI or SFP+ interface and 12Gbps SAS ports if required.		
SAN.0 09	Performance	The offered storage should be configurable to provide throughput & IOPS as per solution		

		provided.		
SAN.0 10	Others	Should support Replication and Snap license		
SAN.0 11	LUN Size	Minimum 64TB or more and shall have no limitation on the LUN size		
SAN.0 12	Protocol Supported	SNMP, SSL, SSH, SMTP, SMI-S Provider, HTTP(s)		
SAN.0 13	Thin Provisioning Shock & Vibration	Proposed array must be supplied with thin provisioning for the configured capacity		
SAN.0 14		Shock, Operational - 3Gs for 11ms, 5 pulses each direction, rail mounted		
SAN.0 15		Shock, Non-Operational - 10Gs for 11ms, half sine, 1" drop to hard unyielding surface per NEBS, GR-63-CORE Unpackaged Equipment Shock Criteria (4.3.2)		
SAN.0 16		Vibration, Operation - 5Hz to 500Hz, 0.1436 Grms flat spectrum		
SAN.0 17		Vibration, Non-Operational - 3-365-3Hz, 1.22 Grms, Z-axis, 0.85 Grms, X- & Y-axis shaped spectrum		

F. Storage Management System

S No.	Item	Description	Compliance (Y/N)	Deviations/ Remarks
SMS.0 01	Functional Requirement	Functional requirement of the Project for Primary SAN Disk Storage & Secondary Tape Storage shall be defined for total of 90 Days Retention, in which Secondary Storage shall keep the copy of Primary Storage Video Surveillance Data as per the Retention Policy. (flagged Data)		
SMS.0 02		Data stored on Primary Storage shall be accessible online according to the Retention & Capacity available. In case Secondary Storage keeping more data than the primary storage, it shall be seamlessly accessible to the users.		
SMS.0 03		Data movement from Primary Storage to Secondary Storage should be automated without using any third-party Backup / Archival Software & LTFS Mechanism to write the Data on to LTO Tapes in Native Format.		
SMS.0 04		By increasing the Retention on the Data stored on Secondary Storage, it shall only require the LTO Media, no any extra license is required.		

SMS.0 05		Solution shall be planned & Structured for future addition in the additional Capacity.		
SMS.0 06		Solution should have the functionality, if adding a New Storage to the Installed Storage Volume It shall allow to add the New Storage into the same existing Storage pool.		
SMS.0 07	General	The Storage File System offered with the Secondary Storage Option shall support large file systems and in-Built data archiving to tape mechanism, scaling from Petabytes(PB) to Exabyte.		
SMS.0 08		File System functionality for the Secondary Storage with Tape solution should not be only responsible to allocate move / Archive the data to tape but it shall be in Native Format between Primary & Secondary Storage automatically without using third party Backup and Archive Software.		
SMS.0 09		Supported Inbuilt Archiving functionality for Un-Structured Data, shall also allow and Confirm the Archived Data access & Retrieval Directly from User/ VMS application without using any third-party Backup & Archive system to retrieve the Data from Tape Library.		
SMS.0 10		Extension of the Retention shall be possible easily in the secondary Storage.		
SMS.0 11		Number of the Total Retention period for the Secondary Storage shall be min. of 60 Days and can be extended further with the minimal cost.		
SMS.0 12	Global Name Space	The Storage file system should be open to support the different/ multiple make of Storage under the same existing Global name space view for all the users/ files in single file system view to all the Heterogenous client at the time of Storage Expansions and volume expansion with Capacity.		
SMS.0 13		The Storage File System should present the location of the file with the same file path and filename to all its clients.		
SMS.0 14	File Sharing	The Storage File System should allow multiple clients to access the same file for concurrent read.		
SMS.0 15		Metadata server should support file sharing locks to assure integrity while supporting concurrent access		

SMS.0 16	Storage Upgrade/ Migration Support	The Storage File System shall allow online expansion and retirement of storage capacity and disk array swap-outs without taking the file system off line. This includes adding addition disks to existing storage arrays, adding incremental or new storage arrays, and/or the removal of older arrays in replacement of new storage subsystems		
SMS.0 17	Archival/ Retrieval	Offered file system shall have the inbuilt Data Archiving functionality as a single software without using the LTFS mechanism, It shall be a single GUI to move the data from Primary Disk to Tape Library in the Native File Format and leave the Stubs on to Primary Storage.		
SMS.0 18		Offered File System shall also have the in-built functionality of retrieving the data from Tape in Native Format to Primary Storage through the User/ application as a normal Data access functionality.		
SMS.0 19		Secondary Storage should have the provisioning of keeping a Duplicate / Second copy of the Primary Storage's Online Video Data. Data Older than the Primary storage's retention will be kept only on Secondary LTO Tape Storage.		
SMS.0 20		Data stored on Primary & Secondary should be accessible online for minimum of 1-7 days as Online data from SAN Storage and older than 7 Days Data will be retrieved from Secondary LTO storage / LTO Media.		
SMS.0 21		Storage File System should be capable of recovery in case of system crash or unplanned shutdown.		
SMS.0 22		Offered Storage file system should be capable of recovering all the Backup & archived data in the Native Format from Tape without using the main server, in case of server is down or not in use.		
SMS.0 23	Retention Scalability	In case of increasing the Retention from 60 Days to 365 Days, only LTO media cartridge to be added to Retain the Data offline /Offsite. No other licenses required to increase the Retention to control the Cost.		
SMS.0 24	Vaulting	It shall have the functionality to vault the media and provide a means of notifying the operator to retrieve a vaulted media when an Offline or oldest file is requested, when the capacity is increased by increasing the Retention.		

SMS.0 25	Administration features of the file system	Shall have automated de-fragmentation capabilities		
SMS.0 26		Shall have administration capabilities through GUI and CLI		
SMS.0 27		Shall provide capabilities for user administration		
SMS.0 28		File system shall provide features for file system audits		
SMS.0 29		File system shall provide extensive alert capabilities.		
SMS.0 30	Replication / DR support	The Storage File System shall support replication for Disaster Recovery		

G. Archived Enabled TAPE Library

Sr. No.	Item	Description	Compliance (Y/N)	Deviations/ Remarks
TL.001	Min. No. of FC Dual Port Drives required	10 Nos. Full Height LTO-7 Drives		
TL.002	LTO Drive Scalability	Up to 50 LTO-7 Drives, Full Height Drives		
TL.003		Total of 1400 Physical Slot availability in the Tape Library.		
TL.004	Min. No. of Active Media Tape Slots License to provide	Out of 1400-Physical slots, 400 Nos. Archive enabled Tape License slot with Vault License, Media cartridges shall be moved from active slots to physical slots on user action/console with in the library using internal robotics using Vault Feature.		
TL.005	Tape Slot scalability	5000 Nos.		
TL.006	Data Cartridge	LTO-7 (rewritable)		
TL.007		LTO-7 Cleaning cartridge: LTO Universal Cleaning Cartridge		
TL.008	Native Capacity data	Min. 6.0 TB		
TL.009	Max. Uncompressed Speed	Min. 300MB/s native		
TL.010		Up to 750 MB/s compressed		
TL.011	Compression capable	2.5: 1 (Compressed capacity – up to Min. 15TB)		
TL.012	Backward Compatibility	Read/write LTO-7 media.		
TL.013		Reads LTO-7 media.		
TL.014	Interface	8Gb/s Fibre Channel		

TL.015	Data Integrity Mechanism in Library	Offered Tape should have the Mechanism to maintain the Data Integrity within the Library by scanning the complete LTO Media tape to check, Update and Migrate the data to new Media in case any problem found.		
TL.016		Should be offered with min. One additional & dedicated LTO Drive for scanning the LTO content for Data Life & Integrity Management.		
TL.017	Min. Media cartridges	1350 LTO-7 media cartridges		
TL.018	Redundancy	Dual Power Supply, Dual Robotic Arm		
TL.019	Reporting feature	Advance Reporting		
TL.020		Drive Utilization Report		
TL.021		Media Usage report		
TL.022		Media Movement report		
TL.023	Vaulting	Job completion report		
TL.024	Advanced Feature	Active Vault License		

H. FC SAN SWITCH

Sr. No.	Description	Compliance (Y/N)	Deviations/Remarks
FCS.0 01	Power Specification - 200-240V, 50-60 Hz		
FCS.0 02	Operating temperature range - 0° to 40° C		
FCS.0 03	Operating Relative Humidity range (non-condensing) - 10 to 90% relative humidity		
FCS.0 04	Total no. of ports on the proposed switch - 24 (No. of SAN Switch to be calculated and proposed as per the consumption)		
FCS.0 05	Throughput of each FC port - 16 Gbps		
FCS.0 06	Support for 4/8 Gb/s HBAs		
FCS.0 07	Aggregate backplane Switch bandwidth - 384 Gbps		
FCS.0 08	Protocol supported FC & FCP		
FCS.0 09	Shall be designed for high availability with no Single Point of Failure		
FCS.0	should have Hot Swappable Power supply		

10			
FCS.0 11	Should have (N+1) redundant power supply		
FCS.0 12	Should have Hot Swappable Cooling Fans		
FCS.0 13	Should have (N+1) redundant Cooling Fans proposed		
FCS.0 14	Capability for streaming the data in multiple paths with Optimization algorithms for streaming data through shortest available path.		
FCS.0 15	Capabilities for cascading of switches		
FCS.0 16	Non-disruptive firmware update		
FCS.0 17	Should have End to end performance monitoring		
FCS.0 18	Capability to interface with host based adapters (HBA) of multiple OEM, supporting multiple Operating System including but not limited to AIX, HP-UX, Linux, Solaris, Windows, etc.		
FCS.0 19	Support all leading SAN disk arrays and tape libraries including but not limited to Dell EMC, Hitachi, Quantum, HP, StorageTek, Sun, etc..		
FCS.0 20	Support for hardware -enforced zoning		
FCS.0 21	Policy based security and centralised fabric management		
FCS.0 22	Support for Encrypted password		
FCS.0 23	Support for PKI Digital certificates		
FCS.0 24	Support for FCAP authentication		
FCS.0 25	Support for RADIUS, SSL / HTTPS, SSH, SNMP V3		
FCS.0 26	Support for LUN masking		
FCS.0 27	Support for dynamic Load balancing of links with no overhead		
FCS.0 28	Compatibility with proposed network devices		
FCS.0 29	Compatibility with proposed servers		
FCS.0 30	The system should not be an end of life / end of service product.		

I. Fabric Controller				
Sr. No.	Item	Description	Compliance (Y/N)	Deviation/Remarks
	Fabric Definition	Fabric is the Close Architecture defined using Spine, Leaf and VXLAN + ISIS or VXLAN + EVPN Protocol.		
		<p>Fabric should have following functionalities to be achieved:</p> <ul style="list-style-type: none"> • Flexibility: allows workload mobility anywhere in the DC. • Robustness: while dynamic mobility is allowed on any authorized location of the DC, the failure domain is contained to its smallest zone. • Performance: full cross sectional bandwidth (any-to-any) – all possible equal paths between two endpoints are active. • Deterministic Latency: fix and predictable latency between two endpoints with same hop count between any two endpoints, independently of scale. • Scalability: add as many Leaf as needed to achieve desired scale in terms of number of servers while maintaining the same oversubscription ratio everywhere inside the fabric. 		
2	Optics	Fabric should have Switch and Optics from same OEM.		
3	Fabric Features	Fabric must support various Hypervisor encapsulation including VXLAN, NVGRE and 802.1q natively without any additional hardware/software or design change.		
		Fabric must auto discover all the hardware and auto provision the fabric based on the policy.		
		The fabric architecture must be based on hardware VXLAN overlays to provide logical topologies that are abstracted from the physical infrastructure with no performance degradation. Fabric must support VXLAN Switching/Bridging and VXLAN Routing.		
		Fabric must provide open programmable interface using python SDK, Jason SDK, XMLS or COBRA etc. from the Central Management appliance / SDN Controller for programming/configuring the entire		

		fabric.		
		Fabric must provide open scripting interface using Bash, powershell, NetConf, YANG from the central management appliance / SDN Controller for configuring the entire fabric.		
		Fabric must support Role Based Access Control in order to support Multi - Tenant environment.		
		Fabric must integrate with different virtual machine manager and manage virtualise networking from the single pane of Glass - Fabric Controller/SDN Controller.		
		Fabric must integrate with best of breed L4 - L7 Physical and virtual appliances and manage using single pane of glass - Fabric Controller / SDN Controller.		
		Fabric must provide deeper visibility into the fabric in terms of latency and packet drop between VM to VM, VM to Physical server and vise versa, Leaf to another leaf etc.		
		Fabric must act as single distributed layer 2 switch, Layer 3 router and Stateless distributed firewall etc.		
		Fabric must provide REST APIs from the Central management appliance/SDN Controller in order to integrate with best of breed Management, Monitoring, Hypervisor and Cloud automation & Orchestration software.		
4	Fabric Layer 2, Layer 3 and Misc. Features	Fabric must support Layer 2 features like LACP, STP /RSTP /MSTP, VLAN Trunking, LLDP etc.		
		Fabric must support multi chassis ether channel/MLAG i.e. Host connects to two different Leaf switches and form ether channel using LACP/NIC Teaming on Host.		
		Fabric must support Jumbo Frame upto 9K Bytes on 1G/10G/25G/40G/100G ports.		
		Fabric must support Layer 2 Multicast i.e. IGMP v1, v2 and v3.		
		Fabric must support IP v4 and IP v6 FHRP using HSRP or VRRP.		
		Fabric must support IP v4 and IP v6 Layer 3 routing protocol OSPF and BGP		
		Fabric must support IP v6 dual stack.		

		Fabric must support traffic redistribution between different routing protocols.		
		Fabric must support IP v4 and IP v6 management tools like - Ping, Traceroute, VTY, SSH, TFTP and DNS Lookup.		
		Fabric must support IP v4 and IP v6 SNMP V1 / V2 / V3.		
		Fabric must support RMON/RMON-II for monitoring.		
		Fabric must support integration with the centralised Syslog server for monitoring and audit trail.		
		Fabric must support NTP		
5	Fabric Security Features	Fabric must have zero trust policy model for connected systems or hosts to help in protecting against any kind of attacks like Unauthorized Access, Man - in - the - middle - attack, Replay Attack, Data Disclosure, Denial of Service.		
		Fabric must provide RBAC policies and support AAA using Local User authentication, External RADIUS, External TACACS+, External LDAP, External AD.		
		Fabric must support VM attribute based zoning and policy.		
		Fabric must support Micro Segmentation for the Virtualize and Non - Virtualize environment.		
		Fabric must support true multi - tenancy.		
		Fabric must be accessible using CLI over SSH and GUI using HTTP/HTTPS		
		Fabric must support SNMP v2/3 with HMAC-MD5 or HMAC-SHA authentication and DES encryption.		
		Fabric must act as a State-less distributed firewall with the logging capability.		
6	Fabric Service Features	Fabric must be capable to provide services of L 4 - L7 services using physical or virtual appliances i.e. Firewall, ADC, IPS etc.		
		Fabric must have zero trust policy model for connected systems or hosts to help in protecting against any kind of attacks like Unauthorized Access, Man - in - the - middle - attack, Replay Attack, Data Disclosure, Denial of Service.		
7	Fabric Scale	Fabric should support scale up and scale out without		

and Performanc e	any service disruption.		
	Fabric must support for 500 VRF/Private network without any additional component or upgrade or design change.		
	Fabric must scale from 100 Tenant to 500 Tenant without any additional component or upgrade or design change.		
	Fabric must integrate with minimum 3 Virtual Machine Manager (i.e. vCenter, SCVMM, OpenStack etc.) of different Hypervisors simultaneously and scalable to 5 in future with or without common orchestrator.		
	Fabric must be capable of connecting 2500 physical servers and scale to 5000 physical servers..		
	Fabric must be capable of integrating minimum of 8 nos. of L 4 - L7 services physical or virtual appliances (i.e. Firewall, ADC, IPS etc.) and scale upto 16 nos of L4 - L7 Services appliances.		
	Fabric must support minimum of 4 Leaf switches and scale upto 250 Leaf switches without any design change.		
	Fabric must support minimum of 2 Spine Switches and scale upto 6 Spine switches without any design change.		
	Spine Switches must have adequate number of line rate 40/100G ports to support desired Leaf Scale.		
	Each Leaf connects to Each Spine using minimum 1 x 40/100 G ports connectivity i.e. Each Spine must have 128 nos. of line rate 40G/100G ports with consideration of leaf to SPINE over subscription ration of 4:1.		
	Fabric must support 20K IPv4 and 10K IPv6 routes scalable to 30K IPv4 and 15K IPv6 routes.		
	Fabric must support 4K multicast groups scalable to 8K multicast groups.		
	Fabric must support 256 nos. of MLAG/VPC scalable to 384 nos. Each MLAG/VPC must support maximum 8 member links.		
	Fabric must support 256 nos. of Port Channel scalable to 384 nos. Each Port Channel must support maximum of 8 member links.		

8	Fabric management	Fabric must provide Centralised Management Appliance or SDN Controller - Single pane of Glass for managing, monitoring and provisioning the entire Fabric.		
		Fabric must Auto discover all the Spine and Leaf switches and auto provision them based on the Fabric policy using Centralised Management appliance or SDN Controller.		
		Centralised management appliance or SDN Controller must manages and provision L4 - L7 Services physical or virtual appliance as well as integrate with Virtual Machine manager.		
		Centralised management appliance or SDN Controller should not participate in Data plane and control plane path of the fabric.		
		Centralised management appliance or SDN Controller must provide necessary report for compliance and audit.		
		Centralised management appliance or SDN Controller must communicate to south bound devices using open standard protocol i.e. OPFLEX, OPENFLOW, OVSDB etc. or using Device APIs.		
		Centralised management appliance or SDN Controller communication with the south bound devices must be encrypted		
		Centralised management appliance or SDN Controller must communicate with the south bound devices using more than one path i.e. in-path connectivity and out of band management connectivity		
		Centralised management appliance or SDN Controller provide dynamic device inventory of the Fabric as well as current network topology of the fabric. It must also validate the cabling connectivity and generate alarms in case of wrong or faulty connectivity.		
		Centralised management appliance or SDN Controller provide dynamic device inventory of the Fabric as well as current network topology of the fabric. It must also validate the cabling connectivity and generate alarms in case of wrong or faulty connectivity.		
		Centralised management appliance or SDN Controller		

		must run in "N + 1 or N + 2" redundancy to provide availability as well as function during the split brain scenario.		
--	--	--	--	--

J. TOR (Top of the Rack) Switch:				
TORS.001	Ports	<ul style="list-style-type: none"> ▪ 24 or 48 (as per density required) 1G/ 10G Ethernet ports (as per internal connection requirements) and extra numbers of Uplink ports (as per requirement) ▪ All ports can auto-negotiate between all allowable speeds, half-duplex or full duplex and flow control for half-duplex ports. 		
TORS.002	Switch type	1) Layer 3		
TORS.003	MAC	2) Support minimum 32K MAC address.		
TORS.004	Backplane	3) Capable of providing wire-speed switching		
TORS.005	Throughput	4) 500 Mbps or higher		
TORS.006	Port Features	5) Must support Port Mirroring, Port Trunking and 802.3ad LACP Link Aggregation port trunks or equivalent support		
TORS.007	Flow Control	6) Support IEEE 802.3x flow control for full-duplex mode ports or equivalent support		
TORS.008	Protocols	<ul style="list-style-type: none"> ▪ IPV4, IPV6 ▪ Support 802.1D, 802.1S, 802.1w, Rate limiting ▪ Support 802.1X Security standards ▪ Support 802.1Q VLAN encapsulation, IGMP v1, v2 and v3 snooping ▪ 802.1p Priority Queues, port mirroring, DiffServ ▪ DHCP support ▪ Support up to 1024 VLANs ▪ Support IGMP Snooping and IGMP Querying ▪ Support Multicasting ▪ Should support Loop protection and Loop detection, and root protection 		
TORS.009	Access Control	<ul style="list-style-type: none"> ▪ Support port security ▪ Support 802.1x (Port based network access control). ▪ Support for MAC filtering. ▪ Should support TACACS+ and RADIUS 		

		authentication		
TORS.0 10	VLAN	<ul style="list-style-type: none"> ▪ Support 802.1Q Tagged VLAN, port based VLANs and Private VLAN ▪ Switch must support dynamic VLAN Registration or equivalent ▪ Switch should support VLAN trunking or equivalent 		
TORS.0 11	Protocol and Traffic	<ul style="list-style-type: none"> ▪ Network Time Protocol or equivalent Simple Network Time Protocol support ▪ Switch should support traffic segmentation ▪ Traffic classification should be based on user-definable application types: TOS, DSCP, Port based, TCP/UDP port number 		
TORS.0 12	Management	<ul style="list-style-type: none"> ▪ Switch needs to have a console port for management via a console terminal or PC ▪ Must have support SNMP V1, V2 and V3 ▪ Should support 4 groups of RMON ▪ Should have accessibility using Telnet, SSH, Console access, easier software upgrade through network using TFTP etc. Configuration management through CLI, GUI based software utility or using web interface 		
TORS.0 13	Resiliency	<ul style="list-style-type: none"> ▪ Dual load sharing AC and DC power supplies ▪ Redundant variable-speed fans 		
K. Online UPS:				
ONUPS .001	Capacity	<ul style="list-style-type: none"> ▪ Adequate capacity to cover all above IT Components at respective location 		
ONUPS .002	Output Wave Form	<ul style="list-style-type: none"> ▪ Pure Sine wave 		
ONUPS .003	Input Power Factor at Full Load	<ul style="list-style-type: none"> ▪ >0.90 		
ONUPS .004	Input	<ul style="list-style-type: none"> ▪ Three Phase 3 Wire for over 5 KVA 		
ONUPS .005	Input Voltage Range	<ul style="list-style-type: none"> ▪ 305-475VAC at Full Load 		
ONUPS .006	Input Frequency	<ul style="list-style-type: none"> ▪ 50Hz +/- 3 Hz 		
ONUPS .007	Output Voltage	<ul style="list-style-type: none"> ▪ 400V AC, Three Phase for over 5 KVA UPS 		
ONUPS .008	Output Frequency	<ul style="list-style-type: none"> ▪ 50Hz +/- 0.5% (Free running); +/- 3% (Sync. Mode) 		
ONUPS .009	Inverter efficiency	<ul style="list-style-type: none"> ▪ >90% 		
ONUPS	Over All AC-AC	<ul style="list-style-type: none"> ▪ >85% 		

.010	Efficiency			
ONUPS .011	UPS shutdown	<ul style="list-style-type: none"> UPS should shutdown with an alarm and indication on following conditions 1) Output over voltage, 2) Output under voltage, 3) Battery low, 4) Inverter overload, 5) Over temperature, 6) Output short 		
ONUPS .012	Battery Backup	<ul style="list-style-type: none"> 30 minutes in full load 		
ONUPS .013	Battery	<ul style="list-style-type: none"> VRLA (Valve Regulated Lead Acid) SMF (Sealed Maintenance Free) Battery 		
ONUPS .014	Indicators & Metering	<p>Indicators for AC Mains, Load on Battery, Fault, Load Level, Battery Low Warning, Inverter On, UPS on Bypass, Overload, etc.</p> <ul style="list-style-type: none"> Metering for Input Voltage, Output Voltage and frequency, battery voltage, output current etc. 		
ONUPS .015	Audio Alarm	Battery low, Mains Failure, Over temperature, Inverter overload, Fault etc.		
ONUPS .016	Cabinet	Rack / Tower type		
ONUPS .017	Operating Temp	0 to 50 degrees centigrade		
ONUPS .018	Management Protocol	SNMP Support through TCP/IP		
L. DG Set:				
DGS.00 1	General Specifications	<ul style="list-style-type: none"> Auto Starting DG Set mounted on a common base frame with AVM (Anti-Vibration) pads, residential silencer with exhaust piping, complete conforming to ISO 8528 specifications and CPCB certified for emissions. <p>KVA rating as per the requirement</p>		
DGS.00 2	Engine	<ul style="list-style-type: none"> Radiator cooled, multi cylinder, 1500 RPM diesel engine, with electronic/manual governor and electrical starting arrangement complete with battery, conforming to BS5514/ ISO 3046/ IS 10002 		
DGS.00 3	Fuel	<ul style="list-style-type: none"> High Speed Diesel (HSD) 		
DGS.00 4	Alternator	<ul style="list-style-type: none"> 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. 		

DGS.00 5	AMF (Auto Main Failure) Panel	<p>AMF Panel fitted inside the enclosure, with the following:</p> <p>It should have the following meters/indicators</p> <ul style="list-style-type: none"> ▪ Incoming and outgoing voltage / Current in all phases ▪ Frequency, KVA and power factor ▪ Time indication for hours/minutes of operation ▪ Fuel Level in fuel tank, low fuel indication ▪ Emergency Stop button ▪ 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 		
DGS.00 6	Acoustic Enclosure	<ul style="list-style-type: none"> ▪ 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). <p>Enclosure must be weather resistant powder coated, with insulation designed to meet latest MOEF/CPCB norms for DG sets, capable to withstand Hyderabad climate. The enclosure must have ventilation system, doors for easy access for maintenance, secure locking arrangement, complete and</p>		
DGS.00 7	Fuel Tank Capacity	<ul style="list-style-type: none"> • It should be sufficient & suitable for containing fuel for minimum 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. 		
M. Structured Cabling Components:				
SCC.00 1	Standards	<ul style="list-style-type: none"> • ANSI TIA 568 C for all structured cabling components 		
SCC.00 2	OEM Warranty	<ul style="list-style-type: none"> • OEM Certification and Warranty of 15-20 years as per OEM standards 		
SCC.00 3	Certification	<ul style="list-style-type: none"> • UL Listed and Verified 		
N. Electrical cabling component:				
ECC.00 1	Standards	<ul style="list-style-type: none"> • All electrical components shall be design manufactured and tested in accordance with 		

		relevant Indian standards IEC's		
O. Internet and Intranet Router				
IIR.001	Internet Router	Router should be chassis based device with minimum 10 Gbps of throughput scalable upto 20 Gbps. It should have minimum 4 GB of RAM/ DRAM		
IIR.002		Router supports management protocol: SNMP v1/v2/v3, CLI (Telnet/Console), TFTP update and configured file management		
IIR.003		Router must have inbuilt state full firewall,zone-based firewall and 3 DES capability technologies to support the access controller strategy based source and destination IP protocol port and time parameters		
IIR.004		Router should have tunneling protocols like IPsec VPN, GET VPN or equivalent, Multi Point VPN and encryption mechanisms like DES, 3DES, AES (128 and 256Bit).It should support minimum 300 IPsec tunnels from day one.		
IIR.005		Router has support for the following routing /WAN protocols PPP/MLPPP, HDLC		
IIR.006		Router should be modular chassis based device and should accommodate a combination of high-density , 10G, Gigabit Ethernet, Fast Ethernet		
IIR.007		Router should support protocols like RIP, OSPF, BGP, VRRP/HSRP, 802.1q, GRE, ACL's and NAT MPLS, traffic engineering, EoMPLS or VPLS or equivalent, L2 VPN from day one		
IIR.008		Shall support the RIPng & BGP for IPv6, OSPFv3, MPLS, BGP from day one.		
IIR.009		Router should have minimum 18000 IPv4 and IPv6 with 50K multicast route support from day one		
IIR.010		The router supports state full packet inspection supporting H.323, SIP and other application level gateway support		
IIR.011		System shall support to provide the ability to filter and gather application information in a flexible manner from day one xflow/jflow		
IIR.012		Router should support QoS Classification and marking policy based routing, IP precedence, DSCP		
IIR.013		QoS -congestion management WRED/RED, Priority queuing, class-based weighted for fair queuing		
IIR.014		IP Access list to limit Telnet SNMP access to router		

IIR.015		Multiple privilege level authentication for console and telnet access		
IIR.016		Time-based ACL for controlled forwarding based on time of day for offices		
IIR.017		Should have extensive support for SLA monitoring for metrics like delay latency, jitter, packet loss and MoS		
IIR.018		Provides QoS features like traffic prioritization, differentiated services, and committed, and committed access rate, QoS Support, RSVP/WFQ/MRED. Router should be able to take pre-configured action on these events like changing routes, changing routing metric		
IIR.019		Router supports for QoS Features for defining the QoS policies. Support for low latency queuing, Layer 2 and Layer 3 CoS/DSCP		
IIR.020		Router should have multicast routing protocols support: IGMPv1, v2 (RFC2236) PIM-SM (RFC2362) and PIM-DM/ Multicast VLAN Registration		
IIR.021		The following interface required from Day-1: 2x 10G SFP+ based ports loaded with single mode transceiver, 3*1GE & 3*1G SFP-based transceiver.		
IIR.022		The router should be IPv6 ready		
P. Intranet Routers				
IIR.023	Architecture	Router should have redundant controller cards and should support stateful switchover, non-stop forwarding, Non-stop routing and Graceful restart.		
IIR.024		Router should be CE2.0/MEF14.0 certified		
IIR.025		Router shall support MEF for Ethernet based services like PW, VPLS or ATOM.		
IIR.026		Router shall support sync any configurations from previous modules to new modules with hot-swap event occurred		
IIR.027		The router should have redundant control & data plane.		
IIR.028		The router shall support following type of interfaces – 10GE, 1GE interfaces, 10G, Ch.STM1		
IIR.029		All the Ports and card on Router should be hot swappable and field replacement of port or card should not require to bring down the chassis.		
IIR.030		Performance	Router shall support non-blocking capacity of 64 Gbps full duplex	
IIR.031	Router shall support 60 Mpps forwarding performance for IPv4 & IPv6 performance			

IIR.032		The router should support 20Gbps per slot throughput.		
IIR.033		Router shall support 16000 Mac addresses		
IIR.034		Router shall support minimum 18000 IPv4 and IPv6 with 50K multicast routes		
IIR.035		router shall support 4000 queues and 128 MPLS VPN's		
IIR.036		Router shall support aggregation of links. Minimum 8 links should be supported as part of single aggregation		
IIR.037		Router shall support IPSLA or equivalent and Y.1731 for performance monitoring		
IIR.038		Router should support Redundant Power Supply and should also support Online insertion and removal of same.		
IIR.039	High Availability	Fan tray should be hot-swappable and should be a Field Replaceable Unit (FRU). The node can run indefinitely with a single fan failure. Shall Support hot-swappable for all modules. And secure normal operations when hot-swap event occurred		
IIR.040		Router shall support MPLS-TE with FRR for sub 50 msec protection.		
IIR.041		Router must support Traffic Engineering for node and link protection.		
IIR.042		Router shall support IPV4 and IPV6, IGMP V2/V3, MLD, IGMP and PIM, 6PE and 6VPE		
IIR.043		mode for IPV6 transport over IPV4, ECMP, LDP, BGP Prefix independent control (EDGE and Core) for IPV4 and IPV6, BGP, ISIS, OSPFv2 and V3, RSVP, VRRP and Traffic Engineering		
IIR.044	Protocol Support	Router should support high availability for all BFD,BGP ,OSPF and IS-IS and no packet loss during controller switch over.		
IIR.045		Router should support RFC 3107 of Carrying Label Information in BGP-4		
IIR.046		The Router should support Point to Point and Point to Multipoint LSP for Unicast and Multicast traffic.		
IIR.047		Router shall support layer3 and layer2 MPLS VPN.		
IIR.048	QoS Features	Router shall support HQOS on all kind of interface in both ingress and egress direction. Similar QOS shall be supported for all type of interface including Bundled interfaces.		
IIR.049		Shall support Ingress classification, marking and		

		<p>policing on physical interfaces and logical interfaces using source/destination IP subnet, protocol types (IP/TCP/UDP),source/destination ports, IP Precedence, MPLS EXP, DSCP,802.1p</p>		
IIR.050		<p>Shall support Strict Priority Queuing or Low Latency Queuing to support real-time application like Voice and Video with minimum delay and jitter.</p>		
IIR.051		<p>Congestion Management: WRED, Priority queuing, Class-based weighted fair queuing</p>		
IIR.052	Security Management &	<p>Support Access Control List to filter traffic based on Source & Destination IP Subnet,Source& Destination Port, Protocol Type (IP,UDP, TCP, ICMP etc.) and Port Range etc. Should Support per-user Authentication, Authorization, and Accounting through RADIUS or TACACS and SNMPv1/v2/V3</p>		
IIR.053	Operating Environmental Requirements	<p>0°C to 40°C operating temperature and 10 to 90%, non-condensing</p>		
IIR.054	Interface	<p>The proposed router should support the following from day1: - 2x10G SFP+ ports supplied with 1x10G single mode transceiver, 1x10G multi-mode transceiver, 8x1G SFP ports supplied with 4x1G single mode transceiver, 4x1G multi-mode transceiver & minimum 12 no's of 10/100/1000 Base- T ports.</p>		
IIR.055	Certifications/ OEM Criteria	<p>The proposed router should be EAL2/ NDPP certified by common Criteria body at the time of delivery. The router should be IPv6 ready from day-1.</p>		

Q. Spine Switch

1		<p>The core/spine layer switches should have hardware level redundancy (1+1) in terms of data plane and control plane. Issues with any of the plane should not impact the functioning of the switch.</p>		
2	General Requirement	<p>The switch should have redundant CPUs working in active-active or active-standby mode. CPU fail over/change over should not disrupt/impact/degrade the functioning the switch.</p>		
3		<p>The Switch should support non-blocking Layer 2 switching and Layer 3 routing. Switch with</p>		

		different modules should function line rate and should not have any port with oversubscription ratio applied		
4		Switch should support in line hot insertion and removal of different parts like modules/power supplies/fan tray etc. This should not require rebooting of the switch or create disruption in the working/functionality of the switch		
5		Switch should support the complete STACK of IP V4 and IP V6 services.		
6		Switch and optics must be from the same OEM		
7		Switch should support non blocking, wire speed performance per line card		
8		Switch should have the following interfaces:		
9	Hardware and Interface Requirement	a. Minimum 30 nos of line rate and Non - Blocking 40/100G ports fully populated with 100G		
10		Switch should have adequate power supplies for the complete system usage, providing N+1 redundancy		
11		Switch should support IEEE Link Aggregation and Ethernet Bonding functionality to group multiple ports for redundancy		
12		The switch should support 1,20,000 IPv4 and IPv6 routes entries in the routing table with multicast routes		
13	Performance Requirement	The switch should support hardware based load balancing at wire speed using LACP and multi chassis ether channel/LAG		
14		Switch should support total aggregate minimum 28 Tbps minimum of switching capacity		
15		Switch should support Network Virtualization using Virtual Over Lay Network using VXLAN (RFC 7348)/NVGRE as per RFC 2890		
16	Virtualization Features	Switch should support VXLAN (RFC7348) and EVPN or equivalent for supporting Spine - Leaf architecture to optimize the east - west traffic flow inside the data center through integration with Orchestration layer / VM manager.		
17		Switch should support Open Flow/Open Day light/Open Stack controller		
18		Switch should support Data Center Bridging		
19		Switch should support multi OEM hypervisor environment and should be able to sense		

		movement of VM and configure network automatically		
20		Switch must support VXLAN Switching/Bridging and VXLAN Routing without any performance degradation		
21	Layer2 Features	Switch should support minimum 160,000 no. of MAC addresses		
22		Switch should support Jumbo Frames up to 9K Bytes on 1G/10G Ports		
23		Support for broadcast, multicast and unknown unicast storm control to prevent degradation of switch performance from storm due to network attacks and vulnerabilities		
24	Layer3 Features	Switch should support MPLS routing		
25		Switch should provide multicast traffic reachable using:		
26		a. PIM-SM		
27		b. PIM-SSM		
28		c. Bi-Directional PIM		
29		d. Support RFC 3618 Multicast Source Discovery Protocol (MSDP)		
30		e. IGMP V.1, V.2 and V.3		
31		Switch should support Multicast routing		
32	Availability	Switch should support for BFD For Fast Failure Detection		
33	Quality of Service	Switch should have a minimum buffer of 80 Mb or more		
34		Switch should support Flow control of Ethernet ports to control traffic rates during congestion by allowing congested nodes to pause link operation at the other end for receiving traffic		
35	Security	Time based ACL		
36		Switch should support for Role Based access control (RBAC) for restricting host level network access as per policy defined		
37		Switch should support for external database for AAA using:		
38		a. TACACS+		
39		b. RADIUS		
40		Should support Standard / Extended ACLs		
41	Manageability	Switch should support for predefined and customized execution of script for device manage for automatic and scheduled system status update		

		for monitoring and management		
42		Switch should provide different privilege for login in to the system for monitoring and management		
43		Switch should support Real time Packet Capture using Wire shark in real time for traffic analysis and fault finding		
R. Leaf Switch - OFC				
1	Solution Requirement	The Switch should support non-blocking Layer 2 switching and Layer 3 routing		
2		There switch should not have any single point of failure like power supplies and fans etc should have 1:1/N+1 level of redundancy		
3		Switch and optics must be from the same OEM		
4		Switch should support the complete STACK of IP V4 and IP V6 services.		
5	Hardware and Interface Requirement	Switch should have the following interfaces:		
6		a. 48 x 10G/25G Multi Mode Fiber Interface populated with required transceivers		
7		b. 6 x 40/100GbE QSFP ports populated with trans receivers		
8		Switch should support IEEE Link Aggregation and Ethernet Bonding functionality to group multiple ports for redundancy		
9	Performance Requirement	The switch should support atleast 60000 IPv4 and IPv6 or more routes entries in the routing table with multicast routes. The bidder may propose best specification as per the proposed solution and city requirements.		
10		The switch should support hardware based load balancing at wire speed using LACP and multi chassis ether channel/LAG		
11		Switch should support minimum 3 Tbps of switching capacity		
12		Each leaf should have connectivity to all spine switches and the over subscription should not be less then 4:1		
13	Advance Features	Switch should support Network Virtualization using Virtual Over Lay Network using VXLAN (RFC 7348)		
14		Switch should support VXLAN (RFC7348) and EVPN or equivalent for supporting Spine - Leaf architecture to optimize the east - west traffic flow inside the data center		

15		Switch should support Open Flow/Open Day light/Open Stack controller		
16		Switch must support VXLAN Switching/Bridging and VXLAN Routing without any performance degradation		
17		Switch should support Data Center Bridging		
18		Switch should support multi OEM hypervisor environment and should be able to sense movement of VM and configure network automatically through integration with Orchestration layer / VM manager.		
19	Layer 2 Features	Switch should support minimum 80000 no. of MAC addresses. The bidder may propose best specifications as per the proposed solution and city requirements.		
20		Switch should support Jumbo Frames up to 9K Bytes on 1G/10G Ports		
21		Support for broadcast, multicast and unknown unicast storm control to prevent degradation of switch performance from storm due to network attacks and vulnerabilities		
22	Layer 3 Features	Switch should support MPLS		
23		Switch should provide multicast traffic reachable using:		
24		a. PIM-SM		
25		b. PIM-SSM		
26		c. Bi-Directional PIM		
27		d. Support RFC 3618 Multicast Source Discovery Protocol (MSDP)		
28		e. IGMP V.1, V.2 and V.3		
29		Switch should support Multicast routing		
30	Quality of Service	Switch should have a minimum buffer of 12 Mb		
31		Switch should support Flow control of Ethernet ports to control traffic rates during congestion by allowing congested nodes to pause link operation at the other end for receiving traffic as per IEEE 802.3x/VOQ		
32	Security	Switch should support control plane i.e. processor and memory Protection from unnecessary or DoS traffic by control plane protection policy		
33		Switch should support for external database for AAA using:		
34		a. TACACS+		

35		b. RADIUS		
36		Switch should support for Role Based access control (RBAC) for restricting host level network access as per policy defined		
37		Should support Standard / Extended ACLs		
	Manageability	Switch should support for predefined and customized execution of script for device manage for automatic and scheduled system status update for monitoring and management		
38		Switch should support Real time Packet Capture using Wire shark in real time for traffic analysis and fault finding		
S. Leaf Switch - Copper				
1	Solution Requirement	The Switch should support non-blocking Layer 2 switching and Layer 3 routing		
2		There switch should not have any single point of failure like power supplies and fans etc should have 1:1/N+1 level of redundancy		
3		Switch and optics must be from the same OEM		
4		Switch should support the complete STACK of IP V4 and IP V6 services.		
5	Hardware and Interface Requirement	Switch should have the following interfaces:		
6		a. 48 x 100mb/1G RJ45 Interface		
7		b. 2 x 40/100GbE QSFP ports populated		
8		Switch should support IEEE Link Aggregation and Ethernet Bonding functionality to group multiple ports for redundancy		
9	Performance Requirement	The switch should support atleast 60000 IPv4 and IPv6 or more routes entries in the routing table with multicast routes. The bidder may propose best specification as per the proposed solution and city requirements.		
10		The switch should support hardware based load balancing at wire speed using LACP and multi chassis ether channel/LAG		
11		Switch should support minimum 690 Gbps of switching capacity		
12		Each leaf should have connectivity to all spine switches and the over subscription should not be less then 4:1		
13	Advance Features	Switch should support Network Virtualization using Virtual Over Lay Network using VXLAN (RFC 7348)		
14		Switch should support VXLAN (RFC7348) and EVPN		

		or equivalent for supporting Spine - Leaf architecture to optimize the east - west traffic flow inside the data center		
15		Switch should support Open Flow/Open Day light/Open Stack controller		
16		Switch must support VXLAN Switching/Bridging and VXLAN Routing without any performance degradation		
17		Switch should support Data Center Bridging		
18		Switch should support multi OEM hypervisor environment and should be able to sense movement of VM and configure network automatically through integration with Orchestration layer / VM manager.		
19		Switch should support minimum 80000 no. of MAC addresses. The bidder may propose best specifications as per the proposed solution and city requirements.		
20		Switch should support Jumbo Frames up to 9K Bytes on 1G/10G Ports		
21		Support for broadcast, multicast and unknown unicast storm control to prevent degradation of switch performance from storm due to network attacks and vulnerabilities		
22	Layer 3 Features	Switch should support MPLS		
23		Switch should provide multicast traffic reachable using:		
24		a. PIM-SM		
25		b. PIM-SSM		
26		c. Bi-Directional PIM		
27		d. Support RFC 3618 Multicast Source Discovery Protocol (MSDP)		
28		e. IGMP V.1, V.2 and V.3		
29		Switch should support Multicast routing		
30		Switch should support for BFD For Fast Failure Detection		
31		Quality of Service	Switch should have a minimum buffer of 12 Mb	
32	Switch should support Flow control of Ethernet ports to control traffic rates during congestion by allowing congested nodes to pause link operation at the other end for receiving traffic as per IEEE 802.3x/VOQ			
33	Security	Switch should support control plane i.e. processor and memory Protection from unnecessary or DoS		

		traffic by control plane protection policy		
34		Switch should support for external database for AAA using:		
35		a. TACACS+		
36		b. RADIUS		
37		Switch should support for Role Based access control (RBAC) for restricting host level network access as per policy defined		
38		Should support Standard / Extended ACLs		
39	Manageability	Switch should support for predefined and customized execution of script for device manage for automatic and scheduled system status update for monitoring and management		
40		Switch should support Real time Packet Capture using Wire shark in real time for traffic analysis and fault finding		
T. Next-generation Firewall with IPS and anti-APT				
1	Hardware Architecture	The proposed solution/appliance MUST be upto Layer 7 protection. There should be no performance degradation in the overall transaction processing. The solution shall be deployed in HA mode in the DC/ICCC.		
2		The appliance based security platform should be capable of providing firewall, application visibility, and control, VPN functionality in a single appliance.		
3		The proposed firewall appliance should have at least 12 ports of 10/100/1000 and minimum 4 ports of 10 Gig SFP+ ports with separate management and 2 * 40 G ports from Day one		
4		Proposed Firewall should not be proprietary ASIC based in nature & should be open architecture based on multi-core cpu's to protect & scale against dynamic latest security threats. The appliance hardware should be a multicore CPU architecture with a hardened 64 bit operating system to support higher memory		
5		The proposed solution should have dual redundant power supply and redundant hot swappable fans.		
6		Firewall Should consume 1RU Form Factor.		
7	Performance & Scalability	Should support at least 10 Gbps NGFW throughput under real world production Conditions. This throughput should include FW,IPS/Threat		

		Prevention and AVC.		
8		Should support minimum 5 Gbps of IPsec VPN throughput.		
9		Firewall should support at least 8 Million concurrent sessions with AVC feature turned on.		
10		Firewall should support at least 65,000 connections per second with AVC feature turned on.		
11		Firewall should support at least 1000 VLANs		
12	Next Generation Firewall Features	Firewall should provide application detection for DNS, FTP, HTTP, SMTP,ESMTP, LDAP, MGCP, RTSP, SIP, SCCP, SQLNET, TFTP, H.323, SNMP		
13		Firewall should support creating access-rules with IPv4 & IPv6 objects simultaneously		
14		Firewall should support operating in routed & transparent mode		
15		Should support Static, RIP, OSPF, OSPFv3 and BGP		
16		Firewall should support manual NAT and Auto-NAT, static nat, dynamic nat, dynamic pat		
17		Firewall should support Nat66 (IPv6-to-IPv6), Nat 64 (IPv6-to-IPv4) & Nat46 (IPv4-to-IPv6) functionality		
18		Firewall should support Multicast protocols like IGMP, PIM, etc		
19		Should support security policies based on security group names in source or destination fields or both		
20		Should support capability to limit bandwidth on basis of apps / groups, Networks / Geo, Ports, etc		
21		The detection engine must be capable of detecting and preventing a wide variety of threats (e.g., malware, network probes/reconnaissance, VoIP attacks, buffer overflows, P2P attacks, zero-day threats, etc.).		
22		The solution must be capable of passively gathering information about network hosts and their activities, such as operating system, services, open ports, client applications, and vulnerabilities, to assist with multiple activities, such as intrusion event data correlation, elimination of false positives, and policy compliance.		
23	The solution must be capable of dynamically tuning IDS/IPS sensors (e.g., selecting rules, configuring policies, updating policies, etc.) with			

		minimal human intervention.		
24		Should support Application Visibility and Control (AVC) supports more than 10000 application-layer and risk-based controls that can invoke tailored intrusion prevention system (IPS) threat detection policies to optimize security effectiveness.		
25		Proposed appliance should also provide Reputation- and category-based URL filtering offers comprehensive alerting and control over suspect web traffic and enforces policies on hundreds of millions of URLs in more than 50 categories		
26		The solution must provide a full-featured capability to detect threats		
27		The NBA capability must provide the option of supplying endpoint intelligence to the IPS for correlation against intrusion events to aid in event impact prioritization.		
28		The solution shall provide on-premise/cloud based sandbox technology where the objectionable content may be executed and inspected.		
29	High-Availability Features	NG Firewall should support Active/Standby failover.		
30		Firewall should support ether channel or equivalent functionality for the failover control & date interfaces for provide additional level of redundancy		
31		Firewall should support redundant interfaces to provide interface level redundancy before device failover		
32		Firewall should support 802.3ad Ether channel or equivalent functionality to increase the bandwidth for a segment.		
33	Management	The management platform must be accessible via a web-based interface and ideally with no need for additional client software		
34		The management platform must provide a highly customizable dashboard.		
35		The management platform must be capable of integrating third party vulnerability information into threat policy adjustment routines and automated tuning workflows		
36		The management platform must be capable of role-based administration, enabling different sets		

		of views and configuration capabilities for different administrators subsequent to their authentication.		
37		Should support REST API for monitoring and config programmability		
38		The management platform must provide multiple report output types or formats, such as PDF, HTML, and CSV.		
39		The management platform must support multiple mechanisms for issuing alerts (e.g., SNMP, e-mail, SYSLOG).		
40		The management platform must provide robust reporting capabilities, including a selection of pre-defined reports and the ability for complete customization and generation of new reports.		
41		The management platform must risk reports like advanced malware, attacks and network		
42		The management platform must include an integration mechanism, preferably in the form of open APIs and/or standard interfaces, to enable events and log data to be shared with external network and security management applications, such as Security Information and Event Managers (SIEMs), and log management tools.		
U. Gateway level anti-virus and anti-spam security solution				
1	General	The solution should provide a comprehensive email security solution that integrates against inbound and outbound, Internal defences against email threat such as spam, virus, etc. Solution should cater to minimum 2,000 User. The solution shall be hardware appliance based.		
2		The solution should be appliance based. Appliance should support ant-spam, anti-virus , outbreak filter, on appliance detail reporting and on-appliance quarantine handling. Same appliance should have provision to integrate or run Advance malware protection for future requirements.		
3		The appliance based Solution should be provided with Proprietary Operating System and MTA on appliance and not open source operating system (send mail, qmail or postfix).		
4		Appliance should have 1.8 TB hot swappable HDD and RAID support		
5		Appliance should have at least 2 hexa core		

		processor and 32 GB RAM		
6		The solution should have performance capability of processing at least 1,00,000 message per hour. The salutation should support at least 4 * 10/100/1000 copper interface.		
7		Appliance have option for DC power, if require		
8		The solution should be IPV6 ready		
9		The solution should be protect Directory Harvesting attacks.		
10		The solution should support LDAP integration and synchronization. LDAP integration should be used defining policies and when delivering mails.		
11		The solution should support multiple email domains on the same system for each domain a specific destination mail server can assigned for delivery.		
12		The solution should be supplied including all hardware, accessories, license, software with pre-hardened operating system. Hardware should be from same OEM		
13	Inbound SMTP Protection (SPAM)	The solution should combine sophisticated content based Anti-Spam technology ,IP reputation and RBL to effective block spam		
14		The solution should accurately filter/detect more than 99% of spam		
15		The solution should support email authentication using SPF (Sender Policy Framework).		
16		The solution should support Domain Key Identified Mail(DKIM) verification of email messages.		
17		The solution should support lookup to the cloud/on appliance to perform sender, message and IP reputation to effectively block spam.		
18		The solution should support defining custom bypass for the sender IP for the IP reputation.		
19		The solution should support anti-relay. It should have capability to configure domain to which to solution accept or refuse mail.		
20		The solution should support RBL lookup .It should support adding of multiple RBL list.		
21		The solution should have an option to block mail by sender domain address .		
22		The solution should have an option to block mail by sender email address.		
23		The solution should support scouring or signature		

		to detect spam. Based on a severity a different action should be configured .		
24		The solution should support anti-phish scanning.		
25		The solution should offer various action offers for spam detect such as monitor, block, quarantine, forward etc.		
26	Anti-virus Protection	The solution should proposed contain a network level solution for the SMTP traffic.		
27		The solution should have ability to block Malware etc.		
28		The solution should protect against mass mailing worm.		
29		The solution should contain an option to configure scan all file or specific file type.		
30		The solution should contain an option to scan archive file.		
31		The solution should have ability to perform reputation analysis. It should ability to send to suspicious file information to the cloud analysis.		
32		The solution should contain an option to configure the maximum size of attachment file, in case size is exceeds the antivirus solution block all or pass all files.		
33		The solution should contain an option to configure the maximum nesting level of attachment file. in case size is exceeds nesting level the antivirus solution should block all or pass the file.		
34		The solution should offer various actions for virus detect clean, quarantine, deliver or forward etc.		
35		Outbound SMTP Protection		
36		The solution should able to monitor and protect mail flowing out of network in SMTP traffic.		
37		The solution should allow to administrator to automatically add text to outbound mail such as legal disclaimer.		
38		The solution should perform image based filtering- It should analyse image to determine attributes that indicate the image has malicious targeted attack payload and zero day malware by removing exploitable content from office and pdf attachments along with pornographic or non-pornographic images.		
39		The solution should contain an option to configure maximum message size. In case message size		

		exceed the mail should be blocked or quarantine.		
40		The solution should contain an option to configure maximum attachment size. In case attachment size exceed the mail should be blocked or quarantine.		
41		The solution should support file category/file extension wise filtering/blocking. Categories should include document, database, multimedia, archive etc.		
42		The solution should support handling of encrypted content.		
43		Appliance should support integration with DLP		
44		Appliance should support Email encryption on the same appliance		
45	Policy Creation & Management	The solution should provide granular policy for Inbound, Outbound and Internal traffic.		
46		The solution should be able to create specific policy based on.		
47		1. Source/Destination IP address.		
48		2. Sender/Recipient email address.		
49		3. Alias recipient email address list.		
50		4. LDAP user group.		
51		5. Masquerade sender email address		
52		The solution should be able to create specific policy message security such as TLS		
53	Email Management	The solution should able to manage the email in the message queue though the GUI.		
54		The solution should able to view the status of all messages in the queue for the GUI.		
55		The solution should able to filter and view message that was		
56		1.Block, 2.Bounced, 3.Delivered, 4.Quarantined, 5.Queued		
57		The solution should able to filter and analyse message using:		
58		1.Sender, 2.Recipient, 3.Subject, 4.Inbound/Outbound, 5.Date, 6.Source IP		
59		The solution should offer a wide range option to the message in the queue such as Delete, Retry, Forward, etc.		
60		The solution should support end-user quarantine. Is it with buttons and click boxes that enable the user to release e-mail, report false positives, add senders to allow-or-block lists and direct links to		

		personal email management portal.		
61		The solution should support on box quarantine or dedicated quarantine appliance.		
62		The solution should have configurable retention period for spam email or events.		
63	System Administration	The solution should support restricted access to the system for management though SSH/web GUI. Administrator should able to specify a list of authorize access.		
64		The solution should provide the real-time health status of all modules on the dashboard for CPU, memory utilization, total number of concurrent connections etc.		
65		The solution should automatically backup all configurations on the system at specific time.		
66		The solution should offer various built in report etc.		
67		1. Overall message summary		
68		2. Inbound message summary		
69		3. Outbound message summary		
70		4. Spam and virus summary		
71		5. Message transfer summary		
72		6. System capacity		
73		The solution should offer alerting capabilities, including e-mail and SNMP/SIEM		
74		The solution should be automatically security update . Vendor should provide update and security enhancement to operating system, MTA, and supporting software include antivirus and anti-spam engine.		
75		The solution should able to generate report in PDF/HTML/Other Format.		
76		The solution should support inbuilt troubleshooting tools to troubleshoot issue.		
77		i. Built-in command to consolidate diagnostic information and configuration and send to customer support		
78		ii. Ability to enable remote tunnel support for remote diagnosis		
79		The solution should analyze email content and attachment of various file type (true file type) to remove malicious active content including embedded URLs that pose a security risk and reconstruct clean document as attachment.		

		Solution must execute on premise all potentially malicious URLs and allow only safe content to be sent to user.		
V. Web Security Appliance				
1	Appliance Requirement and Functionality	The solution should be a hardened Web Proxy, Caching, Web based Reputation filtering, URL filtering, Antivirus and Anti-malware appliance. All the functionalities should be in a single appliance only.		
2	Hardware	Minimum of 1 * 6-core CPUs, Minimum 2.4 TB storage, RAID 5 or 10, 32 GB or more, hot-swappable hard drive		
3	Operating System	The appliance based Solution should be provided with hardened Operating System.		
4	Operating System Performance	The underlying operating system and hardware should be capable of supporting atleast 2000 users from day with licenses & scalable upto 5000 users.		
5	Operating System Security	The operating system should be secure from vulnerabilities and hardened for web proxy and caching functionality.		
6	Forward proxy mode	The solution should support explicit forward proxy mode deployment in which client applications like browsers are pointed towards the proxy for web traffic.		
7	Transparent mode	The solution should also support transparent mode deployment using WCCP v2 and L4 switches/PBR (Policy based Routing)		
8	Pac File support	The appliance should support hosting proxy auto-config files that defines how web browsers can automatically choose the appropriate web proxy for fetching a URL.		
9	Support multiple deployment options	The solution should allow to deploy the appliance in explicit proxy as well as transparent mode together.		
10	Proxy Chaining	The solution should support proxy configuration in a Chain. The Lower end proxies at spoke locations should be able to forward the request to an Higher end proxies at Hub Location forming a Chain of Proxies		
11	DNS Splitting	The solution should support configuration to use Split DNS. It should be able to refer to different DNS for Different Domains e.g. (root dns for all external domains and internal DNS for organization domain		

12	IP Spoofing support in transparent mode deployments	The solution should have facility to do IP spoofing. When enabled, requests originating from a client should retain the client's source address and appear to originate from the client instead of the appliance. This is useful in scenarios where policies are based on original IP and logging/reporting is required to track activity of individual IP basis.		
13	High Availability	Provision of active/active High Availability is required		
14	Proxy support	The proposed solution should be a Fast Web Proxy and should support HTTP, FTP and HTTPS proxy.		
15	HTTPS Decryption	The solution should support HTTPS decryption		
16	HTTPS decrypted traffic scanning	The solution should support scanning of the https decrypted traffic by the on-board anti-malware and/or anti-virus engines.		
17	HTTPS decryption policy	HTTPS decryption should provide flexibility to have multiple decryption policies and should not be just a Global action		
18	File download and size restrictions	The solution should be capable of blocking specific files downloads and based on size and per user group basis. It should also provide option to block object using MIME File types.		
19	IP based Access Control	The solution should allow administrator to define access to internet based on IP addresses OR range of IP addresses subnet OR CIDR basis. It should also support to be forced for Authentication from Specific IP addresses, Subnet or CIDR's		
20	User based Access Control	The solution should support integration with active directory and/or LDAP. This should allow administrator to define user or group based access policies to Internet		
21	Multiple Authentication Server Support	The solution should support Multiple Auth Servers / Auth Failover using Multi Scheme Auth (NTLM and LDAP). It should also support authentication exemption.		
22	Application and Protocol Control	The solution should support granular application control over web eg. Facebook controls like block file upload, block posting text, enforcing bandwidth limits on application types.		
23	Layer 4 Traffic Monitoring	Should detect Phone Home attempts occurring from the entire Network. It should support actions to allow traffic to & from known allowed & unlisted addresses & block traffic to & from known malware addresses & should support monitoring		

		suspected malware addresses.		
24	Bandwidth restrictions	The solution should support providing bandwidth limit/cap for streaming media application traffic. This should be possible at the Global level as well as at a per policy level.		
25	Anti Malware	The appliance should support Anti Malware/Anti-Virus engine that can scan HTTP, HTTPS and FTP traffic for web based threats, that can range from adware, browser hijackers, phishing and pharming attacks to more malicious threats such as rootkits, Trojans, worms, system monitors and Keyloggers and as defined by the organizations policy. Please mention the antimalware engine.		
26	Anti-Malware	AV/Anti-Malware engine scanning when a URL causes different verdicts from the scanning engine the appliance should perform the most restrictive action.		
27	Web Reputation	The solution should provide Web Reputation Filters that examine every request made by the browser (from the initial HTML request to all subsequent data requests) – including live data, which may be fed from different domains to assign a web based score to determine the likelihood that it contains url-based malware.		
28	Customizable Web Reputation	The Appliance should have customizable setting in the Web Based Reputation Services, like Allow, Scan and Block based on the scoring settings by the Administrator.		
29	Incoming/Outgoing Traffic scanning	The solution should scan for Incoming and outgoing traffic.		
30	Outbound connection control on all ports and protocols	The solution shall provide option to scan all HTTP/HTTPS/FTP ports detecting and blocking spyware activity trying to connect to the outside Internet.		
31	Custom URL filtering	The solution should support creation of custom URL categories for allowing/blocking specific destinations as required by the Organisation.		
32	Url Filtering Options	The web Proxy should support following actions like allow, monitor, block, time-based access. Should also support displaying a warning page but allows the user to continue clicking a hypertext link in the warning page.		
33	Dynamic	Provision should be available to enable Real Time		

	Categorization	Dynamic categorization that shall classify in real time in case the URL the user is visiting is not already under the pre-defined or custom categories database.		
34	Reporting Mis-categorization	The solution should have facility for End User to report Miscategorisation in URL Category.		
35	URL check & submission	Support portal should give facility to end user to check URL category and submit new URL for categorization		
36	Filtering Content	Solution should support filtering adult content from web searches & websites on search engines like Google.		
37	Signature based application control	The solution should support signature based application control.		
38	End User Notification	Solution should support following end user notification functionalities.		
39		The proxy should support the functionality to display a custom message to the end user to specify the reason the web request is blocked.		
40		When the website is blocked due to suspected malware or URL-Filters it should allow the end user to report that the webpage has been wrongly misclassified.		
41		The solution should support the functionality of redirecting all notification pages to a custom URL to display a different block page for different reasons.		
42		Should support the functionality to force users to explicitly agree to the terms and conditions for browsing the World Wide Web from the organization's network to let the user know that the Organization is monitoring their web activity.		
43	Remote support	The remote support from principal company should be available via India Toll Free and Email. The Support Portal access should be provided for Case management, knowledgebase, new version information, tools etc.		
44	Secure Remote Access	The Support Engineers should be able to login to appliance using secure tunneling methods such as SSH for troubleshooting purposes		
45	Diagnostic Tools	The appliance should have diagnostic network utilities like telnet, trace route, nslookup and tcpdump/packet capture.		

46	Updates and Upgrades	The appliance should provide seamless version upgrades and updates.		
47	Secure Web Based management	The appliance should be manageable via HTTP or HTTPS		
48	CLI based management	The appliance should be manageable via command line using SSH		
49	Serial Console access	For emergency, the appliance should have serial console access		
50	Ethernet Management	Should have provision for separate Ethernet for managing the appliance		
51	Web Logs	The Proxy Log should be scalable. The log formats shall include Apache, Squid and W3C.		
52	Retention Period	The retention period should be customizable. Options should be provided to transfer the logs to an FTP server using FTP or SCP.		
53	User Reports	Informative and exhaustive set of reports on User Activity and URL filtering activities (GUI to report past activity, top usage users and top malware threat)		
54	Bandwidth Reports	Reports on Bandwidth Consumed / Bandwidth Saved		
55	Detailed logging	Product to maintain detailed proxy access logs that can be searched via filters, for easy location of any desired access of the user and to see how the product dealt with it		
56	Blocked by reputation &malware reports	It should support reporting web requests blocked due to web reputation & blocked by malware		
57	Report Formats	Solution should support generating a printer-friendly formatted pdf version of any of the report pages. Should also support exporting reports as CSV files.		
58	Scheduling of Reports	Solution should support to schedule reports to run on a daily, weekly, or monthly basis.		
59	System Reports	Should support system reports to show CPU usage, RAM usage, percentage of disk space used for reporting & logging.		

W. Network Behaviour Analysis

1	General Requirement	Perform Full Packet Capture of network traffic with zero packet loss		
2		Support the retrieval of relevant packets to a cyber security incident		
3		Support importing archived PCAP files for analysis		
4		Support importing other structured and		

		unstructured content for analysis		
5		Index all the data in the packets to simplify navigation across data silos		
6		Enable search-driven data discovery of packet metadata AND content for incident		
7		Allow for retracing the activities of an entity in a chronological order		
8		Perform full reconstruction of assets transferred, accessed and transmitted		
9		Provide a visual representation of relationships between entities (IP, email ids, etc)		
10		Highlight potentially malicious or suspicious content		
11		Allow for assigning security analysts to specific security incident investigations		
12		The solution should have capability to integrate with SIEM to have unified visibility		
13		Solution should be sized for traffic rate of 1Gbps or higher		
14		Raw packet capture and meta data should be retained for desired duration		
15		The solution must have feature for root cause analysis and while PCAP import the System is performing LIVE packet capture of the network		
16		Anomaly Detection – find anomalous traffic patterns occurring in your network		
17		-Provide a visual representation of relationships between entities (IP, email ids, etc)		
18		-Highlight potentially malicious or suspicious content		
19		3rd Party Threat Feed integration – add live-feeds, like Snort, quickly and easily. Reputation Services provide added value and threat intelligence		
20		Should be able to remediate Endpoints from the same console		
21		Should have ability to filter, view timeline, or readily access Email and IM artifacts in one pane of glass		
22		3rd Party Threat Feed integration – add live-feeds, like Snort, quickly and easily. Reputation Services provide added value and threat intelligence		
23		Should be able to remediate Endpoints from the same console		
24		Should provide Regeneration and Playback		

		functionality: Ability to create shadow networks. Regeneration and Playback: Point and click to instantly regenerate traffic (at configurable speeds) to a chosen NIC on a shadow network for further analysis in 3rd party systems. Without interruption of regular services		
25		Should be an on-premise appliance-based solution with capability to do packet capture, storage, protocol dissection for 3000+ applications		
26		Should capture all packets from network in real time and be able to classify, extract and analytics, reconstructs network activity and forensics over IPv4 and, IPv6		
27		Should be able to provide complete packet-by-packet details pertaining to one or more session of interest including voice/video replay, page reconstruction, image views, artifact & raw packet extractions		
28		Should include Directly Attached Storage with minimum 300TB capacity and should be scalable to 1.5 PB		

X. Privileged Identity Management				
S.No.	Item	Minimum Requirement Description	Compliance (Yes/No)	Deviation/Marks
1	PIM.001	The solution should have preventions policies applied in breach scenarios or as a way to move from monitoring to prevention for privileged password & The solution must enable organization to closely control and monitor all applications within the environment.		
2	PIM.002	The solution should provide fine grained User Control. The proposed solution must allow controlling actions and access to resources such as target servers/network devices of all privileged accounts such as root / administrator. The solution must track the "real user" even in case of surrogates.		
3	PIM.003	The solution should provide Rights Delegation. The proposed solution must provide the ability to designate specific users as Administrators, Auditors, and Password Managers etc. with appropriate rights. The proposed solution must also provide the ability to designate specific users as Subordinate or Group Administrators, to manage users and file permissions for their		

		group.		
4	PIM.004	The solution should support cross platform management. The proposed solution must support management and policy distribution across various OS platform like Windows, Linux,UNIX, Windows application (Windows Service, Schedule tasks, IIS etc.) security (firewall, IPS, Proxy etc.) & network device (router & switches platforms from a central management console. It must support the deployment of the same policies across multiple servers ensuring consistency of security policies across machines in the enterprise.		
5	PIM.005	The solution should intercept and verify every request to change user identity and maintain a reliable audit trail.		
6	PIM.006	The solution must provide support for IPv6.		
7	PIM.007	The solution should provide exploit prevention techniques to shield the OS, applications and services by defining acceptable behaviours and limited false positives.		
8	PIM.008	The solution should support high availability and should not have a single point of failure		
9	PIM.009	The solution should also support multifactor authentication while logging in utilizing tokens, OTP and passphrases.		

7.12.Unified Collaboration Solution

The proposed Unified Collaboration Solution should be software(virtual) based PBX capable of providing following functionalities, The Collaboration Client application must enable streamline communications and enhances productivity with integrated presence, IM, voice and video, voice messaging, call queuing, desktop sharing, and conferencing capabilities. The System must be capable of calling between operator and outside PSTN or mobile network. The system should have capabilities of achieving collaboration between any users of control room. It must be possible to record all session Audio ,Video, Data for training/records purpose. Also, the system should have capabilities of enabling meetings between admin / other users for taking updates on day to day operations. The Collaboration Solution should natively comply to TRAI Regulations. The Collaboration solution should have capability to integrate with Emergency Response/Radio Dispatch system.

The solution must comprise of following equipment's with quantities as specified in the RFP document at respective locations: IP Phones, Soft phone clients, fully integrated HD Video Conferencing unit, Advanced Collaboration Interactive unit, Multipoint control unit and an IP PBX

capable of managing all devices present in the system. The proposed system should be capable of recording of min 10 concurrent meeting/session (audio, video, data). A PRI Voice Gateway should be provided in High-Availability mode to interface with the external world.

A. Soft Phone Specifications

The IP based telephone exchange system shall also provide following Unified Communication Services/Facilities as a minimum. The OEM of this UC services/facilities shall be same as that of IP based telephone exchange system and integration of UC server with the basic Communication Server shall be purely on IP. The UC application shall have a friendly, intuitive and easy to use graphical interface that informs in real time the multiple states of presence using the user-defined list.

S.No.	Item	Minimum Requirement Description	Compliance (Yes/No)	Deviation/Marks
1	Unified Communications Client Features	The presence shall use icons and colours and shall include at least: On-Line Telephony		
2		Presence/Status, User-Choice Presence (Busy, be right back, Away, out to lunch / meeting etc), Calendar Presence, coming from Microsoft Outlook calendar (if integrated).		
3		The solution must be able to support one-to-one and multi-party messaging		
4		It must support ability to send Multimedia (Text, voice, video and photo) messages between users		
5		Conversation persistency should be maintained so that users can view and participate in active conversations from multiple messaging applications, until they leave the conversation		
6		It must support notification events for all new messages		
7		It must support user search for current and active conversations		
8		It should support synchronization with Microsoft Active Directory 2012		
9		It should support multiple devices like Windows Desktop, Android and IOS on iPhones and iPads.		
10		Users should be able to paste objects, files and URLs into IM message and send it to his contacts		
11		The IM messages must be time-stamped.		
12		The UC Client should be able to IM to group of Users defined by AD.		

13	The UC Client should provide Visual & Audio Tone Alerts on incoming Alerts		
14	Should provide the Presence indicator in IM buddy list and from email message		
15	Should provide Location Indicator: For Ex: Set your own locations like "Work", "Home", "Campus", "Sales Office" etc. so that next time the user signs-in from that office UC Client must remember the location		
16	Should Provide Alert When Available: User should be able to Set the client to notify him/her when a contact becomes available. User should be notified the first time the user next becomes available. A message notification should be given to alert the user that the user is available.		
17	Spell Check must be available in chat		
18	Print Chat: The user should have the ability to print a conversation with a right-click from a chat window with another user or by pressing CTRL + P. the user can also highlight a portion of the text to print it.		
19	AutoSave Chat: From the Options menu, the user should be able to automatically save chats to the user computer, when the user closes a chat window. Once the chats are saved to the user computer, search the chat files or use the windows file search capability to search the chat files. The user can save peer-to-peer and group chat conversations		
20	Client Behaviour at Start Up: The client should have the capability to open in a minimized state to open in the same state that it was in when it was last closed.		
21	Group chat: UC Client must allow users to define custom groups with support upto 600 groups. A group chat session must support up to 1000 users.		
22	Persistent chat: Persistent chat rooms should be supported to share ideas and information in a chat room and should be active even after participants leave the room. When participants come back to the room, they can scroll back to read the messages that they missed. Persistent chat room should have the capability to be		

	password protected		
23	Remove Group Chat Participants: The person who starts a group chat should have the capability to remove group chat participants. Removed chat participants can be re-invited to the chat room at any time.		
24	Size Limit for File Transfers Administrator should be able to configure the file size limit for UC Client users when transferring files.		
25	Screen Capture: UC Client must support screen capture allows a user to capture an area of their screen into an image and then send the image as part of an IM conversation. The image is automatically shown at the far end.		
26	Screen share and Remote Desktop Sharing in Group Chat (1 : Many): Users must have the capability to share screen with up to 5 people in group chat session using the IM-Only-desktop-sharing feature.		
27	The UC Client must support three Default Presence status and should have support for multiple states.		
28	Should have the Provision to adjust presence status		
29	Presence status should be available for communication options		
30	The user profile for IM and Presence is maintained in a common enterprise directory, e.g. existing active directory		
31	IM/Presence system should be able to link with other IM systems (known as Federation) as and when required		
32	Ability to add trusted domains for people outside the company.		
33	Should provide user an option to add external contacts with telephone number only for example add home phone number.		
34	User can conduct separate IM conversations with multiple other Federated IM system users		

35	Voice Integration with IP PBX	The Proposed system, apart from providing IM and presence functionality, should be able to integrate with IP PBX on SIP platform to allow click to call functionality on proposed same client.		
36		Should support basic call control with a consistent client interface on PC, web interface, and mobile device.		
37		Integration should be able to provide: Initiate Call, terminate (Hang-Up Call), Hold, Transfer, Divert if Busy		
38		Should provide mobile VoIP clients on popular smart phone platforms such as Apple iOS and Google Android. Should also provide support for Apple iPad tablets and Android based tablets.		
39		Call Conferencing Capability		
40		Should be able to Initiate a conference call involving multiple participants.		
41		Should be able to Conference with participants using computer audio for voice		
42		Should be able to Conference with participants using IP phone for voice		
43		Should be able to Conference with participants using PBX extension for voice		
44	Video Calling	Video Standard - H.264 and above Should support h.239 or BFCP for content sharing.		
45		Should have the capability of Sending and receiving of video upto 30 fps with 720 p video quality		
46		Ability to put a call on hold and resume the call from a different client associated with that user e.g. Hold the call from a PC and resume the call onto an iPad/Tablet or mobile phone.		
47		The video calling capability to be part of the same client for IM and Presence.		
48		UC clients for Desktop, iOS or Android based tablets should be able to participate in the video conferencing call.		
49		The Desktop client should support easy firewall traversal solution such that there is no need to use VPN client when the user is outside the enterprise network --Internet.		

50		The Desktop client solution should be ready for a to scale for more than 800 users, without any hardware upgrade		
51		The user should be able to make point-to-point video calls without utilizing the MCU.		
52		The video conferencing capability to be part of the same client for IM and Presence.		
53		Ability to put a call on hold and resume the call from a different client associated with that user e.g. Hold the call from a PC and resume the call onto an iPad/Tablet or mobile phone.		

B. Integrated HD Video Conferencing unit with built in HD display, Audio System and Microphone

S.No.	Item	Minimum Requirement Description	Compliance (Yes/No)	Deviation/ Marks
1	Set Delivered Complete With:	The system should be an integrated system with Codec, Dual HD 1080p camera with 20x total zoom or higher, Mic , touch screen/ panel, cables and power supply, single 65" or higher LCD/LED and a floor mount kit.		
2		The 65" screens, codec, cameras, microphones, floor cum wall mounted kit should be from same OEM with a single OEM part code. The system should not be a locally fabricated unit.		
3		The system should be capable giving HD 1080p @60fps.		
4		The system should deliver 1080p@60fps in motion and in sharpness video mode day one.		
5	Bandwidth	H.323, SIP at least 4 Mbps point-to-point		
6	Firewall Traversal	H.460.18, H.460.19 Firewall Traversal		
7	Video Standards	H.263, H.264, H.265		
8	Video Features	Native 16:9 Widescreen		
9		Advanced Screen Layouts so as to view the presentation and presenter in different quadrants and sizes.		
10		Local Auto Layout		
11	Video	Must have a total of at least 4 HD inputs		

	Inputs	The system should have 2 Video Inputs to connect 2 x HD Camera (1080P) and 2 PC Inputs (One HDMI and/or one DVI/VGA) for presentation sharing		
12	Video Outputs	The system should have an integrated LED/LCD/Plasma screen which is at least 65 inches or higher.		
13		Additionally, the unit must have at least two HDMI/DVI outputs to connect additional displays.		
14	Live Video Resolutions (Encode/Decode)	The system should supports Video resolutions from CIF, QCIF, 4CIF, 448p, 576p,w448p, w576p, VGA, SVGA, HD 720p@30fps, 720p@60fps , 1080p@30fps and HD 1080p@60fps, XGA and SXGA. The PC resolution should be WXGA or 720p		
15	Audio Standards	G .711, G.722, G.722.1, 20KHz or better		
16	Audio Features	CD-Quality audio		
17		acoustic echo canceller		
18		Automatic Gain Control (AGC)		
19		Automatic Noise Reduction		
20		Active lip synchronization		
21	Audio Inputs	should have at least 4 microphones inputs-XLR or Euro block to connect 4 microphones.		
22		The system should have one additional Audio line-in Input to connect PC audio and line in audio		
23	Audio Outputs	Built-in wide band audio speaker and amplifier system to the far end audio and line-in audio. No external audio system is acceptable. The unit must provide a sound output of at least 300W		
24	Dual Stream	The system should have the capability to support H.239 in H.323 and BFCP for SIP Mode		
25		The system should support 1080p30 resolution during H.239 call		
26		The system must have the ability to pair mobile devices such as Tablets and Smartphones based on iOS or Android platforms so that these devices can be used for:		
27		1) View the Presentation that is being shown in the VC call.		

28		2) Add and disconnect call.		
29		3) Take snapshot of the presentation being shown		
30		The system must have the ability to pair with laptop for sending content without any wires to the VC system.		
31		In case the above feature is not available natively, then additional components can be provided to achieve this.		
32	Protocols	The system should have H.323 and SIP capability		
33	Embedded Encryption	The system should support AES Encryption. H.239 capability should be supported in an encrypted call. AES encryption is required for complete secure call between locations		
34	IP Network Features	The system should have features such as QoS, RSVP, standards based packet loss based downspeeding, TCP/IP, DHCP , Auto gatekeeper discovery, Dynamic playout and lip-sync buffering, H.245 DTMF tones in H.323, Date and Time support via NTP		
35		Packet Loss based Downspeeding		
36		URI Dialling		
37		Must support IPv4 and IPv6 from day one.		
38	Security Features	The administration of the Video endpoint should be through Web Interface using HTTPS/HTTP		
39	Network Interfaces	1 x LAN/Ethernet (RJ-45) 10/100/1000 Mbit		
40	Camera (1080P)	1/3" CMOS Camera, 20x Total zoom, +15°/-25° tilt, +/- 90° pan, 1920 x 1080 pixels, minimum 72 deg horizontal field of view		
41		Dual cameras must provide the ability of automatically tracking the speaker in a meeting room and zooming onto that person. External disturbances and noise such as mobile phone ringing should not cause the camera to move.		
42		The camera tracking mode must be such that in the event the far end is talking, the cameras must automatically zoom out to capture the entire room.		
43	Adhoc Multipoint Capability	Must have built-in Multiconference capability to connect at least 1+4 sites at 720p in a continuous presence mode		

44		It should be possible to view the presentation in a separate quadrant as well as each of the far end sites in individual quadrants. The far end sites must not appear in only one quadrant together.		
45		All sites must be visible in a continuous presence mode with rate matching and transcoding such that different sites may connect at different speeds and protocols and still maintain a resolution of at least 720p		
46	System Management	Total management via embedded SNMP, Telnet, SSH, XML, SOAP		
47		Remote software upload: via web server, SCP, HTTP, HTTPS, Remote control and on-screen menu system		
48	Directory Services	Support for local directory (My Contacts), Received Calls, Placed Calls		
49	Cables and Connectors	The video endpoint should be accompanied with Power Cable, LAN Cable, DVI to VGA Cable, Power adaptors if any, DVI to HDMI cables		
50	User Interface	In order to provide a good user experience, the unit must be equipped with an intuitive Touch Screen/Panel for controlling the VC unit.		
51		Must have ability to browse the directory, search a contact, Enable / disable speaker tracking, change layouts, mute/ unmute, increase-decrease volume.		
52		Optionally Must have the capability to integrate with external control systems to control Blinds, Lights, air conditioning using the API's . The User interface must have the necessary icons for controlling the external devices		

C. Three Screen Telepresence System

S.No.	Item	Minimum Requirement Description	Compliance (Yes/No)	Deviation/Marks
1		The proposed TP solution should be high definition 1080p@30 fps video.		
2		The proposed TP solution should support high definition 1080p@30 fps content.		

3		The Telepresence system should accommodate minimum 6 participants, with life-size images, around a virtual table, to support an interactive and collaborative, virtual face to face immersive meeting over the network.		
4		Minimum of three High Definition Cameras (1080 P) to cover all the 6 participants in each location. Cameras should be able to provide segmented view of the rooms. The room at each location should be divided into atleast 3 segments. Each segment should be covered by atleast one HD camera.		
5		The Telepresence camera should be 4K HD cameras or better with min. 200 lux illumination		
6		The video conferencing will have business quality transmission. The business quality transmission is defined as 1080p high-definition video resolution at 30 frames per second and 20 kHz or more wide-band spatial audio.		
7		Minimum Three Plasma/ LCD screens, each of atleast 70 inches or a Video Wall based solution at each location supporting atleast HD 1080P@30fps. The screens should be able to display life size images of the participants. At any given instance the screens should be able to display Life like image of at least 6 participants.		
8		Solution should support following video standards H.264 and H.265.		
		Video frame rate should be minimum 30 frames and 60 fps is desirable		
9		Solution should support following voice standards G .711, G.722, or better, Spatial/ stereo audio 20 KHz or higher, Acoustic echo canceller and Automatic Gain Control (AGC)		
10		Should support voice-activated switching of either site-by-site or by individual segment with integrated elimination feature to avoid changes due to stray noises.		

11		Support audio-only participant by integrating audio conferencing bridge into point to-point and multipoint calls		
12		Solution should use standards SIP/H.323 control signalling		
13		The user must have the ability to view the presentation on any of the three screens simply by dragging and dropping the required content via a touch interface . Additionally, the Telepresence unit must have the ability to view the presentation on a dedicated screen.		
14		The solution must comply with standard based video formats like HD 720p and HD 1080p.		
15		The telepresence should be operated using the touch panel for call initiation, disconnection, presentation sharing, volument control etc.		
16		The TP unit should allow the ability to connect more than one presentation source via a laptop or PC.		
17		The system must also have the ability to share presentation without any wires. A laptop on the network must be able to share a presentation if it is in the same room by using an application on the laptop. Typing or configuring of any IP address for presentation sharing is not accepted. This feature can be available as a built-in feature or using any third party component. However bidder has to take full responsibility of the entire set up.		
18		It should be possible to share a 'WhiteBoard' as a presentation source during a meeting. This whiteboard can be wall mounted. This feature can be built-in or can be achieved using additional cameras such as document camera etc or additional third party components. However, bidder has to take full responsibility of the entire set up.		

19		The system must also have the ability to view the presentation on any of the 3 large 65 inch (or higher) LED screen. In case this feature is not available as part of the OEM offering, additional hardware and software components can be added. However bidder has to take full responsibility of the entire set up.		
20		Solution should use standards TIP control signaling protocol to allow for flexibility for interoperability. The solution must comply with standard based video formats like HD 720p and HD 1080p.		
21		The bidder should provide all the relevant software and hardware to achieve above mentioned conferencing requirement.		
22		The proposed system should able to integrate with HD document camera for sharing document during the Telepresence call.		
23		The proposed solution should be IPV6 enabled		
24		The system is required to ensure End to End AES 128 bit encryption for Telepresence calls.		
25		Telepresence system components including 70 inch display screens, speakers, cables, accessories and table should be single OEM sourced. For moveable accessories like Chair and collaboration screens, Vendors may quote third party sourced equipment. Bidders are required to provide supporting documentation from OEM website for the same. Customised solution such as HD video conferencing based boardroom solutions will not be accepted as telepresence system.		

D. IP PBX Specifications

The network must have SIP based call control system. The solution architecture must support call control functionality either centralized or distributed across multiple nodes across WAN for enhanced redundancy. The System should have IP capability for interfacing & communicating with Voice, Video and Data infrastructure along with GUI support for web based management console.

Further, it should be possible to monitor the call control system i.e. system performance, device status, device discovery, CTI applications, voice messaging ports etc.

S.No.	Item	Minimum Requirement Description	Compliance (Yes/No)	Deviation/ Marks
1	General Specifications	A comprehensive IP based solutions based on a Server Gateway Architecture.		
2		Support for integrated telephony solution for Video conferencing devices, Analog & IP Phones, PSTN gateways over IP architecture.		
3		The solution should offer users the ability to use their UC clients and IP Phones outside of the enterprise (Internet) to make audio and video calls along with IM/Presence with or without VPN.		
4		The solution should allow for business to business (B2B) video calls using SIP, H.323 with other organizations without bypassing existing firewalls.		
5		The solution should allow provisioning of gateways with redundant power supplies.		
6	System Architecture	The call control system should be fully redundant solution with NO single point of failures & should provide 1:1 redundancy. Both the server should do call processing all the time and act as backup in case of the failure of one server.		
7		The call control should support clustering over WAN		
8		The proposed system should be Integratable with ACD, IVR.		
9		The call control system should support IPv4 and IPv6 from day one.		
10		The system should natively support tenant partitioning so as to comply with TRAI regulations for not allowing VoIP (CUG calls) and PSTN calls to be bridged. Any third party applications to manage tenant partitioning should not be quoted in the architecture.		
11		The proposed call control server should provide support for standards based SIP IP Phones (Wired & Wireless), Analog Phones, Video Phones, Video Conferencing endpoints and soft clients to provide centralized		

		management and unified dial plan.		
12		Conference Bridge—provides software conference bridge resources that can be used by IP EPABX.		
13		The system should support an inbuilt reporting tool for calls. Reports that are provided include Calls on a user basis, Calls through gateways, Simplified Call Quality.		
14		Should support signaling standards/Protocols – SIP, MGCP, H.323, Q.Sig.		
15		CODEC support - G.711, G.729, G.729ab, g.722, iLBC		
16		The system should provide the ability to perform tasks in bulk i.e. Add, Remove, Update users, phones, gateways, dial plan etc.		
17		The system should support creation of users and their authentication locally and via an integration with LDAP.		
18		The system should support an inbuilt reporting tool for calls. Reports that are provided include Calls on a user basis, Calls through gateways, Simplified Call Quality.		
19		The system should support call admission control to configure number of calls that can be active between locations – intercluster and intracluster.		
20		Call preservation – redundancy and automated failure – on call-processing failure. In progress PSTN calls at each of the locations should not be interrupted in the event of any WAN failure or call control server failure.		
21		Open API should be provided when required which will help to develop customized IP applications which will integrate with call processing.		

22		It is required to provide Survivable Call Control functionality so that the survivable system at the remote location i.e. Media Gateway shall provide fall back call control service in case the remote site loses all connectivity to the main Call Control system placed. It is expected that the survivability call control system will provide a minimal set of essential telephony features to the end-users that could be a subset of the feature that are available from the main call control system.		
23	Security	All the appliances in the call control system should have dual redundant and hot swappable power supply and fans for high availability.		
24		All appliances in the call control system should have hot swappable storage media to ensure high availability.		
25		Support for configuration database (contains system and device configuration information, including dial plan)		
26		Having inbuilt administration web based administration. No additional thick client for administration on the Admin PC. Should also support HTTPS for management.		
27		Access to the system should be secure for the purpose of access over IP network. The protection of signaling connection over IP by means of authentication, Integrity and encryption should be carried out using TLS.		
28		There should be provision of defining password aging, one time passwords. Provision shall be available to bar unauthorized user to connect to the system. The system should monitor and report the following types of security \ violation login Violations, authorization code violation Station security code violations etc.		
29		IP Phones should not support direct, external initiated, connections via HTTP, telnet, FTP, TFTP or any other protocol as means to prevent distributed Denial of Service attack exploitation, except those required for routine firmware upgrades.		

30		Role Based Account Management to define different levels of administrator access depending on specific function responsibility		
31		The system should support complete encryption capabilities with the ability to encrypt all traffic (media and call control signaling) between IP phones, softphones, call controllers, gateways and all other associated endpoints using a strong encryption algorithm (AES, IPsec and SRTP, for example).		
32		All management traffic between the remote console/session and control server should be encrypted (SSH for Direct Command Line Sessions, Interface, HTTPS (SSL) for Web Sessions, SFTP for File Transfer Etc.).		
33		Should support SSL for LDAP directory integration.		
34		All Hardware & Software with license required for providing above Security measures must be incorporated.		
35	System Capabilities Summary	The architecture should support a minimum of 2500 IP phones and VC systems per Server		
36		The architecture should support single Server Clustering to provide scalability to offer support for 30,000 IP devices and also to provide redundancy. All the 30,000 users to be managed in a single database which is managed centrally, no multiple databases.		
37		The System should support Alternate Call Routing		
38		System backups: The management system should have the provisioning for taking manual as well as scheduling of automatic periodic backup of complete system & data.		
39		The System should support Audio message-waiting indicator (AMWI)		
40		The System should have Automated bandwidth selection		
41		Should support SNMP v2, v3		
42	IM & Presence	Solution should provide a "presence" application for users, so that they can see the availability status of their contacts in their contact list.		

43		The common supported status for this application should be available, busy, idle, away etc.		
44		Should support the users to see other user's IP phone's on/off hook states		
45		The instant messaging application should support manual setting of user status to: Available, Away, Do Not Disturb (DND) etc.		
46		Shall provide support for open protocols like XMPP.		
47		Presence based desktop application shall allow escalation of Instant Message to Audio call and further to Video call		
48		Should support management of contact list and personal settings from Presence based desktop application		
49		Should support click to call, click to Video and click to conference features.		
50		The Soft Client should have soft phone capability and should support desktop and iPad based point to point video calls.		
51	Video Telephony Support	The call control system should provide integrated video telephony features to the users so that user with IP Phone / Soft phone and video telephony end point should be able to place video calls with the same user model as audio calls.		
52		The users should be able to transfer video calls as audio calls		
53		Call-Server should provide a common control agent for signaling, configuration, and serviceability for voice or video end points.		
54		Call control system should handle CODEC and video capabilities of the endpoints, bandwidth negotiation to determine if video/audio call can take place.		
55	End user Features required:	Extension mobility		
56		Call forward all		
57		Do not disturb		
58		Hunt groups		
59		Dial-plan partitioning		
60		Distributed call processing		

61		Deployment of devices and applications across an IP network		
62		"Clusters" of Call-Servers for scalability, redundancy, and load balancing		
63		Forced authorization codes and client matter codes (account codes)		
64		H.323 interface to selected devices		
65		Hotline and private line automated ringdown (PLAR)		
66		Interface to H.323 gatekeeper for scalability, CAC, and redundancy		
67		Multi-Level Precedence and Preemption (MLPP)		
68		Multilocation—dial-plan partition		
69		Multiple ISDN protocol support		
70		Prepackaged alerts, monitor views, and historical reports with Real Time Monitor Tool (RTMT).		
71		Trace setting and collection utility		
72		Cluster wide trace setting tool.		
73		Multisite (cross-WAN) capability with intersite CAC		
74		Q.SIG (International Organization for Standardization [ISO])		
75		Video calls to be placed with the same user model as audio calls.		
76		Call-Server should support new video end points.		
77		SIP Video endpoints which should inherit the functionality of audio calls which gives the user the same call model for both video and audio calls.		
78		Call-Server should have the infrastructure to handle codec and video capabilities of the endpoints, bandwidth negotiation to determine if video/audio call can take place, single point of administration, management of media devices such as gateways and MCUs.		
79		Call-Server should provide a common control agent for signaling, configuration, and serviceability for voice or video end points.		

E. High Definition Multipoint Control Unit (MCU) Specifications

S.No.	Item	Minimum Requirement Description	Compliance (Yes/No)	Deviation/ Marks
1	General	All necessary hardware to support the required capacity needs to be supplied from day one. Each of the server supplied for the MCU must have a redundant power supply from day1.		
2		The MCU must have 90 HD ports @720p 30 fps with H.264 AVC and Continuous presence from day1.		
3		All the 90 ports must be able to connect different sites at different bandwidths and protocols. H.264 AVC standard must be supported at the minimum to connect all the 90 sites.		
4		The MCU must be able to host at least 4 simultaneous conferences each having different capacities restricted by the maximum port capacity of the MCU		
5		The MCU must also support Full HD mode and it must provide a capacity of connecting at least 40 sites @1080p30 fps		
6		MCU should be capable of supporting participants using various means i.e. via video enabled phones, room based video endpoints, soft clients on mobile/tablet or via the browser using WebRTC compatible browsers in a single conference. The meeting quality has to be consistent and of high quality. The end points can be present on the WAN network or on the internet. 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 MCU 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 MCU/solution should support H323 and SIP protocols.		
9		The MCU should support geographical redundancy, so that MCU could be placed in DC/DR setup in case future expansion is needed.		

10		The MCU must support the concept of virtual meeting rooms to users who Hosts meeting frequently. Such meeting rooms should support dialing in from standard based video end points, internal and external users and browser based clients. The system should allow one Virtual meeting room per employee, however it should not consume resources when not in use.		
11		The MCU should be able to maintain the dynamic resource allocation capacity for 1080p, 720p and SD participants simultaneously without having to reboot or change any configuration.		
12		The MCU should support 90 ports or more at HD 720p (transmit and receive) up to 4Mbps on IP in continuous presence mode with 30fps, 1500 audio ports, 100 WebRTC connections and H.264 resolution and AES encryption on the same MCU.		
13		The MCU should display a security icon on the endpoint if the conference is secure.		
14		The administrator should be able to specify maximum resolution for main video content.		
15		Video conferencing endpoints deployed at other organization must be able to take part in video conferencing. The endpoints can be of various makes such as Polycom, Cisco, LifeSize etc using open standards.		
16		Interoperability with all organization must be possible using standards based dialing methodology using the Internet.		
17		The MCU should support on-screen text messaging on video endpoints, so that if there's a delay in starting a meeting, participants can be informed.		
18		The MCU should be able to integrated with existing IP PBX to provide audio conferencing ports to phones.		
19		The MCU should be able to integrate with Call Control system using SIP.		
20	Video Standards	Should support H.263, H.263+, H.263++, H.264 AVC , H.264 SVC/H.264 High Profile video algorithms		

21	Video Resolution	Should support video resolution from SD to Full HD to join into a conference		
22		The proposed MCU should be able to combine HD and SD in the same conference without degrading the HD resolution from and to the HD endpoints. The MCU shall interoperate with multiple vendors' endpoints. The supported mediums should be IPv4 and IPv6.		
23	Audio Standards	Along with the support for basic algorithms like G.711 and G.722.1 the MCU should also support wideband Audio protocols like MPEG 4 AAC - LC and MPEG 4 AAC - LD		
24	Transcoding & Rate Matching	The MCU should support transcoding of different Audio/video Protocols.		
25		MCU should be able to combine HD and SD in the same conference without degrading the HD resolution from and to the HD endpoints.		
26	Dual Video	The MCU should have H.239/BFCP protocol for sending and receiving dual video streams (Presenter + Presentation).		
27	Video Layouts	At least 16 sites to be seen simultaneously on the screen in traditional Continuous Presence mode.		
28		The MCU 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.		
29	Security	The MCU must be a secure Non-PC Hardware with a strong operating system. The Hardware and software must be from the same OEM.		
30		The MCU should support 128 Bit strong AES encryption for calls and H.235 for authentication		
31		The MCU must support encryption for calls on SIP.		
32	Network /USB Interface	At least 1 LAN /Ethernet--10/100/1000 Mbps full duplex and dedicated serial/USB connection for maintenance/upgrade.		
33	Conference Layout	MCU Solution should support minimum of 10 layouts		
34	Firewall Traversal	Should support firewall traversal solution for Business to Business (B2B) Video Calling.		

F. IP Phones

S.No.	Minimum Technical Specifications	Compliance (Yes/No)	Deviation/ Marks
1	The phone should support Power over Ethernet IEEE 802.3af class 1/2/3 and should also have AC power adapter option		
2	Should feature a LCD display of at least 3.5" for information such as calling party name, calling party number, and digits dialed to be displayed.		
3	The phone should have two ethernet ports of at least 10/100 BASE-T Ethernet ports, one for the LAN connection and the other for connecting to PC/laptop.		
4	Corporate directory and Lightweight Directory Access Protocol (LDAP) integration.		
5	Ready access to missed, received or placed calls (plus intercom history and directories).		
6	The phone should support QoS mechanism through 802.1p/q.		
7	IP address Assignment by DHCP or statically configured		
8	Hands-free operation with full-duplex speaker-phone		
9	The phone should be a SIP based Phone i.e session Initiation protocol (SIP) supported		
10	The phone should support XML based services & applications.		
11	Should have a distinct LED indicator for message waiting.		
12	Keys for specific functionalities such as – voicemail, directories, settings, transfer, speakerphone, mute on/off, headset etc		
13	Media Encryption (SRTP) using AES		
14	Signalling Encryption (TLS) using AES		
15	Should support 802.1x		
16	Encryption of Configuration Files		
17	The phone should have the ability to register to call control server over an internet link with or without VPN.		
18	The phone should support IPv4 and IPv6 from day1.		
19	The phone should support at least 100 entries for call history i.e. missed, received, placed etc.		
20	It should support the following codecs: G.711a/μ-law, G.722, G.729a, iLBC		
21	The phone should have RJ9 headset port to connect any standards based headset. The phone should also have a separate headset key		

22	The phone also includes the following settings - Display contrast, Ring type, Network configuration, Call status		
23	The Phone should support the ability to provide different ringtones for internal and external calls.		
24	Should have volume control button for easy volume adjustments for the speakerphone, handset and ringer.		
25	The phone should support mounting against a wall		
26	The phone should support 2 programmable lines keys.		
27	The phone should the following features:		
	i. Call forward		
	ii. Call pickup		
	iii. Call waiting		
	iv. Extension Mobility		
	v. Auto answer		
	vi. Message waiting indicator		
	vii. Music on hold		
	viii. Forced Authorization Code (Account Code/FAC)		
	ix. Conference		
	x. Music on Hold (MoH)		
	xi. Corporate directory		
	xii. Auto-detection of headset		
	xiii. Busy Lamp Field (BLF)		
	xiv. Callback		
xv. Immediate Divert			

8. Component 8 : City Communication and Network Infrastructure

8.1. Scope of Work

- 1) MSI should tie up with an Internet Service Provider or Telecom Service Provider to provide connectivity from Field Device Infrastructure to physical location of ICCC and Data Centre / Disaster Recovery Centre at Cloud
- 2) MSI should use public internet for transmission of information between field devices infrastructure to the core router. Required security applications should be factored in to avoid hacks at field devices infrastructure level.
- 3) MSI should estimate the bandwidth requirement for connectivity to desired Cloud Service of DC /DR and the same shall be clearly provisioned in the technical proposal with detailed calculations.
- 4) Connectivity between ICCC and Data Centre / Disaster Recovery Centre shall be mentioned explicitly and approved from ASCL.
- 5) Bandwidth provisioned needs to adhere to following minimum benchmark requirements:
 - I. Latency should be less than 15 ms
 - II. Jitter should be less than 2% of one-way latency
 - III. Packet loss should be less than 0.01%
- 6) MSI shall meet the parameters of video feed quality, security & performance. MSI should factor the same while designing the solution.

8.2. Security Requirements for Network as a Service

- 1) Every field device should be authenticated in the IoT Platform before being able to access to the network resources
 - I. Field devices should use X.509 certificate based authentication
 - II. Certifying Authority chosen, should be mutually agreed upon.
 - III. Along with X.509 certification, Device should also support authentication
- 2) Other information regarding the security is mentioned in IoT Platform section.

8.3. Network Operations Centre

It is proposed that a Network Operations Centre (hereinafter referred to as “NOC”) shall be established for monitoring the network infrastructure through which the connectivity to be established with Service Provider. MSI will have to discuss and get into an agreement with concerned ISP (providing connectivity & bandwidth) for extending their NOC to the City Operation Control Centre.

The NOC shall analyze network problems, perform troubleshooting, communicate with various AMC officials / technicians and track problems through resolution. The key objective of the NOC is to ensure the health and availability of components. When necessary, NOC shall escalate problems to the appropriate stakeholders. The MSI shall develop service catalogue for NOC and get a sign off on the same from purchaser / authorized entity.

The overall Scope of Work (SoW) for the MSI shall be establishing a Network Operation Centre (NOC). Primary responsibilities of NOC personnel shall include but not limited to:

- 1) **Network Supervision and Monitoring:** Monitor the complete network 24/7, to keep network and systems functioning in a stable operation mode
- 2) **Configuration Management:** Ensure the proper configuration of network, systems and applications for the provision of reliable and high-quality end-user services
- 3) **Change Management, Network Extension:** Ensure efficient day-to-day management of short-term network changes and optimization, including their implementation. This activity shall be synchronized with the maintenance scheduled activities
- 4) **Performance Management:** Provide efficient performance management procedures ensuring a reliable, high-quality network performance and service
- 5) **Service and Network Provisioning:** Define all necessary actions to be performed when a request for a new customer service is issued by customer care, and control the actions performed at NOC level or field level until completion
- 6) **Scheduled Activities Planning:** Provide regular plans for all scheduled activities, including preventive maintenance. Respect a schedule, and achievement of the plan. This is linked to the change management function which ensures overall synchronization of all network activities
- 7) **Security Management:** Define and implement security policies, guidelines, and best practices, and check for compliance with security regulations
- 8) **Quality Management:** Define quality management policies, and ensure implementation and usage for competitive quality of service
- 9) **Workforce Management:** Manage field personnel to ensure timely interventions and respect of the preventive maintenance plan
- 10) **Network Inventory Management:** Ensure consistent management of network equipment, and accurate, up-to-date documentation of it
- 11) **Repair and Return:** Receive and repair defective boards, return repaired or replacement boards.

Features of NOC

- 1) Incident Management based on resource workload, incident category etc.
- 2) Tracking and reporting of all contractual SLAs in an automated way.
- 3) Updateable knowledge base for technical analysis and further help end-users to search solutions for previously solved issues.
- 4) The NOC shall escalate issues in a hierarchical manner, so if an issue is not resolved in a specific timeframe, the next level is informed to speed up problem remediation.

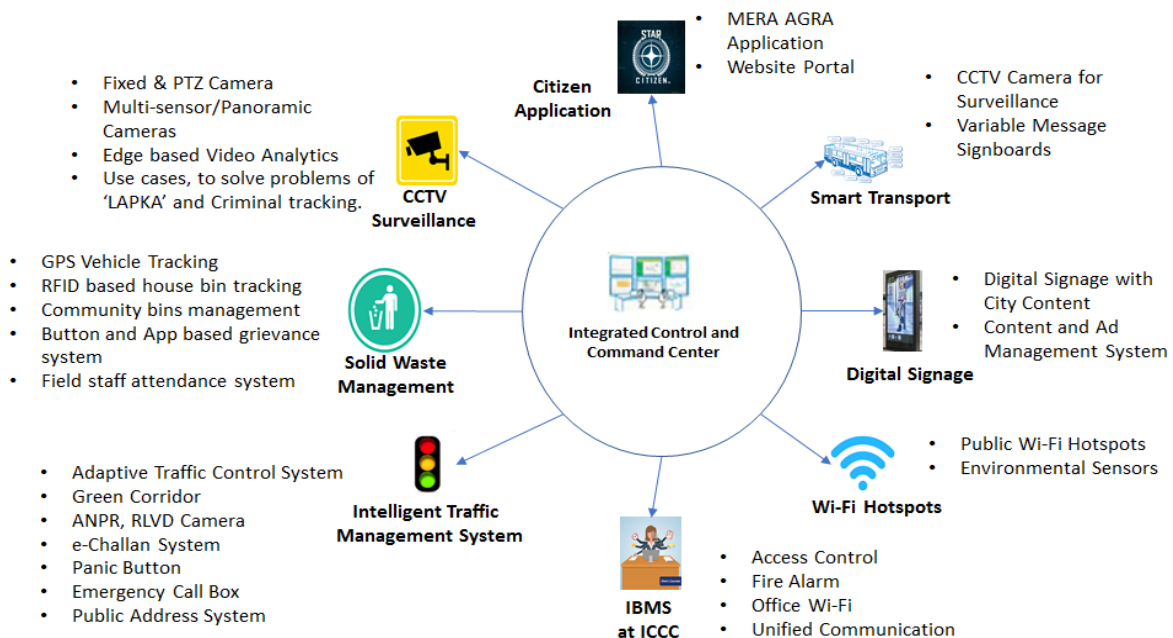
9. Component 9 : Integrated Centralized Command and Control Centre (CCC)

9.1. Overview

City Operation Command Centre (OCC) main objective is break silos between departments and in departments, make process integrated to serve public in an efficient manner. As part of Agra Smart City; it is proposed to build one common operation centre. This centre will provide an integrated view of all smart component projects identified in this document, its primary focus is to serve as a decision support engine for city administrators in day to day operations or during emergency situations.

This centre, shall leverage information provided by various departments and provide a comprehensive response mechanism to the day-to-day challenges across the city. City Operation Centre shall be fully integrated, client-server/web-enabled solution that provides seamless incident – response management, collaboration and geo-spatial display. Various ICT projects shall be able to use the data and intelligence gathered from operations of other elements so that civic services are delivered more efficiently and in an informed fashion.

MSI shall develop application module for the smooth operation of City Operation Command Centre, and shall deploy support and maintenance manpower at the OCC. 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 to have a proven Enterprise Management System (EMS) for the efficient management of the system, reporting, SLA monitoring and resolution of issues.



State-of-the-art Command Control Centre is required to be established as part of the City Surveillance solution. The proposed CCC shall handle feeds from field cameras and display them on the video wall in the CCC and shall provide necessary interface for integrating with other applications and response mechanism as required by ASCL, it shall present a Common Operating

Picture (COP) of real time events in the area of surveillance. Functions of the Command Control Centre shall include but not limited to the following:

- Video Surveillance
- Video Investigations
- Emergency Response activities
- Video data storage & retrieval

Command Control Centre shall work in fully automated environment for optimized monitoring, regulation and enforcement of traffic with various law enforcement services. Various applications/ modules like ANPR/RLVD/E-Challan specified in this RFP shall be integrated into one functional system and shall be accessible by operators and concerned agencies with necessary login credentials. The operators shall be able to access master data like Vahan and Sarathi databases (that are available with the government agencies which can be integrated). The integration with such systems will be in the scope of MSI.

Location for Command Control Centre shall be provided by ASCL. Responsibilities of MSI shall include site preparation activities. MSI shall ensure that the Command Control Centre shall manage, control and integrate various systems in a seamless manner. Command Control Centre shall provide a comprehensive system for planning, optimizing resources and response. The system shall thus be an “end to end” solution for safeguarding and securing people and assets.

MSI shall be required to undertake detailed assessment of requirements at Command Control Centre and prepare a plan to implement Command Control Centre and commission required IT and non-IT infrastructure and civil/structural/ electrical work as required.

Data and surveillance network shall share the same physical infrastructure with guaranteed bandwidth for each individual segment. The software components should provide comfortable monitoring experience, easy extraction of clips and management of storage.

The video feed from surveillance cameras shall be received at Command Control Centre where a video wall shall be installed for viewing. The surveillance team shall receive live feeds from surveillance camera and shall also control PTZ camera using joysticks. They shall be alerted if an incident is detected through video content analytics, ANPR/RLVD system, events generated from various sensors sending feed to Command Control Centre and shall be able to view relevant feed from surveillance cameras. The operator on each workstation shall be able to work on multiple monitors at the same time, for which there multi screens with one computer (specifically three) to be installed on work desks (with appropriate furniture) with appropriate multi monitor mounts.

9.2. Project Intent

The Command Control Centre will be the nerve center for monitoring and management of all surveillance cameras for crime management and traffic enforcement and all smart city solutions. The center will have a video wall which will display the status of various ICT

applications and video feed from various field CCTV cameras. The CCC will be manned by at least 30 operators and will be equipped with all office infrastructure such as cubicle, cabins, conference, meeting room, etc. A common Data Centre and Disaster Recovery Centre for the CCC and OCC will house the entire IT and related infrastructure.

9.3. Scope of Work

- 1) MSI should inspect the location and factor in amount of work needed to build ICCC in the bid document. MSI should provide a universal dashboard to view all applications in a consolidated manner on GIS map provided by ASCL and also general KPI View.
- 2) MSI should be able to provide Unified view for each Departments on GIS map and general KPI views.
- 3) MSI should also continuously monitor Field infrastructure / Servers / Routers and physical infrastructure with Logical resources of Hosted Datacentre or Cloud Based Services
- 4) KPI's which need to be tracked & projected on video wall shall be agreed during inception stage
- 5) Key KPI for each domain needs to be tracked:
 - KPI's list given are indicative and a detailed list of KPI's need to be furnished by MSI during feasibility study
 - KPI's should include from the following categories
 - Process KPI: KPI's which measure the efficiency of integrated processes
 - Event Based KPI
- 6) System should create new KPI's on the fly.
- 7) MSI should setup a dedicated helpdesk to support field infrastructure laid.

9.4. Design and Implementation of Control Room

9.4.1. Control Desk



Figure 1: This is indicative diagram of Control Desk

1. General Requirements/Overview of Proposed Facility

- 1.1 The specification covers Design-Build, transportation to site, site installation and site acceptance of Control Room Consoles.
- 1.2 The desking solution shall conform to high standard of engineering as mentioned in the document; meeting the specified codes, standards and designs. It shall be capable of performing 24X7 operations under the specified environmental condition.
- 1.3 Workmanships shall be of highest standards meeting the specified requirement/purpose.
- 1.4 The supplier shall refer country specific anthropomorphic data and ergonomic standards to define the dimensions and equipment layouts, to suits the 95th percentile of country's population.

2. Overview of Control Desk

- 2.1 Requirement of the project is state of the art console system. It should be the latest and undoubtedly the best. Space age, futuristic and ahead of time is a mandatory requirement of the console system in terms of aesthetics, ergonomics and functionality.
- 2.2 The entire desk should be free from any sharp edge as per standard HSE norms.
- 2.3 Monitor arms shall be fitted on extruded heavy duty aluminum slat walls of min 5 kg / meter weight. This is to ensure no sagging takes place in the life time. The slat wall shall be of one single piece (per module).
- 2.4 Side Leg should be made of Laminated Fiber Board with premium finish. Logo of the Owner shall be beautifully integrated on the side leg. It should not be made of sticker or steel.
- 2.5 The desk shall have / ensure sufficient knee & foot space as per latest Ergonomic Norms of ISO 11064.
- 2.6 The desk can be accessed from front and back open able shutters. The cabinet of desk shall be flexible and capable of mounting generally used control room equipment's. Supplier to provide drawing for the same.

3. Scope of Work

- 3.1 The scope of the work shall be Design-Build-Install basis but shall not be limited to the following: -
 - 3.1.1 Designing, manufacturing, testing, integration etc., all complete, preparation of the related drawings, documents, etc. of the consoles shall be in the supplier's scope. The consoles shall confirm the requirements & specifications of this bid document.
- 3.2 In broad, the scope of work and supply shall consist of the following parts: -
 - 3.2.1 Design, engineering of Consoles.
 - 3.2.2 All related services for supply, installation, testing.
 - 3.2.3 Spares & Documentation
- 3.3 Detailed scope of work and supply shall include but not be limited to the following: -
 - 3.3.1 Data Collection: Gather all information related to design of the control desk
 - 3.3.2 Design Proposal: - Submission of various options of control desk layout for client's approval, strictly complying to latest ISO 11064 ergonomic norms.
 - 3.3.3 General: -

- a. The tentative control room area shall be provided to the desk manufacturer to develop the various options.
 - b. Supply of the product catalogue, technical proposals including but not limited to drawings, documentation, 3D views, color pallets, for the complete desking solution.
- 3.3.4 Spares: -A list of manufacturer's recommended spares for operation and maintenance shall be provided.
- 3.3.5 Provide commissioning & warranty spares (Contractor shall utilize these spares of all the equipment that may be required during commissioning & warranty period separately).
- 3.3.6 MSI shall be responsible for safety and security of the installed items till commissioning and final acceptance by Owner (before start of warranty period).
- 3.3.7 Quality assurance & commissioning of the complete system at site to the complete satisfaction of the Owner/Consultant

4. Mandatory Requirement (Mandatory submission by the desk Manufacture to be submitted along with the Technical Bid) :-

- 4.1 The project demands for a contemporary, visually light and ergonomically designed 24X7 desking solution. Traditional bulky box type control desk should not be quoted.
- 4.2 Submittals: -
- 4.2.1 Certificate for ISO 9001-2015 quality certification as a proof of quality system implementation in Manufacturing processes for at least 5 years.
 - 4.2.2 Certificate for ISO 14001 for Environment Management System.
 - 4.2.3 Certificate for OHSAS 18001 for Occupational Health and Safety.
 - 4.2.4 FSC: Forest Stewardship Council Certified manufacturer from a reputed certifying agency. OEM should have had FSC Certification for at-least 2 year.
 - 4.2.5 Ergonomic compliance report as per latest ergonomic norms of ISO 11064 to be submitted along with the bid.
 - 4.2.6 The consoles shall be certified for areas of Seismic zone 4 or better.
 - 4.2.7 Manufacturing Unit/Capability: If asked, supplier to arrange factory and product inspection before placement of order, to ensure that the vendor is capable of in-house production of the ordered goods.
 - 4.2.8 To prove supplier's seriousness in the business; Printed Catalogues and Locations of Demo rooms to be furnished.
- 4.3 Design Criteria: -
- 4.3.1 Table top front end should be injection molded polyurethane edge (minimum 55mm in depth) on the profiled wooden core and must not be inserted or glued. Consoles must be of modular design, facilitating future equipment retrofits and full reconfigurations without requiring any major modification to the structure.
 - 4.3.2 An edge slope and radius spreads the weight over a larger surface. Enhancing end user comfort.
 - 4.3.3 Consoles must be of modular design, facilitating future equipment retrofits and full reconfigurations without requiring any major modification to the structure or exterior elements
- 4.4 Product Specific Mandatory Requirement

- 4.4.1 ANSI BIFMA X5.5: 2014 certified console (from a reputed agency and that too on all parameters). OEM should have had BIFMA X5.5 certification for at-least 2 year. The tests must be on the following parameters.
 - a. Concentrated Functional Load Test.
 - b. Distributed Functional Load Test.
 - c. Concentrated Proof Load Test.
 - d. Distributed Proof Load Test.
 - e. Stability Under Vertical Load Test.
 - f. Tests must be based on ANSI BIFMA X5.5 -2014 standards applied to the proposed product solution.
- 4.4.2 Copy of Test certification for ASTM E84 for the surface burning characteristics of products and materials. Test must reference the actual assembled components for wood-core panels including core, laminates, edging.
- 4.4.3 Raw-material supplier data alone is not acceptable.
- 4.4.4 The entire console must be RoHS (Intertek/UL) certified, valid certificate to be submitted along with the technical documents with the bid.
- 4.5 Quality Criteria: -
 - 4.5.1 To ensure uniformity, consistency & quality in final product the desk manufacturer should have In-house Powder Coating Plant, metal manufacturing and wood processing plant.
 - 4.5.2 OEM to produce sample of Injection Molded PU Edging on profiled wooden core for technical approval.
- 4.6 Proven Track Record: -
 - 4.6.1 The desk manufacturer must produce documents proving that they have executed order(s) with 100 plus consoles/desks/operator station at single location with injection molded Polyurethane edging & scratch resistant laminate.
 - 4.6.2 The Console design offered under this project should have been supplied and working satisfactorily for a period of minimum one year on the bid issue date in control room application.
 - 4.6.3 Minimum 100 installation of control desk with reputed companies of similar reputation.
 - 4.6.4 The desk manufacturer or supplier should have supplied Minimum One desk with BIFMA X5.5 (all parameters) certifications & Seismic Zone 4 (or better) to any one Government/PSU (either customer or end user) in past five years.
 - 4.6.5 Desk manufacturer should have executed at least one order of a reputed organization where the following specifications were asked for: -
 - a. BIFMA X5.5: 2014; all parameters.
 - b. Seismically qualified console

5. Equipment Mounting

- 5.1 The control desk shall house computer equipment's, HMIs, Ethernet switches, Rack mounted equipment's, Power Distribution Unit. The CPUs shall be mounted on Slide out metallic CPU trays (mounted on Heavy duty slides) for ease in maintenance.

6. Structure

- 6.1 Horizontal and Vertical extrusions Made of heavy duty Extruded Vertical and Horizontal Aluminum profiles of HE9WP grade. The Extrusions shall be duly powder coated with 40+ micron over all surfaces.
- 6.2 All sheet metal parts must be finished with a durable, black, electrostatic powder coating with average application of 60-90 microns over all surfaces.
- 6.3 Pre-treatment process shall not generate sludge or heavy material.
- 6.4 The supplier to perform following tests during inspection: -
 - a. Adhesion test: ISO 2409:
 - b. Impact test: ASTM D 2794: 40kg
 - c. Conical mandrel test: ASTM D 522:
 - d. Scratch test: IS 101-1964:
 - e. Salt spray (FOG) test: ASTM B 117: 600 hrs
- 6.5 To allow future extension and expansion; a weld free system to be proposed. Interconnecting joints should not be visible.
- 6.6 The structure should be rigid enough to withstand BIFMA X5.5. The structure should allow easy assembly of Hinged Shutters, Slat wall, Gland Plate, Monitor arms in extremely rigid manner.
- 6.7 Grouting of the desk is not allowed for BIFMA test as well as site installation.
- 6.8 Standard office type, panel, post and open furniture will not be acceptable. Structural integrity of the Console System is a priority; therefore “cubicle” type walls shall be deemed unacceptable.

7. Work Surface: -

- 7.1 The material of the working surface should be minimum 25 mm thick MDF with High Pressure Laminate finish. The laminate shall be fire retardant, Insulated, Water Proof, Scratch resistant and high hardness.
 - a. The MDF shall confirm to ANSI A208.2
 - b. The Laminate shall be scratch resistant
 - c. The laminate shall be Green guard certified. This laminate shall have added benefit of an extra-wear surface and provide a high resistance to scuffing, and cigarette burns. The material shall also have a skid resistant surface.

8. Designer Front Edging Option

- 8.1 Front ergonomic edge shall be of injection molded Polyurethane(PU) on profiled wood core which gives cushion/comfort to wrist/palm during working hours. It should be perfectly flushed with the laminate to give a seamless finish and should not obstruct during operations. The PU shall have varying depths across the length of the console to increase the aesthetical appeal of the desk.
 - a. PU edge shall have flexibility to design at radius.
 - b. T shape of PU / PVC / PP shall not be acceptable as they can be pulled out manually.
 - c. Shape of the PU shall have an ergonomic slant with min 55 mm depth at the operator’s sitting area. This is to give a grand look and maximum comfort.
 - d. The overall thickness of the PU shall be within a range of 30-40mm.

- e. Other open edge shall be of PVC / ABS / PP with Greengard specs.
- f. Manufacturer to show in-house facility to ensure smooth service in case of any such requirement in future.

9. Shutters & Side Legs

- 9.1 Front, back shutters shall be of 18 mm Laminated MDF Board with premium finish. Side leg shall be of 25mm of the same finish. Hinges shall have life time warranty. Entire console to be RoHS certified (from UL / Intertek). The Laminated MDF shall confirm to E1 Grade, ANSI A208.2 and CARB certified and must follow EN 622-5 standard.

10. Monitor Arms/Arrays and Attachments

- 10.1 Die cast mounted Aluminum arm; fixed firmly on MS Pole.
- 10.2 These poles will have same powder coating as that of Modular Rear wall.
- 10.3 Monitor and Functional holder shall guarantee optimum viewing distance. All ergonomic aspects shall be taken in to account. It shall be capable for mounting all type of LCD display with Dimensions between 17" to 27" using suitable adopter/additional base plate for complying VESA standards 75 x 75, 100 x 100, 200 x 100 & 200x200 mm.
- 10.4 For configuration of working position, it shall allow the technical staff to rotate/ tilt/ raise/the monitors as well as fix their adjustment in a quick and easy manner.
- 10.5 The Monitor and functional holder shall bear the weight of the mounted Monitors; hold the monitors firmly without shaking. Max load for monitor shall be 10kgs for single & dual tier arrangements.
- 10.6 The monitor arm should be Articulating monitor arm.
- 10.7 Up-down moment can be performed without tools.
- 10.8 Pole Height - 455mm
- a. Extension - 400mm
 - b. Tilt - 180 Degrees
 - c. Swivel - 270 Degrees
 - d. Rotation around Monitor Pole 360
 - e. It shall be designed to enable replacement of existing LCD display with other type during monitor changes necessitated by future developments.
 - f. Articulating monitor arm, Flexible monitor arm, depending on console configuration. e. Upper-level articulating monitor arm (Double high option).

11. Modular rear walls

- 11.1 Modular rear walls shall be made of heavy duty extruded aluminum profile with better aesthetic appeal; allowing for various viewing levels and privacy. Conventional office type slat wall shall not be accepted.
- 11.2 Modular walls shall be made of approx. 2mm thick Extruded Aluminum (HE9WP aluminum alloy).
- 11.3 Shall be designed in such a way that no joints or gaps are visible in the entire width of the console.
- 11.4 Load bearing capacity shall be min 30 kg per meter.

- 11.5 It should have linear slots running throughout the length to accept modular components (slat wall mounting system, telephone arms, pen holders, paper holders).
- 11.6 It should have high Load bearing capacity.
- 11.7 No buckling when arms are fully extended
- 11.8 No screws should be visible when joining table top to the Slat wall and on the top of the slat wall. OEM to produce sample before commencing the manufacturing activities.
- 11.9 Bidder to ensure that the desk manufacturer has done minimum 20 projects with Slat wall (this is a mandatory requirement).

12. Electricals

- 12.1 Each console shall be equipped with individual power distribution unit. The Electrical power distribution unit shall be capable of being switched on/off and provide safe supply to all the consuming equipment individually. The console should be electrically earthed for all the body part which are conductive.
- 12.2 Power supply socket should be dual type i.e. Universal type.
- 12.3 Rear vertical mounting with powder coated CRCA body with RAL 9005 color having universal sockets with Inbuilt 16A single pole MCB.
- 12.4 Shall confirm to BS 546. Entire control desk to be RoHS (From UL/Intertek) certified.

13. Cable Routing Arrangement

- 13.1 Designed with vertical and horizontal cable trays to allow for continuous cable management between the cabinets. The design of console shall allow cable run, from the floor hollow channel.

14. Cooling

- 14.1 Rear shutters of each console should have provision of Airflow opening for cooling and heat dissipation effect.
 - a. Rear panel/door-mounted ventilation fans (optional).
 - i. Ventilation fans shall have the following properties:
 - 1. Fans must be available for mounting on the doors. The individual situation may dictate a change in the ventilation requirements.
 - 2. Axial fans should be aerodynamically shaped with metal construction and metal blades for longer life
 - 3. Can operate in -10deg to +55 deg
 - 4. Noise level should be below 50dB
 - 5. Air flow should be approx. 105 CFM
 - b. Screws shall not be visible on the front metal plate where the fan shall be mounted.

15. Illumination

- 15.1 Service light should be provided inside the cabinet enclosure for maintenance of equipment with provision of manual on/off switch.
- 15.2 The illumination of service lights shall be such as not to interfere with the vision of the operator sitting in front of the console.
- 15.3 LED shall be of 14 Watt, with 30,000 hours life.

15.4 Connections on the door switch must be covered to avoid accidental contact with live wires.

16. Hardware

16.1 All bolts must be of SS material to avoid rust due to environment. Remaining hardware shall be Nickel Plated with RoHS certificate.

17. Sustainability Requirements

17.1 Total recyclable content shall be greater than 50%.

17.2 All metal components shall be 100% recyclable.

17.3 All materials shall be free of hexavalent chrome, CFC's, and PDBE's.

17.4 Adhesives used shall be solvent free and free of any hazardous air pollutants.

17.5 Metal parts shall be powder coated and finished with a durable VOC-free finish which is applied in a process that generates low levels of recyclable waste.

18. Logistics

18.1 As per negotiation during ordering stage.

19. Warranty

19.1 05 years against manufacturing defects.

19.2 05 years on structure stability.

19.3 02 Years on all moving parts.

20. Quality Assurance of Consoles

20.1 Quality Assurance Plan to be submitted during designing stage and All raw material should be from verified supplier.

21. Certificate for Maintenance Support

21.1 Supplier to generate the same with BID document.

- a. Supplier to maintain the components for 5 years to support expansion and similarity.

22. Self-Declaration format

22.1 Vendor to declare; whatever has been complied will be there in the end-product. If anything is faulty then the consoles are liable for rejection and shall be replaced on FOC.

23. Checklist for Certificates, Norms etc. (To be submitted along with technical Bid)

23.1 Certification of BIFMA X5.5:2014 (on all test parameters) by a Reputed test facility.

23.2 Certificate for ISO 9001:2015

23.3 Certificate for ISO 14001

23.4 Certificate for OHSAS18001

23.5 The consoles shall be qualified for areas of Seismic zone 4 or better. Bidder to provide Seismic Test Report from government approved research institute along with the bid.

23.6 Entire console should be RoHS (UL/Intertek) certified

24. Testing Methods (As per Standard Norms)

24.1 To be shown during Inspection or BID time as per the Project Owner / client requirement.

- a. Drop Test
- b. Abrasion Test
- c. Conical Mandrel
- d. Powder Hardness test
- e. Load Bearing Capacity of Desk

25. In House Quality Lab

25.1 Supplier to demonstrate in-house test lab to prove quality consciousness / seriousness.

26. Accessories

26.1 Supplier to demonstrate the following attachments in BID, to quote unit price of each if not asked 3 sets of printed catalogues to be submitted for attachments.

- a. Articulating monitor Arm,
- b. Telephone arm,
- c. Key board tray,
- d. Task Light,
- e. Service light,
- f. File storage,
- g. Monitor arm,
- h. File holder,
- i. Pen holder,
- j. Telephone holder

27. Packing

27.1 Wooden crate packing. Time being the crux of the project, supplier to ensure quality packing is done to avoid any damages and consecutive delays.

28. Dispatch Instructions

28.1 The material to be dispatched to site in Semi Knock down condition for quick installation at site.

29. Vendor Selection Criteria

29.1 Vendor to give point by point compliance on all points mentioned in the specification document.

9.4.2. CONTROL ROOM

1. Scope of Work

The scope of the project includes designing; engineering, supply & installation of 24X7 mission critical Control Center Interiors. As the Control room is a significant place, it is imperative that it is designed properly in terms of Aesthetics, Ergonomics and Functionality. Various aspects should be considered while designing Control Room area to create ideal

work place, considering physiological aspects such as line of sight and field of vision and cognitive factors such as concentration and perceptivity as per ISO 11064.

The design of systems, equipment and facilities shall reflect human factors requirements including the following:

- 1.1 Satisfactory environmental conditions for operator personnel. Including noise, air flow, temperature and humidity, and precautionary measure under uncontrolled conditions (like fire) beyond acceptable limits.
- 1.2 Adequate space for personnel and equipment for the movements and activities they are required to perform during operation and maintenance, under both normal and emergency conditions.
- 1.3 Adequate visual / auditory status information and other communication links between personnel and equipment under normal and emergency conditions.
- 1.4 Adequate illumination for the performance of operation, control, maintenance and training.
- 1.5 The control room shall be built as per the criteria of “Human Factor Engineering” to improvise the efficiency utilization of the operators and provide them Fatigue free working environment.
- 1.6 Objective: -
 - a. Ensure maximum standard of safety.
 - b. Allow Flexibility
 - c. Minimize maintenance
 - d. Improve operator’s efficiency & alertness.
- 1.7 Designing, manufacturing, testing, integration etc., all complete, preparation of the related drawings, documents, etc. of the CONTROL room shall be in the supplier's scope. The CONTROLS design shall confirm the requirements & specifications of this bid document.
- 1.8 In broad, the scope of work and supply shall consist of the following parts: -
 - a. Interior Design, engineering of CONTROLS.
 - b. All related services for supply, installation, testing.
 - c. Spares & Documentation
- 1.9 Detailed scope of work and supply shall include but not be limited to the following: -
 - a. Data Collection: Gather all information related to design of the CONTROL rooms.
 - b. Design Proposal: - Submission of ISO 11064 ergonomic compliance report of console in reference to the control room layout.
- 1.10 General: -
 - a. Supply of the product catalogue, technical proposals including but not limited to drawings, documentation, 3D views, color pallets, for the complete solution.
 - b. Spares: -A list of manufacturer’s recommended spares for operation and maintenance shall be provided.
 - c. Provide commissioning & warranty spares (Contractor shall utilize these spares of all the equipment that may be required during commissioning & warranty period separately).

- d. Manufacturer shall be responsible for safety and security of the installed items till commissioning and final acceptance by Owner (before start of warranty period).
- e. Quality assurance & commissioning of the complete system at site to the complete satisfaction of the Owner/Consultant.

2. Acoustic Requirements of Control room

- 2.1 Control room being dead zone in acoustical terms, threshold should be lower than the normal.
- 2.2 Use of Acoustics and psychoacoustics measurements are must. Vendor to highlight the same in drawings.
- 2.3 Materials which define acoustics; it's the detailing which ensures controlled reverberations & resonances and reflections.
- 2.4 Selection of fire retardant/rated material is must.

3. Mandatory Requirement:

The project demands for a contemporary, aesthetically appealing, ergonomically designed, safe and 24X7 working facility. Conventional wooden cladding, painting, gypsum, 2'X2' Metal, POP ceilings (for Control area) shall not be accepted.

This facility being the first of its kind, scale & prestige it is mandatory for the bidder to provide Designer Control Room interiors without compromising on the safety and functionality of the facility. Materials having the adverse impact on the environment and nature shall not be accepted. 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 an experience of minimum 10 turnkey control room project's supply and installation of Control Rooms or War rooms, including but not limited to Control desk, Illumination, Floorings, Custom designer metal ceilings, wall claddings and doors, completion/appreciation letters to be submitted by the OEM along with the bid. Conventional office designers shall not be accepted.

- 3.1 Submittals : - (OEM must submit the documents along with technical Bid for project level approval)
 - a. Certificate for ISO 9001-2015 quality certification. 9001 certificates to be submitted as a proof of quality system implementation in manufacturing processes.
 - b. Certificate for ISO 14001 for Environment Management System.
 - c. Certificate for OHSAS 18001 for Occupational Health and Safety.
 - d. Ergonomic compliance report for control room layout as per ISO 11064
 - e. Manufacturing Unit/Capability: If asked, supplier to arrange factory and product inspection before placement of order, to ensure that the vendor is capable of in-house production of the ordered goods.
 - f. To prove supplier's seriousness in the business; Printed Catalogues and Locations of Demo rooms to be furnished.

- g. The control room interiors must be Greengard Certified (from UL). Valid test certificate to be submitted along with technical Bid.

3.2 Warranty:

- a. Five year's warranty against any manufacturing defect on Control Room design including but not limited to Illumination, Floorings, Custom designer metal ceilings, wall claddings and doors.

3.3 Proven Track Record:

- a. The bidder to produce following documents from the control room interior Manufacturer or supplier: -
- b. Minimum 10 installation of control rooms/ NOC areas with completion/appreciation letters for the turnkey scope including but not limited to ceiling, flooring, illumination and wall cladding from reputed companies to be submitted along with the bid. These packages should have been executed on or before Bid release date.

3.4 Design Criteria: -

- a. The ceiling, paneling and partition must be of modular design, facilitating future equipment retrofits and full reconfigurations without requiring any major modification to the structure.

3.5 Product Specific Mandatory Requirement

- a. Copy of Test certification for ASTM E84 (from UL) for the surface burning characteristics of wall paneling tiles and ceiling tiles to be submitted along with the technical Bid. This is mandatory requirement from Fire safety point of view.
- b. Raw-material supplier data alone is not acceptable.

3.6 Quality Criteria: -

- a. To ensure uniformity, consistency & quality in final product the control room & Control desk manufacturer should have In-house Powder Coating Plant, metal manufacturing and wood processing plant.
- b. Forest Stewardship Council: The OEM should be a FSC Certified manufacturer from a reputed certifying agency. OEM should have had FSC Certification for at-least 2 year. Certificate need to be submitted along with the technical Bid.

4. PANELING

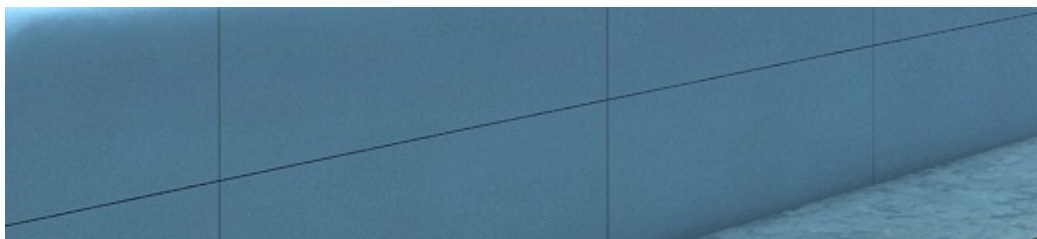


Figure 2: This is indicative representation

4.1 Design & Material Specification for Paneling

- a. Factory made removable type self inter lockable metal panels of Preformed textured Hot dip galvanized strips and sheets of low carbon steel coated on one side with rigid polyvinylchloride (PVC) film and on the other side a coating based on cross linkable polyester resins (sheet thickness 0.6mm & PVC Coating 0.15mm). Make shall comprise of specially designed combination of perforated and non-perforated panels through CNC laser Cutting, bending & punching. Panel shall be of 0.75mm thick galvanized metal of approved color. Panels shall be designed to achieve shape and design as per the design consultant. Panels shall be fixed using hook fitting on structure. Overall system thickness for paneling shall be 70mm to 85mm and for partition shall be 85mm to 110mm.
- b. As per design panel shall comprise of hexagonal perforation for making paneling and partitions acoustically sound. Acoustic grade fire retardant fabric (min 1.5mm thick) will be fixed at some parts of the control room. Wall paneling system must be RoHS certified from UL/Intertek. Valid certificate to be submitted along with the technical Bid.
- c. Panel shall be design in such a manner that it takes care of undulation of civil walls and gives perfect flat surface finish and compile easy service & maintenance procedure.
- d. Sound transmission class (STC) value of 35 for Wall Paneling & Partition. (According to IS: 9901 (Part III) – 1981, DIN 52210 Part IV- 1984, ISO:140(Part III) -1995, test report from reputed agency to be submitted along with the technical Bid.
- e. Wall Paneling & partition should be Seismic Zone 4 or better Tested, relevant certificate to be submitted along with the technical Bid.
- f. Control Room Interior must be Greengard certified.

4.2 Design:

- a. The cladding panels shall be made up of combination of two sheets locked and riveted together and polystyrene shall be used as infill to achieve strength and acoustics. The front tile (PVC pre-coated metal sheet) shall be perorated/ non-perforated as per the design requirement and the back tile (Powder coated 0.6mm GI sheet) shall be designed in such a manner that it fits on the back portion of the front tile. Once the tiles are fitted together then these will be manually riveted. These tiles shall be bend through CNC, machine punched & laser Cut to achieve perfect accuracy.
- b. Structure Shall be made from heavy duty powder coated modular steel frame (minimum sheet thickness 1 to 1.6mm) and shall allow uninterrupted flow of wires/cable/tubes of max. dia. 25mm.
- c. Structure Shall be securely grouted from wall, roof and floor. It shall be made up of 1-1.6mm thick vertical Slotted rolled C sections (Upright) and horizontal rolled 'C' connectors. Grid of desired dimension shall be formed by Vertical and horizontal sections having 50mm pitch.

4.3 Surface Finish:

a. For Panels:

- i. Front Panel: PVC pre-coated GI sheet (sheet thickness: 0.6mm and PVC coating: 0.15mm)
- ii. Back Cover: Powder coated GI sheet. (sheet thickness: 0.6mm with powder coating:)

b. For Structure:**i. Powder coated sheet. (sheet thickness: 1.0mm to 1.6mm with powder coating)**

The metal sheet shall have possibility of being formed mechanically per the specific needs of the project. It shall be able to undergo stretching up to 100% and therefore follow (adhere to) bend with the steel in all its deformation. The sheets shall have specific fire retardant additives as an important barrier to slow down the combustion processes. It shall have electrical insulation property and shall be sustainable and easy to maintain.

Panel shall provide better thermal, electrical insulation as compared to normal GI panels. It shall be non-reflective/glare free and be eligible for food contact.

4.4 Material Selection:

- a. Available Width- 300mm to 1200mm (in multiples of 150mm).
- b. Available Height- 150mm to 750mm (in multiples of 150mm).
- c. Thickness- 10mm to 15mm for perforated tiles with acoustic fleece without back cover
- d. 25mm to 30mm for non-perforated tiles with back covers

4.5 Material Testing/Certification (all certificates to be submitted along with technical Bid):**a. PVC pre-coated sheet:**

- i. Fire rating and Low flame spread: EN ISO 11925-2, EN 13823 and ASTM E-84
- ii. Food grade: EU10/2011

b. Core material (compressed polystyrene):

- i. Acoustic test: 9301/ ISO: 140/ASTM 413, ASTM C 578.

c. Powder coating

- i. Adhesion test: EN ISO 2409 (2 mm)
- ii. Impact resistance test: ASTM D 2794 (5/9' ball)
- iii. Flexibility test: EN ISO 1519
- iv. Salt spray test: 600 hrs.
- v. Resistance to humid atmosphere test: DIN 50017.

4.6 Component Specification:**a. Floor Mounting: -**

- i. 3mm thick C channels are welded together to form a 'I' section having minimum height of 150mm. This I section shall be welded on 3mm thick MS grouting plate.
- ii. This assembly shall be grouted on the floor with the help of M10 Anchor Fasteners.
- iii. These Floor Mountings shall be the base support to the vertical uprights spaced at a center to center distance of 1200mm maximum.
- iv. Contractor must ensure proper marking and leveling before proceeding with any floor grouting.

b. C Section (Upright) fixing: -

- i. 56 mm wide Slotted rolled C section (UPRIGHT) (1 to 1.6 mm thick CRCA). Maximum single piece Length shall not exceed 2700mm.
- ii. All sections will be dual slotted with 50 mm pitch.
- iii. These Uprights shall be mounted over the floor mountings and shall be connected by C connectors made up of 1.0mm to 1.6mm thick cold rolled 'C' sections.
- iv. The installation to be carried out with Uprights spaced at 1200 mm (centre to centre) securely fixed to the floor slab by means floor mountings.
- v. The uprights shall be firmly held with L shaped wall mounts made up of 2 mm thick MS sheet duly powder coated. One portion of L mount shall be grouted with wall and other will be having a minimum slot length of 75mm.
- vi. The L clamp and the upright will be bolted together with M6 bolts.

c. End Cap

- i. 0.6mm to 0.75mm thick C shaped tile; like the panel tile will be bolted on the extreme end Uprights so as to hide the grid structure.

d. Panel:

- i. The panels shall be hooked on the uprights.
- ii. Panels shall have integrated hooks (which shall cut and bend on high precision laser machines).
- iii. The panels shall have minimum gap of 5mm between two tiles (on vertical and horizontal edges) so that the tiles can be replaced and installed easily.
- iv. The hooks of the Panels shall have a length of 20mm (for the upper hook) and 10 mm (for the bottom hook). So that these panels are firmly held on the uprights.
- v. The panel shall have HOOK in arrangement (With gravity lock).

e. Corner Cap:

- i. On extremes ends of control room the wall connector (L- profile) shall be fixed on the perimeter walls. This L-section shall be snap fitted and then bolted to the walls.

f. Door Profile:

- i. Door frame shall be fixed with these profile only so as to have proper integration of doors with the overall system.

g. Feature:

- i. Raw material for tile & powder coating should not affect environment, vendor to provide necessary test certificate.
- ii. Color should not fade over 10 years.
- iii. No sagging
- iv. Easy and quick installation
- v. Low cleaning effort
- vi. Vendor to demonstrate one portion at wall paneling & ceiling at their premises before dismantling & shipping to site. In short a FAT (Factory acceptance test) to be carried out at vendors works for ceiling & paneling.

- vii. 100 % modular design. At site, no cutting, chipping work is allowed.
- viii. The tile shall be bend resistant

5. Glass Partition

- 5.1 Full glass wall partitions will be made of 12mm Toughened laminated glass with frameless structure. The glass partition shall be supported by 600mm high Modular metal partition (having the same finish as that of wall cladding) from the floor. Proper structure shall be made to ensure the fixing of glass from RCC slab above false ceiling and flooring.
- 5.2 No straight and vertical structural members shall be visible. Safety film shall be applied on the glass to avoid shattering. Glass shall be fitted on anodized extrusion with tool less technology and having a provision for replacing glass with perforated sheet/acoustic tile by removing the glass.
- 5.3 NOTE: - The nature of installation should be replaceable, expandable and flexible to cater the future expansion/technical up-gradation.
- 5.4 Designer privacy film for glass Partition/glass Door

6. Curve Glass Partition

- 6.1 Including full glass partitions of minimum 12 mm thick clear toughened glass, structural support system for top and bottom including holding system from RCC slab above false ceiling, including runner hung anchor fastener to fix it. Rubber interlinear & gaskets to fix bottom into SS "U" channel in floor. silicon sealant to filled gap.

7. DOORS

7.1 Metallic Door

- a. With door spring and locking arrangements and both way handle. Prepare with rigid thermo fused film metal panels. Specification: 0.6mm thick Metal panel sheets, cavity filled with glass wool insulation of density 24kg/cum in roll form of make inside adequate quantity. Material of the partition and that of metal door will remain the same.

7.2 Metal door with Toughened Glass Vision Panel: -

- a. The door shall have 100mm frame (made of same material as that of wall Paneling /partition) and shall have 12mm thick glass pane in between.
 - i. 12mm thick tempered clear glass door with door spring and locking arrangements and both way handle and patch fittings.
 - ii. Glass Properties: Safety (tempered): when broken, must split into tiny harmless pieces.

8. Ceiling

8.1 Designer Composite Ceiling System:

a. Powder Coated Baffle False ceiling

- i. The baffles shall be made up of powder coated GI/MS/Aluminum sheet. These baffle Planks shall be processed on laser Machine have dimensions to suit control room illumination requirement as per architect's approval.
- ii. Center to Center distance between baffle shall be minimum 150 mm.
- iii. Specifications (Finish and component details):
 - a) CEILING Baffle tile: minimum 0.7 mm thick powder coated sheet/1mm Aluminium sheet.
 - b) Carrier made of 0.50 mm GI, powder coated to matching baffle colour or black as directed by the architect. Ceiling to have arrangement to fix, hang and lock the baffles of required sizes and at required intervals. the size of punched carrier would be 35x20x35mm bent channel with holes for suspension and fixing secondary channel or as per engineer in charge approval.
 - c) The baffles top edge will have a flange of 5mm to fix in the carrier profile.
 - d) Mother C Channel: 1.6 mm Thick GI Sheet with Laser cut profiles.
 - e) Suspension: The carriers would be placed at every 1200mm (maximum) and suspended by means of a secondary angle, channel fixed to the carrier at every 900 to 1200 mm and this secondary member in turn would be suspended by means of a 3 mm wire and level adjustment butterfly clip fixed to the slab by means of a 6 mm diam., dash fastener.
 - f) Top Clamp: 1.0 mm Thick GI Sheet for holding the threaded rod.
 - g) Tile Top clamp: minimum 1.0 mm thick GI Sheet snap fit clamp.
 - h) End Cap: minimum 0.7 mm thick GI end cap
 - i) Finish: Epoxy Powder coated.
 - j) Color: As per approval
 - k) Entire structure will be in powder coated MS.
 - l) Metal Strip where baffle planks will be hanged should be sleek & sturdy.

b. Designer Metal False ceiling with integrated illumination channel:

- i. Panel shall be of 0.6mm galvanized metal of approved powder coating finish. Panels shall be designed to achieve shape and design as per the design consultant with the combination of acrylic panels with lights, designed to enhance visual feel, with provision for easy installation and maintenance, integrated lighting.
- ii. Structure Shall be made from heavy duty powder coated modular steel frame (minimum sheet thickness 0.8 to 1.6mm). It Shall be securely grouted from roof with help of anchor fastener and GI self-threaded rods. It shall be formed with the help of slotted rolled W

- sections (stiffener) and M section (Master) with help of M6 cage nut and bolts.
- iii. The master section shall have laser cut profile to enable fixing of Baffles & diffused continuous LED section with acrylic sheet.
 - iv. Panels are then snap fitted individually on the grid frame work. The panels are also hold by safety wire to ensure that these tiles do not full during seismic vibrations.
 - v. The System must be RoHS Certified (From UL/Intertek) & Greenguard Compliant. Certificate need to be submitted along with the technical Bid.
- vi. Dimensional Details:**
- i. Baffles Tile: - Machine profiled GI sheet of Aluminum sheet available in various length.
 - ii. Type- Clip on with double locking arrangements. (Key requirement). Should be easily openable to access above ceiling services.
- vii. Material Testing/Certification:**
- i. Powder coating: Must qualify 600 hours' salt spray test.
- viii. Component Specification:**
- i. Master M Section:
 - a) 1.2 mm thick GI section length 1200mm. the installation to be carried out with runner's spaces at 1200/1500/2100 mm center to center securely fixed to the hanging "c" section by means at M6Nut and bolts.
 - b) The end section shall be covered by 0.8mm thick powder coated MS sheet.
 - ii. Hanging W Section:
 - a) Specially machine profiled W section 65x15x0.8mm.the section should be 2400 mm long & shall run across the length at the room.
 - b) Centre to center distance between W section shall be 1000mm.
 - c) These sections are securely fixed to the slab by means of Metal fastener and 8mm GI rod fully threaded (with hex nut for precision level adjustment.)
 - d) The two-master section shall be attached to each other by means at fixing pate 45x34mm & M6 cage nut & bolts.
- c. **The ceiling** shall be supplied with demountable translucent stretch ceiling membrane with harpoon, corners ready to install. Membrane shall transmit 76.60% light and absorb 23.40% of light. CE Certified & fire rated to European standards B-S2-d0 with 10 years warranty on membrane seam ruptures, discoloration, sag and profile. All joints shall

be provided with appropriate interface trims to be able to demount the ceiling to access the lights.

The ceiling must be installed using ceiling aluminium suspension system, complete as per manufacturer's installation guidelines and as per approved shop drawings in line with the design intent and approval by Architect.

The LED Modules shall be supplied with 5 year warranty, appropriate drivers and dimming system. LED strips shall be installed using custom aluminium extrusions to ensure longevity of the installation. The Flexible membrane must be ASTM E 84 class A certified, necessary test report to be enclosed with the bid before commencement of Job.

The ceiling shall have following features and properties:-

- i. Simple and maintenance friendly: Installed in a few hours and finished product shall not require any taping, spackling, or painting, and shall be easily cleanable.
- ii. Durable: The systems shall resist shocks and shall not crack with movement or under stretch conditions.
- iii. Safe: The membranes and profiles shall have passed the stringent fire and safety tests. The membrane must have been classified as non-toxic upon burning.
- iv. Green: Membranes must be 100% recyclable.
- v. Warranty: Membranes shall come with a 10-year warranty against any welding defects in the perimeter edging or in the factory seams.

8.2 Designer Acoustic Metal False ceiling with Planks

- a. Factory made acoustic modular metal false ceiling of powder coated panels. Make shall comprising of perforated and non-perforated metal panels made through CNC laser Cutting, bending & punching. Panel shall be of 0.6mm galvanized metal of approved powder coating finish. Panels shall be designed to achieve shape and design as per the design consultant with the combination of acrylic panels with lights, designed to enhance visual feel, with provision for easy installation and maintenance, integrated lighting and scope for integration of building services like HVAC and fire detection/ fighting system. Metal modular false ceiling must have Sound absorption coefficient (NRC) value 0.30 according to IS:8225-1987, ISO: 354-1985 and ASTM 423-90. These certificates must be submitted along with the technical bid.
- b. As per design panel shall comprise of micro perforation for making false ceiling acoustically sound. The non-perforated ceiling tile shall be Class A fire rated as per ASTM E-84. Test certifications to be submitted along with the technical bid.
- c. Structure Shall be made from heavy duty powder coated modular steel frame (minimum sheet thickness 1 to 1.6mm). It Shall be securely grouted from roof with help of anchor fastener and GI self-threaded rods. It shall be formed with the help of slotted rolled W sections (stiffener) and M section (Master) with help of M6 cage nut and bolts.
- d. The powder coating metal sheet shall have possibility of being formed mechanically per the specific needs of the project. The powder coating shall be able to undergo stretching up to 100% and therefor follow (adhere to) bend with the steel in all its deformation.

- e. The master section shall have laser cut profile to enable fixing of perforated, Non-Perforated & diffused continuous LED section with acrylic sheet.
- f. The ceiling system should have double safety system to take care of seismic vibrations. Seismic joint clip on main W & cross runner will be made up of section having sizes 100 mm by 20mm.
- g. The ceiling planks shall have locking redundancy to enhance seismic impact resistance.
- h. Panels are then snap fitted individually on the grid frame work. The panels are also hold by safety wire to ensure that these tiles do not full during seismic vibrations.
- i. The Ceiling must be RoHS certified (from UL/Intertek) to ensure restriction of hazardous substance in any of the materials. (Certificate to be submitted along with the technical Bid)
- j. The Ceiling must be Seismically Certified (from UL/Intertek). Certificate to be submitted along with the technical Bid)

k. Dimensional Details:

- i. Non- Perforated Tile: - Machine profiled GI sheet of 290mm (Wide)available in various length of 600mm to 1800mm in multiple of 300mm
- ii. Perforated Tile: - Machine profiled GI sheet with fleece of 146mm (Wide) in various length of 600mm to 1800mm in multiple of 300mm.
- iii. Type- Clip on with double locking arrangements. (Key requirement). Should be easily openable to access above ceiling services. Special connection joineries to take care of seismic vibration.

l. Material Testing/Certification:

- i. Powder coating: Must qualify 600 hours' salt spray test.

m. Component Specification:

- i. Master M Section:
 - m) 1.2 mm thick GI section length 1200mm. the installation to be carried out with runner's spaces at 1200/1500/2100 mm centre to centre securely fixed to the hanging "c" section by means at M6Nut and bolts.
 - n) The end section shall be covered by 0.8mm thick powder coated MS sheet.
 - o) The master section shall have laser cut profile to enable clip on tiles viz. perforated, Non- Perforated & diffused continuous LED section with acrylic sheet.
- ii. Hanging W Section:
 - a) Specially machine profiled W section 65x15x0.8mm.the section should be 2400 mm long & shall run across the length at the room.
 - b) Centre to center distance between W section shall be 1000mm.
 - c) These sections are securely fixed to the slab by means of Metal fastener and 8mm GI rod fully threaded (with hex nut for precision level adjustment.)
 - d) The two-master section shall be attached to each other by means at fixing pate 45x34mm & M6 cage nut & bolts.
- iii. U Section:
 - a) Machine profiled 'U' Section 150x77x0.6mm section to accurate continues running light.

- b) It shall have provision for fixing acrylic sheet.
- c) This whole assembly shall be hang from roof slab with help of anchor fastener and full threaded GI rod.
- iv. Ceiling Plank:
 - a) It shall have Laser cut holes/cut-outs for light fixing as per defined lux requirement and approved layout.
 - b) Non-perforated tile slots to be punched to accommodate AC grills.

8.3 Grid Type 700mm X 620mm Snap fit Ceiling

- a. Factory made acoustic modular metal false ceiling of powder coated panels. Make shall comprising of perforated and non-perforated metal panels (700X620mm) made through CNC laser Cutting, bending & punching. Panel shall be of 0.6mm galvanized metal of approved color. Panels shall be designed to enhance visual feel, with provision for easy installation and maintenance, integrated lighting and scope for integration of building services like HVAC and fire detection/ fighting system.
- b. As per design panel shall comprise of micro perforation for making false ceiling acoustically sound with fire rated acoustic fleece.
 - i. **Ceiling Plank:**
 - 1. Plank shall be made from 0.6mm thick GI powder coated sheet of approved shade and sizes.
 - 2. Light fitting can be defined as per the LUX requirement.
 - 3. It shall have Laser cut circular hole for light fixing as per defined lux requirement and approved layout.
 - 4. Non-perforated tile slots to be punched to accommodate AC grills.
 - ii. **Properties:-**
 - 1. High NRC (Noise Reduction Co-efficient)
 - 2. Better Light reflectance & Fire performance.
 - 3. Humidity Resistance.

8.4 Calcium Silicate Board:

- a. Plain Calcium Silicate Acoustic Boards for false ceiling with 08mm Approx. thick, Structure for underside of suspended grid formed of GI perimeter channels. Wood screws and metal expansion raw plugs for fixing with wall. Plastic emulsion paint of approved make and shade for finishing surface of Calcium Silicate Boards.
- b. General Specification of Calcium Silicate Board: this board is manufactured from a mixture of Portland cement, fine silica, special cellulose fibres and selected fillers to impart durability, toughness, fire and moisture resistance.
- c. Expansion after expose to the water for 24 Hr.: 0.12%, Noise Resistance: B38, Water absorption by Weight: 34%, Fire resistance: BS 476 incombustible A1 Class.

9. Lighting and Illumination of Control Room.

9.1 LED lights

- i. Brief:- The lights shall be available in flat panels. These shall be designed and developed with slim shape for stylish look. The product shall have better colour rendering index for interior illumination.
- ii. In LED shall have three basic choice of colours like cool white, warm white and neutral white. The LED lights shall have uniform light distribution without any spots on surface of panel, to make it highly luminous.
- iii. **Features: -**

a. Round LED Lights

- i. Temperature- 3000 K to 6500K
- ii. CRI >70
- iii. Power Consumption 12W to 24W
- iv. Aesthetically designed enclosures
- v. Highly efficient constant current LED drivers
- vi. Ideal replacement for traditional PAR/CFL lamp
- vii. Up to 80% energy saving.
- viii. LED's life >25,000 hrs @ L70

b. LED based Square Light

- i. Light source: LED
- ii. Lumen output: 2800 – 3500
- iii. Light color: 3000K - 6500K
- iv. Power consumption: 29 to 38 W
- v. Voltage: 220-240V AC 50Hz
- vi. Color: White
- vii. Lifetime: 35000 burning hrs. (At L70)

c. LED based Strip Light

- i. Light source: LED
- ii. Lumen output: 840 lm/Mtr.
- iii. Light color: 3000K/6000K
- iv. Power consumption: 9.8 W/Mtr.
- v. Voltage: 12V AC 50Hz
- vi. Optics: Sand-blasted matt finish reflector
- vii. Color: White
- viii. Lifetime: 40000 burning hrs. (At L70)

d. MASTER LED tube

It integrates a LED light source into a traditional fluorescent form factor. Its unique design creates a perfectly uniform visual appearance which cannot be distinguished from traditional fluorescent. For those

that are looking for value for money within limited budget and re-lamping efforts for better light effect and lifetime.

9.2 Wiring for Ceiling Light

a. Wiring for Ceiling Light:

- i. Wiring for ceiling lights: For ceiling wiring inter looping will be done and switches will be provided.
- ii. The system of wiring shall consist of PVC insulated copper conductor stranded flexible FRLS wires of 1100 volts grade of insulation, in metallic conduits for all exposed wiring and PVC/ metallic conduits for all concealed wiring. Minimum size of copper conductor shall be 1.5 sq. mm for lighting and 2.5 sqmm for power. Color code shall be maintained for the entire wiring installation that is Red/Yellow/Blue (or as per Local Standards) for the all single phases, Black for neutral and Green for earthing.
- iii. Appropriate ferrule will be used in both the side (LDB Side & Switch's Side)
- iv. Note – Each Light Fixture will have 3 Wires: Phase, Neutral & Earth individually & If there is a need of another wire for Dimming/Dynamic Lighting Purpose then it will add on.

9.3 SWITCHES & SOCKETS

- a. Compliance to stringent quality norms, Dual shutter mechanism for easy & better fitment Wide & flat switch knob for easy operation. FR grade polycarbonate with high impact resistance, shock proof & UV rays stabilized.

9.4 MCBs

- a. For the control and protection of low voltage installations against overload and short circuits.
- b. Ripping characteristic: C Curve – 5 to 10 x In
- c. Rated at 25°C to -50°C
- d. Isolation function
- e. Double entry points, separate bus bar entry, open mouthed terminal and lift clamps.

10. Plastic emulsion paint :-

The surface shall be free from dust, dirt, grease and other foreign matter and shall be smooth by sand papering. The primer coat shall be alkali resistant primer or emulsion primer and shall be same manufacture as plastic paint.

11. Wall Putty :-

Material for 1mm thick Putty on all exposed portions of beams, columns and walls as directed by the consultants including mixing, scraping, and levelling the surface, cleaning and complete in all respects to receive the paints & finishes.

12. FLOORING

12.1 Acoustic Laminate Flooring: -

Acoustic flooring (shall reduce impact sound by 14dB (ISO 717-2)). It shall be twinlayer linoleum built up from 2 mm acoustic laminate and a 2 mm Corkment backing. Flooring shall be decorative type of approved shade, pattern, texture and design and of approved manufacturer. Dimensions shall be as per the final approved design and site requirement. Flooring shall be laid over concrete floor with laying compound strictly as per manufacturer's specification.

For Fixing details please refer the procedure mentioned below.

- a. Areas to receive material should be clean, fully enclosed and weather tight with the permanent HVAC in operation. A minimum temperature 68° F maintained during the installation, and for at least seven days following the installation.
- b. Installation should not begin until the work of all other trades has been completed, especially overhead trades.
- c. Areas to receive material shall be adequately lighted to allow for proper inspection of the substrate, installation, seaming and for final inspection.
- d. Concrete substrates shall be structurally sound, rigid, smooth, flat, clean, and permanently dry. The concrete surface must be free of all foreign materials including, but not limited to, dust, paint, grease, oils, and solvents, curing and hardening compounds, sealers, asphalt and old adhesive residue.
- e. Concrete substrates shall have a minimum compressive strength of 3,000 psi and a dry density of at least 150 pounds per cubic foot.
- f. Concrete substrates on or below grade are required to have an effective moisture vapor retarder installed directly below the slab. The vapor retarder shall be puncture and tear resistant with a minimum thickness of 0.010" and a presence of 0.1 y. (Refer to ASTM E 1745.).
- g. Imperfections such as chips, spills, cracks, and joints must be repaired using suitable patching and leveling materials. Always follow the manufacturer's recommendations for the use and application of these products. Refer to the Substrate Preparation section of this guide for additional information.
- h. Use material from the same batch/dye lot.
- i. Install rolls in sequence by roll number and cuts from each individual roll in consecutive order.
- j. Do Not Reverse sheets for seaming.

- k. Install one sheet at a time, making sure to place the material into wet adhesive.
- l. Remove fresh adhesive residue immediately with a clean white damp cloth. Dried adhesive can be removed with a clean white cloth and mineral spirits.
- m. Linoleum will expand slightly in the width and shrink slightly in the length when placed into the adhesive. Proper installation procedures will compensate for this characteristic.
- n. Measure the area to be installed and determine the direction in which the material will be installed and. seam placement. Seams must be a minimum of 6" away from underlayment and concrete joints, saw cuts, etc.
- o. Cut the required length for the first sheet off the roll, adding approximately 3" - 6" for extra trimming.
- p. The factory edge must be trimmed to produce a clean edge suitable for seaming.

12.2 False Flooring

- a. Raised height above the RCC floor – 150 to 300mm (as per Customer's approval).
- b. Mandatory: Top Surface Shall be Green Guard (UL) certified to avoid VOC free / low emitting surface and finish shall be similar to the Acoustic Laminate flooring.
- c. The flooring should be manufactured with all steel welded construction with an enclosed bottom pan and top surface should be finished with durable & environment friendly acoustic laminate pasted with special glue serving life of 5 years minimum. Tile Size should be 600mm X 600mm.
- d. The system should have: -
 - i. Bear Concentrated Loads: 360 Kgs
 - ii. DIN 4102 class A1 for Heat Resistance &
 - iii. BS 476 for fire resistance.
- e. The acoustic laminate should be made up of twin-layer linoleum built up from 2 mm Laminate.
- f. The laminate should be made up of natural products and should not emit any volatile organic compounds, should be Sustainable & 100% biodegradable. Also it should be Impact, chemical & fire resistant with anti-bacterial & anti-static properties with Colors & patterns permeate through the surface to reduce noticeable wear.
- g. This false floor panel should rest on Edge support rigid grid system having Galvanized Iron base plate dimensions as 100mm X 100mm. The stringer should be fixed on pedestal having height adjustment of ± 25 mm.

12.3 Vitrified Flooring:-

Fully vitrified, 10 mm thick non-porous, homogenous, abrasion resistant, minimum size 600 mm x 600 mm x 10mm of approved color and shall be laid over concrete floor with laying compound strictly as per manufacturer's specification. Total thickness of the flooring shall be 40mm thick including the thickness of the tiles, under bed. Tiles will be laid with 2 mm gap using spacers and gap will be filled with black color epoxy latictere.

12.4 Granite Stone for floor Highlighter/steps: -

Providing 18 mm Prepolished Granite stone for Floor Highlighter/steps, in required design and pattern, with 12 mm (average) thick cement mortar 1:3 (1 cement : 3 coarse sand) laid and joint with white cement slurry including pointing with white cement slurry admixed with pigment of matching shade, all as per Architectural drawings, and as directed by the Engineer-in-Charge.

13. MISCELLANEOUS:**13.1 Conference table**

- a. Open type conference table for 08 people. Table top shall be of 25 mm thick Prelaminated MDF board.
- b. Legs: Ergonomically designed and matching with the open office concept. The leg is made out of specially designed aluminum extruded section.
- c. Beam: Beam is made of heavy duty Extruded Horizontal Aluminum profile.
- d. Cable tray: Shall be made up of 1mm thick CRCA sheet
- e. Accessories: With POP Up Boxes Switch and Socket.

13.2 Shoe Rack:

- a. Made up with 0.8 mm thk CRCA sheet powder coat finish/Prelaminated Particle Board 18mm thick.

13.3 Coat & Helmet Stand made up of matt finish SS

13.4 Operator Chair:-High back executive chair with synchronized tilting mechanism with multiple locking systems, ABS for seat, mesh back with Silver Epoxy Backbone with extra lumber Support with fine tuning for depth adjustment, with four way adjustable armrest, gas lift for height adjustment, nylon base with castors. Upholstery: Black fabric seat & mesh backrest & Black Leatherite headrest

13.5 3 Seater Sofa With Wooden Frame, SS Legs, Leatherite Tapestry Size (in mm)
1950 (L); 760 (D); 750 (H)

13.6 Printer Table for A4 size printer:-

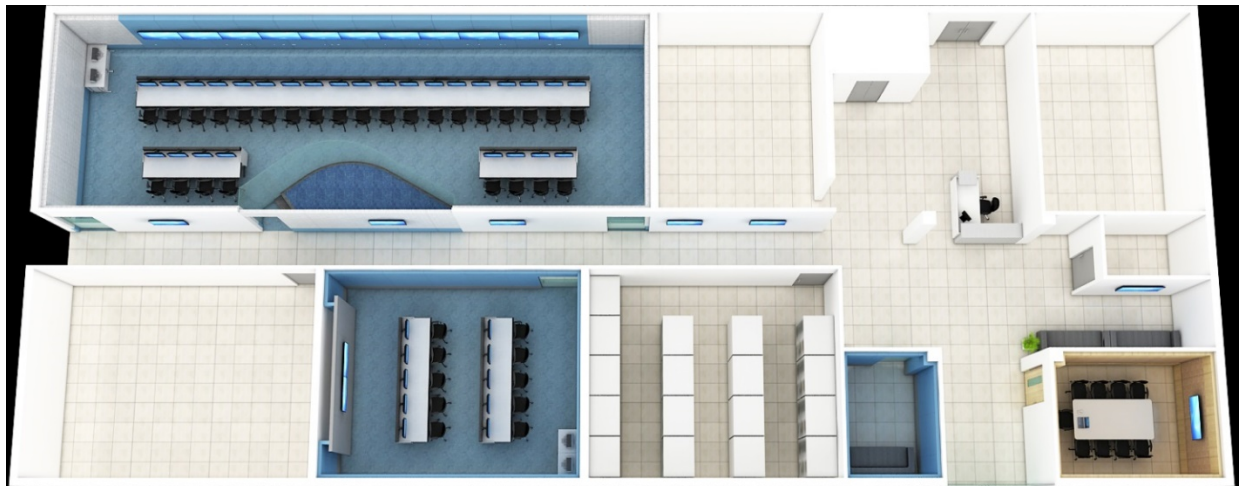
- a. Table top made of 25mm MDF.
- b. Extruded aluminum profile with 2 mm thk. Vertical support.
- c. Proper Cable tray for flow of wire.

GENERAL NOTES: -

1. The CONTROL & Development Centre room paneling and partition to have minimum 15% thermo-fused printed tiles (with similar material of construction as that of paneling and partition tiles) to print local art of state and increase the association of the facility with the state. Design will be selected by the Customer.
2. Warranty (for the entire CCR):
 - a. Lifetime warranty on structural stability.
 - b. Five years' warranty against any manufacturing defect on all modular/removable system.
 - c. Two year's warranty on all the consumables like Ceiling light, MCB's etc.

9.4.3. Indicative Representations of Command and Control Center

- a. 3D Top View of Command Centre



- b. 28-30 Seater Control Room with Viewing Gallery





c. Police Control Room for UP Dial 100

9.5. UP Dial 100 Control Room

At present there is an existing UP Dial 100 Control Room at Police Lines, Agra. The MSI should provide for display screens in the existing UP Dial 100 Control Room and/or provide for additional new UP Dial 100 Control room as part of command control Centre in the city.

A UP Dial 100 based police control room would empower people to connect to police and get police assistance anytime, anywhere at very short “response time”. The objective of UP Dial 100 Police Control Room in ICCC is to receive and respond immediately to emergency calls made by public seeking police assistance by directing the patrolling police vehicles available for the purpose. The center will be equipped with latest technological tools like GIS Map, CAD (Computer Aided Dispatch) and GPS enabled PCR VANS to handle public distress calls.

UP Dial 100 control room shall be provided with one PRI line inline hunting-single telephone number (100) to a group of 30 lines. The UP Dial 100 control system shall ensure that:

- 1) Calls can be made to 100 from any phone whether landline or mobile.
- 2) System has multiple caller interface and capable of receiving 30 calls at a single instance.
- 3) Caller’s name and address is automatically visible.
- 4) Exact location of incident & nearest available police vehicle identified on GIS map.
- 5) Status of response by police vehicle can be monitored by control room.
- 6) Information received, police action taken shall be automatically logged into the system, generating a fool proof database of events.
- 7) System should have facilities such as cell ID, Observed Time Difference of Arrival (OTDOA) and assisted GPS to acquire and push accurate location information for both wireless and wire line phone to emergency.

All communications in the call center shall be recorded for future reference. 50 TB storage capacity shall be allocated for recording voice communication through telephone line and radio gateway. The stored communication shall be available for hearing at any future point of time. The UP dial 100 control room shall be equipped with IT and Non-IT hardware and software.

9.5.1. Functional Requirements

- 1) Basic requirements of Police for setting up UP Dial 100 Control Room include but not limited to:
 - I. Establishing a quick and efficient emergency response system
 - II. Dispatch vehicles rapidly to required location
 - III. Automation of Call-taking & Dispatching
- 2) Computer Aided Dispatch (CAD) software platform integrates various modules:
 - I. CAD framework
 - II. Call Reception System
 - III. Call Recording and Logging
 - IV. GIS (Geographical Information System)
 - V. AVLS (Automatic Vehicle Location System)
 - VI. Responder Systems (Mobile Data Terminals)
 - VII. Incident Reporting System
 - VIII. Video Interface (CCTV Video Integration to GIS)
 - IX. Converged Communication Platforms [PSTN, Wireless (Cell Phone), SMS, e-mail]
- 3) Integrated Software Platform should support all features required for efficiently handling all stages of a call made in emergency.

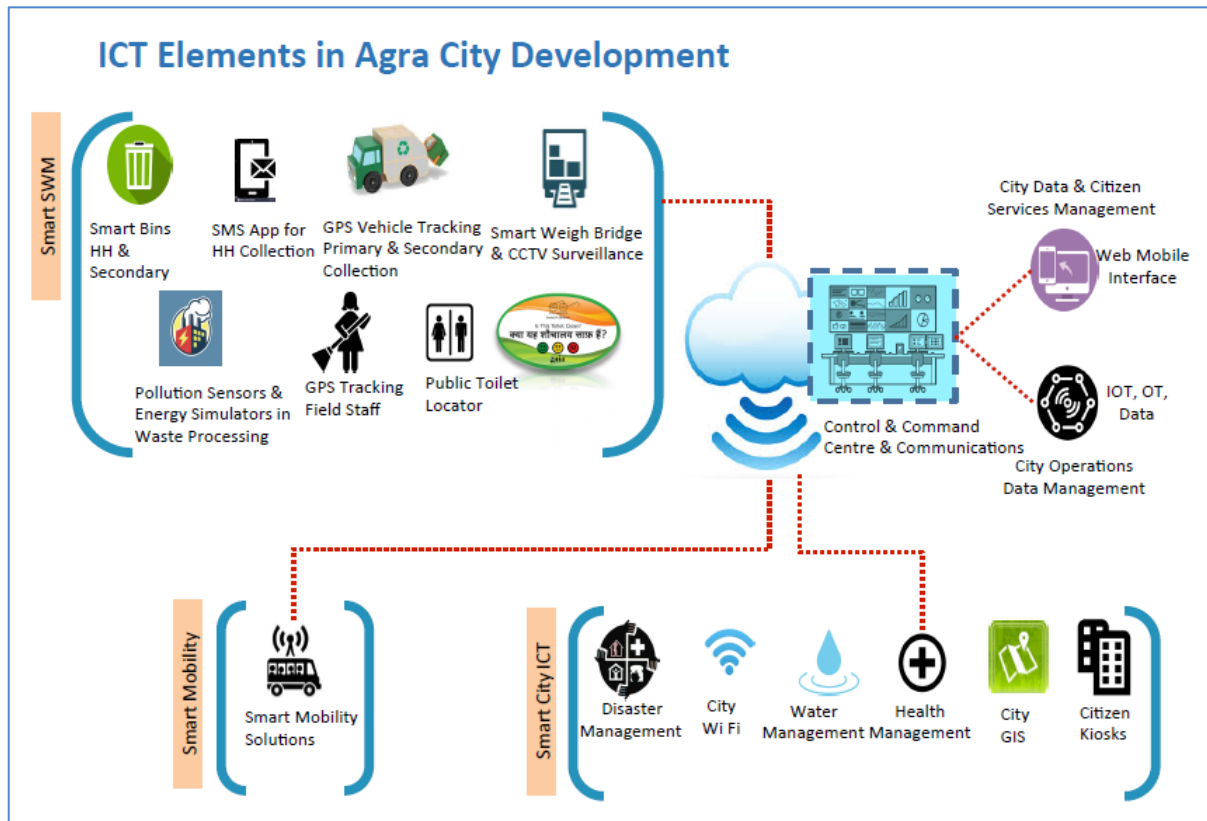
9.5.2. Operational Requirements

- 1) UP Dial 100 control room shall be equipped with EPABX comprising of 1 PRI line inline hunting-single telephone number (100) to a group of 10 lines.
- 2) Control room shall have seating capacity of minimum 10 operators.
- 3) Citizen can dial 100 for any complaints related with police. The system shall have capability to display name, address and find the geographical position of the caller at the time of receiving call in call Centre.
- 4) All phone calls shall be recorded for future references. The phone calls of last at least 90 days shall be stored in suitable Storage system.
- 5) Dial 100 operators shall be able to receive call, Dispatch calls, use GIS maps and can send the alerts to the nearby free patrolling vehicles on their MDT and also inform the nearest Police Station about the event.
- 6) Dial 100 operator shall be able to view the nearest Fire Station, Hospital, Blood Bank for providing additional assistance at the site of incident.
- 7) Dial 100 operator shall also be able to use police radio network for emergency handling and for communication with PCR Vans etc.
- 8) A web based incident analytic software shall be made available that will help the Police to do detailed analysis so that the response can be made proactively and also the effectiveness of the service is improved.

- 9) After the Call has been logged in by the call taker, the UP Dial 100 System shall send a SMS to the Caller stating the CFS/Tracking Number along with a password as acknowledgement to the call made to the control room. The caller can use this number on department website to access the event progress details such as Action Taken Reports (ATR), file attachments, remarks, or other information's as per the prevailing departmental policy for data sharing.
- 10) The analytics should have Social Media Analytics as one of the components. The city police and public functionalities need to be in touch with and accessible to general citizens especially youth, older citizens, media, etc. especially through social media. Analytics would leverage highly unstructured social media data in real time by using streaming social media analytics to identify rumors, potential threats and evolving events, find evidence through photos or track down witnesses. Analytics would also acquire location and tactical information of victims or criminals from information posted on Twitter, Facebook or other social media

9.6. City Operations Platform - Functional Specifications

- 1) Integrated Operations Platform (IOP) shall have IoT Platform Software (Data Normalization software) & City Operation Centre Software functionalities
- 2) All applications which have field infrastructure like – CCTV and Surveillance Components, Smart Traffic, Solid Waste Management, etc., proposed to be built as part of Smart City initiative shall pass information processing via IoT Platform.
- 3) IoT Layer must integrate lots of Services in the current scenario and must deliver an architecture which will be future scalable and can accommodate more Services / Utility Solution Integration as available in future.
- 4) IoT shall be a Common layer and is required for the Normalization of the data from different edge applications. This layer will aggregate and integrate utilities & sensors data to ensure that Device management, Analytics, Reporting, Dash Boarding and Integration of the Different Authorities data can be performed from a single operational screen. This layer shall also integrate with different Independent Software Vendor (ISV) applications hosted at Data Centre.



9.7. Forensic Investigation Room

- 1) Analysis in CCC 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.
- 2) The software must allow simple and quick search based on frequently used search parameters.
- 3) 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.
- 4) The software must be capable of replaying an unlimited number of multimedia channels in synchronized mode. The software must allow the user the capability of selecting and replaying part of a call, transmission, and video in either single item selection or when selecting multiple items.
- 5) 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.
- 6) 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.

- 7) 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.
- 8) The software system should provide detailed incident reporting and debriefing with time-coded playback of incident data on a single timeline.
- 9) It should allow synchronized playback - Exactly as it happened for postmortem analysis and review.
- 10) It should enable the authorities to find gaps in the incident handling and improve or rewrite SOPs.
- 11) CCC should have facility of integrating operator screen recording, Police (100), Fire (101) and 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.
- 12) 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.

9.7.1. Forensic Investigation Room – Operational Requirements

- 1) Forensic Investigation room shall be equipped with one video wall, four workstations, IP telephone and at least five operators in the city.
- 2) The forensic investigation room shall have seating capacity for min. 5 operators.
- 3) 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.
- 4) Video analytics software shall run on selected camera feeds to be further investigated by forensic operators.
- 5) Forensic operators shall be equipped with software for:
 - I. Examination of authenticity of uploaded photos and videos
 - II. Repair and recover videos
 - III. Match photographs
 - IV. Provide forensic video enhancement of video evidence for identifying suspects,
 - V. Provide recorded and archived media to authorized persons
 - VI. Transfer the evidence into a format that can be used for legal purposes etc.
 - VII. Post analysis of video provided through secondary source through various attributes like identified object, size, color etc.
- 6) Forensic operators shall also have access to recorded voice communications of dial 100 control room and radio gateway.
- 7) Forensic Analyst/Operator shall have following roles and responsibilities:
 - I. Examine, enhance and authenticate digital and analogue CCTV video evidence for both criminal and civil litigation
 - II. Assist the police in respect of preparation of evidence for legal and judicial purpose in court.
 - III. Providing recorded and archived media to authorized persons.
 - IV. Transfer the evidence into a format that can be used for legal purposes

- V. Provide Forensic video enhancement of video evidence for identifying suspects.
- VI. Attending and examining scenes of crimes
- VII. Repair and recovery of evidence

9.8. Integrated Operation Platform (IOP)

With the increasing urbanization, the operational issues are increasing which in turn affect the quality of services offered to the citizens. Various government agencies provide multiple services to the citizens. These agencies function in silos and provide a wealth of information which can be utilized for efficient services across the city in making decisions anticipating the problems and by ensuring cross-agency responsive actions to the issues with faster turnaround time.

Integrated Operation Platform (IOP) involves leveraging on the information provided by various departments and providing a comprehensive response mechanism for the day-to-day challenges across the city. IOP shall be a fully integrated portal-based solution that provides seamless incident – response management, collaboration and geo-spatial display.

IOP shall provide real-time communication, collaboration and constructive decision making amongst different agencies by envisaging potential threats, challenges and facilitating effective response mechanisms. Thus, the Integrated Operation Platform (IOP) provides a Common Operating Picture (COP) of various events in real-time on a unified platform with the means to make better decisions, anticipate problems to resolve them proactively, and coordinate resources to operate effectively.

IOP solution should be capable of seamless integration to various government and emergency services such as law enforcement, disaster and emergency services, utility services etc., the proposed solution should support recording of external mobile video feeds, data communication, telephony etc.,

MSI should ensure and support scenario reconstruction and analytics capabilities with event timelines. The solution should support event logs including operator's onscreen activities, voice & video events etc, for further analysis, training and similar activities. This can be in an integrated manner or through a standalone solution integrated with central platform.

Built in analytical tools provide real-time analysis of individual events and also a measure of the incidents for each of the silos integrated on the platform. These help the decision makers with the in-situ challenges and facilitate immediate responsive actions to mitigate / control multiple complex challenges.

Under the Agra Smart City initiative, it is intended to cover various disparate systems including:

- 1) Smart and Adaptive Traffic Signal Management (ATMS)
- 2) Intelligent Traffic Management System like ANPR, RLVD, No Helmet Detection, Face Recognition System etc.
- 3) CCTV based City Surveillance
- 4) ICT enabled SWM
- 5) Integrated Command and Control Centre

- 6) GIS Application
- 7) Meragra Citizen Engagement Application
- 8) Integrations with other systems which may arise in future like SCADA, Water Meter, City Wi-Fi, and Smart Components at Bus Shelters etc.

However, the platform shall support adding more layers of solutions seamlessly with minimal effort which purchaser intends to develop in time to come. On the Integrated Operation Platform (IOP), the system shall provide Standard Operating Procedures (SOPs), step-by-step instructions based on ASCL policies and tools to resolve the situation and presents the relevant situation information in a quick and easily digestible format for an operator to verify the situation. The system shall provide reporting & audit trail functionalities to track all the information and monitor operator interactions with the system and to impart necessary training to the users

9.9. IoT Platform – Functional Specifications

9.9.1. Data Aggregation, Normalization and Access

- 1) The city will be using various device vendors for various smart services. For example, in the Smart city journey of the city, various vendors of smart elements will be used for deployment and each will be generating data in their own format. This Platform should be able to define its own data model for each smart service like waste, lighting, transport, etc. and map data from different device vendors to the common data model.
- 2) Data from the IoT platform must be exposed to application eco system using secure APIs or any other secure methodology
- 3) Platform should be able to integrate with any type of sensor platform being used for the smart services irrespective of the technology used. Agnostics to sensor technologies such as LoRA, ZigBee, GPRS, Wi-Fi, IP Camera
- 4) Platform should also allow the manufacturers of the sensors to develop integrations themselves using the platform SDKs without affecting the northbound applications and existing integration.
- 5) Platform should be able to normalize the data coming from different devices of same type (i.e. Different lighting sensor from different OEMs, different energy meters from different OEMs etc.) and provide secure access to that data
- 6) Platform should support distributed deployment of functions (workflows & policies) across city's network and compute infrastructure with centralized management and control
- 7) Platform should be able to handle high data volume, handle a high events rate (upto 10,000 events per sec) with low latency processing
- 8) Platform should be able to correlate and handle multiple data streams, while providing real-time logic, analysis and routing applied to incoming data streams and aggregating data over time
- 9) Platform should store data in-memory (or to an external database) for use by other components or flows inside platform
- 10) Platform should an interface to graphically build and edit complex workflows that include data transforming, analysis, filtering and routing to destination system or using your output stream as input to other workflows. Adding an input or output device shall be as easy as dragging an adapter from a template and connecting it to flow

9.9.2. GIS Map Support

System should support GIS supported solutions like ESRI, etc.

- 1) Provides geographical coordinates of specific facilities, roads, and city infrastructure assets, as well as unmapped facilities
- 2) Calculates distance between two, or more, locations on the map
- 3) Locates and traces devices on the map
- 4) Software shall include an inherent Geographic Information Systems (GIS) view, supporting real world coordinates with predefined coordinate systems and DATUMS.
- 5) Software shall provide integrated capability with maps from survey of India and ESRI.
- 6) Software shall provide integrated capability to display high resolution satellite imagery and vector maps. To show the camera location on the map the map scale required is 1:1000 and to be created from high resolution satellite imagery of 0.5m
- 7) The GIS view shall provide a common operational picture enabling information sharing in real time between different users filtered according to predefined organization hierarchy. All GIS entities shall be automatically synchronized in the background between all client workstations.
- 8) The software shall display the building outline for all important buildings.
- 9) The GIS map shall support easy navigation operations such as pan, zoom in/ out, zoom to extent, previous zoom and next zoom
- 10) Software shall enable system administrators to define different data layers for displaying on GIS maps. Different layer types supported including geo referenced raster images, lines, zones , location of sensors and other objects (tracked vehicles for example)
- 11) Defined data layers can be turned on/off on demand or automatically according to predefined rules.
- 12) Software shall enable authorized users to edit the vector data presented within the defined layers.
- 13) When displaying layers, the Software shall enable administrators to turn their layers on/off when they are displayed
- 14) Software shall support saving of multiple GIS map views for later on demand or automatic popup. These views shall determine the selected layers and the exact map zoom level. The system shall support the ability to automatically bring up these predefined map views or locations most relevant to an incident.
- 15) Software shall support the customization and real time activation of multiple-level drill downs by linking objects placed on map layers to other GIS views.
- 16) Software shall support the placement of Action map objects on layers. Whenever these objects are clicked, the predefined action shall take place.
- 17) Software shall support the placement of predefined objects on map locations
- 18) Software shall allow for region of interest areas to be drawn on the map and pull out all the camera view simultaneously along with alerts like boundaries of police stations etc.
- 19) Software shall enable operators to add points, polylines and polygons to maps in order to identify multiple locations related to an incident.
- 20) Software shall enable users to open up a new incident and directly associate it with a map location or to associate an already opened incident with a new map location. The

system shall also be capable to receive an API call which will open up a new incident and automatically place it on the map using a map location passed via the API. The relevant map location shall be displayed on the map for as long as the incident is open.

- 21) Software shall support display of heat maps, pin map, trend map, repeat incident count map etc. over GIS maps based on incident data
- 22) Software shall support for configuration and display of cameras Field of View (FOV) overlay. It shall be possible to display the FOV for a single camera or for all cameras at once.
- 23) Users' (responders) map context menus shall include the capability to send other users messages, assign tasks and initiate phone calls. It shall also be possible to view the tasks presently assigned to selected users.
- 24) Software shall allow administrators to define and draw zones of arbitrary shapes and sizes. These zones shall be used for triggering various activation rules. The GIS shall be able to show/hide these zones as layers.
- 25) Software shall provide the ability to track movements and status of all location-based technologies (e.g. GPS, RFID, etc.). Software shall also support the on demand visual display of historical movement path.
- 26) Software shall support the searching of objects on the GIS map by name. The search shall support wild cards and shall highlight the found objects for easy identification.
- 27) Software shall support the ability to easily capture and send snapshots of the GIS maps.
- 28) Software shall provide users with a map 'Toolbox' with the most frequently used map operations for selected map entity types. The Toolbox operation buttons shall be customizable.
- 29) Software shall support the searching of a geographical location on the map, via entry of ZIP code, street address, milestone etc. ("Geo-coding").
- 30) Software shall support the calculation and map representation of the nearest geographical route between two locations. The calculation shall be capable of including factors such as street directionality.

9.9.3. IOT platform shall enable online Developer Program tools

It should help produce new applications, and/or use solution APIs to enhance or manage existing solution free of cost. The IoT platform vendor shall provide the platform SDK to such new application/system developers for such requirements.

9.9.4. Authentication

Authorization System should support standard Authentication and Authorization Methodology

9.9.5. Resiliency

- 1) Architecture should provide smart city use cases much needed resiliency.
- 2) Platform must support fault tolerance, load balancing and high availability
- 3) Provides ways to define policies that make applications or things respond to external

environments

- 4) Schedule actions to happen at future time points
- 5) Platform should have integrations with the network layer to proactively monitor any incidents on the network for active troubleshooting and triaging
- 6) Platform should be able to alert any incidents in the network proactively on City Operation Command Centre.

9.9.6. API Repository / API Guide

- 1) SDK/APIs should be available for the smart system domains (Outdoor Lighting, Traffic, Environment, Urban mobility etc.) to monitor, control sensor and/or actuators functionality to enable app developers to develop apps on the platform
- 2) For example - Vendor agnostic SDK/API to control Lighting functionality.
- 3) Platform OEM should provide the SDK/ APIs for the smart system domains (Parking, Outdoor Lighting, Traffic, Environment, Urban mobility etc.) to allow sensor vendors and app developers to develop their connectors / adaptors to the platform

9.9.7. Platform upgrade and maintenance

- 1) OEM should be able to securely access the platform remotely for platform updates / upgrades and maintenance for the given duration
- 2) Platform should be able to be deployed on DC/DR for disaster recovery

9.9.8. Platform functionality API management and gateway

Provides secure API lifecycle, monitoring mechanism for available APIs

- 1) User and subscription management: should provide different tier of user categorization, authentication, authorization, and services based on roles and responsibilities
- 2) Application management: should provide role-based access view to applications
- 3) Enabling analytics: Time shifted and real-time data available for big data and analytics
- 4) Platform should also be able to bring in other e-governance data in City Operations Command Centre dashboard
- 5) All data should be rendered / visualized on command and control centre dashboard.

9.9.9. SDK/API Based Open Platform

- 1) Provides SDK/API to develop applications for each of the Smart city Services domains.
- 2) Platform should have API Management capabilities like API Security
- 3) Platform should be able to provide SDK/API access based on roles and access control policies
- 4) MSI should have already documented the platform SDK/APIs using which applications can be developed
- 5) MSI should be able to demonstrate existing applications that are developed using these platform SDK/ APIs

9.9.10. Trending Service

System should provide trends in graphical representation from data sources over a period. Trends should allow to monitor and analyse device performance over time.

9.9.11. Policies and Events

- 1) System should allow policy creation to set of rules that control the behaviour of infrastructure items. Each policy should a set of conditions that activate the behaviour it provides. System should allow Default, Time-based, Event-based and Manual override polices creation. For example, an operator might enforce a "no parking zone" policy manually to facilitate road repairs.
- 2) System should provision to defines a set of conditions that can be used to trigger an event-based policy

9.10. Visualization Layer – Functional Specifications

9.10.1. ICCC Operations

Solution should be implemented and compliant to industry open standard commercial-off-the-shelf (COTS) applications that are customizable.

- 1) Solution should have the capability to integrate with GIS
- 2) Solution shall integrate with GIS and map information and be able to dynamically update information on the GIS maps to show status of resources.
- 3) Solution should allow defining key performance indicators and visualize the indicators on a web based configurable dashboard infrastructure
- 4) Solution should allow configuration and monitoring of service levels for key performance indicators and triggering of actions towards the incident management system when those service levels are breached.
- 5) Solution should provide current business status (snapshot) of City's facilities, departments and a holistic perspective of incidents and situations. Including incident handling time, number of false alerts, number of active and closed incident.
- 6) Solution event engine shall at minimum allow ingestion and processing of 10,000 events a second and provide a mechanism to scale to 100,000 events a second
- 7) 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. The above attributes shall be colour coded.
- 8) 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
- 9) Shall provide complete view of sensors, facilities, e-governance/ERP, video streams and alarms in an easy-to-use and intuitive GIS-enabled graphical interface with a powerful workflow and business logic engine
- 10) Shall provide a uniform, coherent, user-friendly and standardized interface
- 11) Shall provide possibility to connect to workstations and visualization layer shall accessible via web browser

- 12) Dashboard content and layout shall be configurable, and information displayed on these dashboards shall be filtered by the role of the person viewing dashboard
- 13) Solution should allow creation of hierarchy of incidents and be able to present the same in the form of a tree structure for analysis purposes
- 14) Shall be possible to combine the different views onto a single screen or a multi-monitor workstation
- 15) Solution should maintain a comprehensive and easy to understand audit trail of read and write actions performed on the system
- 16) Solution should provide ability to extract data in desired formats for publishing and interfacing purposes
- 17) Solution should provide ability to attach documents and other artefacts to incidents and other entities
- 18) Solution is required to issue, log, track, manage and report on all activities underway during these modes of operation:
 - recovery
 - incident simulation

9.10.2. Integration capabilities

Platform shall also be able to integrate, connect, and correlate information from IoT Platform and other IT & non-IT systems, providing rule based information drawn from various sub-systems for an alert. Platform shall have the ability to add / remove sensors including new vendor types as per future business requirements. It should support SDK/API based integration with the Smart system elements.

9.10.3. Notifications, Alerts and Alarms

System should generate Notification, Alert and Alarm messages that should be visible within the Dashboard and the Field Responder Mobile App if required.

- 1) All system messages (notifications, alerts and alarms) should always be visible from the Notifications view, which provides controls that operator can use to sort and filter the messages that it displays.
- 2) 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.

9.10.4. Users and roles

Users access the platform to perform various tasks, such as adding new locations, configuring new devices, managing adapters etc. Each user should be associated with one or more roles and each role is assigned a certain set of permissions.

- 1) Platform should allow different roles to be created and assign those roles to different access control policies.
- 2) Platform should allow single or multiple users to view and manage alarms in defined areas/Locations. User can be part of Single or multiple Areas/Locations.

9.10.5. Reports

Platform should have capability to provide access to real time data and historical data from various connected devices for reporting and analytics.

System should have ability to generate reports and have provision to add reports in favourites list.

- 1) Incident Reports
 - I. Detailed incident reports shall include an incident summary, all the tasks associated with the incident, sensor related activities, relevant snapshots, and maps.
 - II. Periodic Reports
 - III. Maintenance Reports
 - IV. Statistical Reports
- 2) Ability to display report on monitor and print report.
- 3) Ability to capture Operators response in Text
- 4) Ability to select information to be included in report at time of report generation.
- 5) Details of alarm including severity, time / date, description, and location.
- 6) Capture the operator response by text
- 7) Allow operator to transfer the incident report to Mobile Device/another operator's console

9.10.6. Standard Operating Procedure

SOP is a standard operating procedure which provides the step-by- step instruction in the shape of drop down menu to Command and Control Centre operator on how to handle a particular incident in an organized manner.

- 1) Software shall provide SOP's in English and Hindi language
- 2) SOP tasks should serve as an instructional resource that allows operator to act without asking for guidance.
- 3) There shall be the provision to define various SOPs in Command and Control System such as alert category specific SOPs, Location Specific SOPs
- 4) It should be possible to write SOPs in Hindi.
- 5) It shall have facility to define more than one SOP for the selected alert category or location
- 6) There shall be a provision to define multiple tasks under single SOP
- 7) The system shall select & present the appropriate SOP automatically based on predefined policies
- 8) Actions taken as part of SOP should be logged in audit trail with date time stamp and operator comments
- 9) SOP shall contain the lists of tasks to be performed by operator categorized under following headings
 - I. Task: Task to be performed by the operator in the sequential order.
 - II. Description: Task description.
 - III. Comments: Space for operator to enter the comments.
 - IV. Action: Actions (like email, sms escalation) to be initiated by operator.

- V. Done: Indication by operator that the task is completed.
- VI. User: User name of the operator for audit trail.
- VII. Date & Time: date time of the action.

9.10.7. Collaboration among Stakeholders

- 1) OCC platform should enable multiple stake holder Collaboration where incidents/tasks triggered automatically or manually by control room operators are distributed to the correct owners in incident/task context, such collaboration to include:
 - I. allowing departments to work autonomously
 - II. allowing logical locations or project groups to work autonomously
 - III. allowing inter-department
- 2) Stakeholders can be on various types of devices like computer, smart phones, tablets or normal phones
- 3) Platform should allow stakeholders to share multi-media content relevant to the issue in the collaboration space.
- 4) Platform should allow stakeholders with various smart devices (smart phones, Laptops, Analog Phones etc.) to invoke/participate in a web conferencing session directly from the collaboration space.
- 5) Platform should allow the stakeholders to acquire data from such devices and to control such devices, subject to access privileges for each user and device.

9.10.8. Analytics Engine

Smart city analytics platform module to maximize business value through advanced analytics capabilities. These advance analytics capabilities aid in automating policies that result in better asset and infrastructure management.

- 1) Solution should be flexible to integrate with other city and government software applications.
- 2) Analytics Engine module should have below intelligence capabilities;
 - I. Advanced Predictive Analytics should be part of the solution.
 - II. Solution should be flexible to integrate with other city and government software applications
 - III. Solution should be able to predict insights consuming data from city infrastructure viz., Traffic, Parking, Lighting etc.
 - IV. Solution should have predictions with acceptable & measurable accuracy Solution
 - V. Should be able to predict and integrate with Smart City solutions helping in driving operational policies creation.
 - VI. Solution should have a visualization platform to view historic analytics
- 3) Solution should have predictions with acceptable measurable accuracy
- 4) Application should enable the operators to discover, compare, and correlate data across heterogeneous data sources to unravel the patterns that are previously hidden. At a broader level, system should be do the following tasks:
 - I. Connect to a variety of data sources

- II. Analyse the result set
 - III. Visualize the results
 - IV. Capable of linear and empirical prediction using historical data.
- 5) Analytics Engine should support multiple Data Sources. Min below standard data sources should be supported from day 1 – CSV, TSV etc.
 - 6) Analytics Engine should provide analysis of data from a selected data source(s).
 - 7) Analytics engine should provide capability to check analysis with multiple predictive algorithms
 - 8) Analytics Engine Visualizations - Analytics Engine should provide visualizations dashboard.
 - 9) In the visualization workspace, it should allow to change visual attributes of a graph.
 - 10) User should not be allowed to alter the graph/visualization definition.

9.10.9. API & Interface Security

- 1) Access to the platform API(s) should be secured using API keys.
- 2) Software should support security standards: OAuth 2.0, HTTPS over SSL, and key management help protect the data across all domains.
- 3) Should support security features built for many of its components by using HTTPS, TLS for all its public facing API implementations. For deployment where OCC Software API(s) exposed to application eco system, API Management, API security features and API Key management functions are required.
- 4) Platform vendor should maintain complete inventory of critical production assets. Asset could be defined as source code, documents, binaries, configuration data, scripts, supplier agreements, SW Licenses

9.10.10. Business Operations Audit & Logging

Platform should support centralized logging & auditing framework.

- 1) Legal / Supplier chain agreements: Platform provider vendor should have policies and procedures established, and supporting business processes and technical measures implemented, for maintaining complete, accurate and relevant agreements (e.g. SLAs) between providers and customers
- 2) Critical production assets: Platform vendor should maintain complete inventory of critical production assets. Asset could be defined as source code, documents, binaries, configuration data, scripts, supplier agreements, SW Licenses
- 3) Audit trail must be available in the platform

9.10.11. Field Responder Mobile

Provide Integrated Mobile Application for capturing real-time information from the field response team using Mobile- Standard Operating Procedure. Overall Integrated Operations Platform should account for below solution components, City Tenant activation license with one lakh device connection

- 1) Operator Client License min 25 with one city activation license
- 2) Field Responder should be able to acknowledge the incident and provide real time

updates from the incident site.

- 3) Field Responder should be able to view the recorded stream and image of the event
- 4) Field Responder should be able to view live stream of the camera
- 5) Field Responder should be able to send ATR or action taken for the event to the command and Control application

9.11. Video Management System – Functional Specifications

Video Management System (VMS) shall bring together physical security infrastructure and operations and shall use the IP network as the platform for managing the entire surveillance system. End users shall have rapid access to relevant information for analysis. This shall allow operations managers and system integrator to build customized video surveillance networks that meet their exact requirements. Software suite shall be a scalable and flexible video management system that could be easily managed and monitored. Scalable system shall permit retrieval of live or recorded video anywhere, anytime on a variety of clients via a web browser interface.

Video management server, on which the VMS is hosted upon, shall run seamlessly in the background to manage connections, access and storage. Video management server shall either accept directly or indirectly the feed from IP Camera installed at field locations. Server shall stream incoming video to a connected storage. VMS shall support directly or indirectly video IP fixed color / B&W cameras, PTZ / Dome cameras, Multi-sensor Cameras, infrared cameras, low light/IR cameras and any other camera that provides a composite PAL video signal.

VMS shall facilitate situational awareness of the on-ground condition at Command Control Centre or any other view Centre. This shall be achieved by transmission of real time imagery (alarm based or on-demand). This imagery can be viewed live by operators and/or recorded for retrieval and investigation. Major functionalities are described here:

- 1) VMS shall support a flexible rule-based system driven by schedules and events.
- 2) VMS shall be supported for fully distributed solution for monitoring and control function, designed for limitless multi-site and multiple server installations requiring 24/7 surveillance with support for devices from different vendors.
- 3) VMS shall support IP cameras of different makes.
- 4) All the offered VMS or integrated Analytics Systems for cameras shall have ONVIF compliance.
- 5) VMS shall be enabled for any standard storage technologies and video wall system integration.
- 6) VMS shall be enabled for integration with any external Video Analytics Systems.
- 7) VMS shall be capable of being deployed in a virtualized environment without loss of any functionality.
- 8) VMS server shall be deployed in a clustered server environment for high availability and failover.
- 9) All CCTV cameras locations shall be overlaid in graphical map in VMS Graphical User Interface. Camera selection for viewing shall be possible via clicking in the camera location

- on graphical map. Graphical map shall be of high resolution enabling operator to zoom-in for specific location while selecting a camera for viewing.
- 10) VMS shall have an administrator interface to set system parameters, manage codecs, manage permissions and manage storage.
 - 11) VMS day to day control of cameras and monitoring on client workstations shall be controlled through the administrator interface.
 - 12) Whilst live control and monitoring is the primary activity of the Operator workstations, video replay shall also be accommodated on the GUI for general review and also for pre and post alarm recording display.
 - 13) Solution design for VMS shall provide flexible video signal compression, display, storage and retrieval.
 - 14) All CCTV camera video signal inputs to the system shall be provided to command control Centre, and the transmission medium used shall best suit the relative camera deployments and access to the CCTV Network.
 - 15) VMS shall be capable of transferring recorded images to recordable media (such as CD/DVD and/or DAT tapes) in tamper evident and auditable form. All standard formats shall be supported including, but not limited to:
 - I. AVI files
 - II. Motion- Joint Photographic Experts Group (M-JPEG)
 - III. Moving Picture Expert Group-4 (MPEG-4)
 - 16) All streams shall be available in real-time (expecting network latency) and at full resolution. Resolution and other related parameters shall be configurable by administrator to provide for network constraints.
 - 17) VMS shall support field sensor settings. Each channel configured in the VMS shall have an individual setup for the following minimum settings, the specific settings shall be determined according to the encoding device:
 - I. Brightness/Contrast
 - II. Colour/ Sharpness
 - III. Saturation/ Hue
 - IV. White balance
 - 18) VMS shall support the following minimum operations:
 - I. Adding an IP device/ Updating an IP device
 - II. Updating basic device parameters
 - III. Adding\Removing channels
 - IV. Adding\Removing output signals
 - V. Updating an IP channel/ Removing an IP device
 - VI. Enabling\Disabling an IP channel
 - VII. Refreshing an IP device (in case of firmware upgrade)
 - 19) VMS shall support retrieving data from edge storage. When a lost or broken connection is restored, it shall be possible to retrieve the video from SD card and store it on central storage.
 - 20) VMS shall support bookmarking the videos. Thus, allowing the users to mark incidents on live and/or playback video streams.

- 21) VMS shall be capable of intrusion detection: Detection of moving objects in selected areas covered by the camera (those that are specified as restricted areas like those before some major events, etc.). Avoid false alarms due to wildlife or other moving objects (e.g., tree leaves).
- 22) VMS shall be capable of tracking of a specific person in multi-camera videos: Track a specific person across several surveillances (e.g., to trace and identify criminals and/or anti-social elements). The operator shall be able to efficiently locate and track a specific person across time and location to minimize search time from hours to minutes when time is of the essence. This application should be opened from the native VMS client application without the need to login again.
- 23) VMS shall be capable of counting of people and detection of abnormal crowd behavior: Detection of people flow and counting of people in selected areas. To identify abnormal crowd behavior and raise alarms to avoid untoward incidences in public places, and maintaining law & order.
- 24) VMS shall provide a seamless integration between all recorders types under the same user interface and management system.
- 25) VMS shall have a central database (AMS) for consistent configuration of site equipment and user data. The centralized management shall be available from remote locations over the network.
- 26) VMS shall allow the user to select the streaming method to workstation running the VMS application. The user shall have the ability to select RTP/UDP, TCP or direct multicast protocol.
- 27) VMS shall support ipv4 and ipv6 at least between the camera and the recording server
- 28) VMS shall allow the user the ability to define a homepage to be displayed in the local workstation. The homepage shall include a specific layout of video panes and pre-selected cameras either in live or playback modes, as well as other security sensors and maps
- 29) VMS shall support automatic failover for recording.
- 30) VMS shall support manual failover for maintenance purpose.
- 31) VMS shall support access and view of cameras and views on a smartphone or a tablet
- 32) VMS shall support integration with the ANPR/RLVD application.
- 33) VMS shall support integration with other online and offline video analytic applications.

9.11.1. VMS Core Components

- 1) CCTV Camera Management: enables management of cameras associated with VMS.
- 2) Video recording, retrieval and archiving: manages live camera viewing, recording of live feeds for future review, search and retrieval of recorded feeds and archiving of recorded video feeds for optimum utilization of resources.
- 3) Video Analytics (VA) alert management: enables defining of rules for handling of alerts using the VA handling of events as per the defined rules.
- 4) MIS and Reporting: provides users with business analytics reporting and tools to organize evaluate and efficiently perform day to day operations.
- 5) Security and Roles: manages role definitions for internal & external access.

9.11.2. VMS General

- 1) VMS shall be Codec and IP camera agnostic such that it can support devices that are not supplied by manufacturer/developer of VMS software and Codec hardware.
- 2) When viewed on GIS map, text description of each camera shall be capable of being positioned anywhere on the monitor screen, on a camera by camera basis, shall afford options for size variations, and display with a flexible solid, semi-transparent or transparent background.
- 3) VMS shall support tamper detection for all cameras to warn of accidental or deliberate acts that disable the surveillance capability.
- 4) For alarm interfacing requirements, VMS shall allow selection of minimum five (5) cameras per single alarm source. The designated primary camera shall be automatically displayed as a full-screen image on the main GUI CCTV screen. VMS shall also, on alarm, present associated pre/post event video allowing the Operator to assess the alarm cause. Other associated cameras, when called up, shall be displayed as split-screen images on the other monitor of the operator workstation.
- 5) VMS shall provide LoS support in MPEG4 or H.264 for monitoring of dual streaming devices. Therefore, it shall automatically select the most appropriate stream from the edge device in accordance with the workstations/decoder performance and network bandwidth.
- 6) VMS shall provide by the LoS mechanism different streams for recording and monitoring, improving monitoring quality while preserving storage space. The streams can be configured to different resolution, frame rate or bit-rate.
- 7) Playback of any alarm related video, (including pre and post alarm video) shall start at the beginning or indexed part alarm sequence.
- 8) Video management software shall incorporate online video analytics. It shall include the following video analytics detection tools:
 - I. Loitering detection
 - II. Improper Parking
 - III. Camera Tampering
 - IV. Abandoned objects detection
- 9) Off-Line Video Analytics should allow for quick retrieval of video footage to metadata stored with each image. System should provide results within few seconds, system should support for below listed the user's query.
 - V. System should allow to specify the following search criteria:
 - i. Motion in the zone, user-defined with any polyline
 - ii. Detection of crossing a virtual line in a user-defined direction
 - iii. Loitering in an area
 - iv. Motion from one area to another.
- 10) Video clips of specific events via Video Analytics or by operator action shall be capable of being separately stored and offloaded by operator with appropriate permissions on to recordable media such as CD or Write Once Read Many (WORM) together with any associated meta-data for subsequent independent playback.
- 11) System shall provide the capability to select duration and resolution of storage by camera, time and activity event and user request. Frequency/trigger of transfer shall be configurable by user.

- 12) System shall provide the capability to digitally sign recorded video.
- 13) Live video viewing: System shall allow the viewing of live video from any camera on the system at the highest rate of resolution and frame rate that the camera shall support on any workstation on the network.
- 14) Recorded video viewing: System shall allow the viewing of recorded video from any camera on the system at whatever rate the camera was recorded.
- 15) Storage of video: System shall store online thirty (30) days of video for all cameras. Balance 60 days will be on low cost secondary storage /tape library
- 16) System shall provide the capability to manage the video storage to allow selective deletions, backups, and auto aging.
- 17) VMS shall have an extensive reporting capability with ability for administrator to define reports in a user-friendly manner. The pre-existing reports shall include, but not limited to, the following:
 - I. Reports on alerts received by type, date and time, location
 - II. Reports on system errors and messages
 - III. Reports on master data setup including cameras, decoders, locations
 - IV. Reports on cameras health check
 - V. Reports on audit trails such as user actions
 - VI. Reports on system health including storage availability, server performance, recordings

9.11.3. VMS GUI Capabilities

- 1) User interface shall be via a GUI providing multiple video streams simultaneously on multiple monitors.
- 2) GUI shall have the minimum capability of naming locations, users, and cameras events be displayed correctly on user's screen.
- 3) System shall have the capability to store and record operator specific options, such as screen layout, video layout, action on alarm, and automatic video transmission settings on events.
- 4) GUI shall conform to standard Windows conventions.
- 5) System shall provide unified GUI camera control at an operator's workstation for all types of cameras installed whether existing or new or connected via another agency. By means of this unified control the following functions shall be provided:
 - I. Selection
 - II. Display
 - III. PTZ
 - IV. Setup and adjustment
 - V. Determination of pre-sets
 - VI. Any other commissioning and camera setup activity
- 6) All user interfaces shall support English Language and shall conform to standard Windows protocols and practices and allow the control of all functions via a simple easy to use interface.

9.11.4. VMS Map Functionality

- 1) System shall support a mode of operation whereby a map of all or part of the map (at

operator request) is displayed on a separate or same screen and that status information can be provided via an icon, and access to any cameras shall be accessible by means of an icon on that screen.

- 2) These Maps shall be defined so that an operator may select from the same source of mapping that is available to the other systems within the command control Centre, displaying whichever Map or section the operator needs, and it shall be displayed within one (1) second.
- 3) VMS shall allow the user to perform operations on cameras or any other sensors that are placed on a map.
- 4) VMS shall allow the user to “drag & drop” a camera or any other sensor from the map area to a video window or to click on a camera to start viewing it in a pop-up window.
- 5) The map supported formats shall be: BMP, GIF, JPG, PNG and TIFF.

9.11.5. VMS Configuration

- 1) VMS shall include a configuration facility to provide system administrators with a single interface utility to configure all VMS operating parameters.
- 2) Configuration tool shall be as sophisticated as necessary to support the following:
 - I. Log every action so an audit or report can be completed
 - II. Only update & log configurations where there is a difference between the system configuration and the new configuration file to be loaded
 - III. The import configuration file can contain any amount of data
 - IV. Ability to run an update on the fly i.e. no or minimal system downtime
 - V. Not require a reset or restart after any upgrades
 - VI. Definable update times
- 3) VMS configuration tool shall define:
 - I. Cameras (whether via codec units or directly connected IP cameras) and text based names
 - II. Camera Groups / User Groups
 - III. Monitors / Codec parameters
 - IV. Alarms
 - V. Workstations/ Storage
- 4) Configuration utility shall allow the system administrator to:
 - I. Install new devices
 - II. Configure all aspects of existing devices
 - III. Configure and set up users/user groups and their rights/ permissions/ priorities
 - IV. To define multiple camera groups
 - V. Each group to be defined for combinations of viewing and control rights
 - VI. Individual Operators to be assigned multiple groups
 - VII. Each group to be allocated to multiple Operators
 - VIII. Each camera may be in multiple groups
 - IX. To program macros for individual and group camera characteristics
 - X. Program camera/monitor selection and configuration of the video wall(s) in response to an incoming alarm
 - XI. Designate workstation destination for picture presentation in response to alarm

initiation

- 5) User permissions/privileges, to be allocated, shall extend from full administrator rights down to basic operation of system, and shall include the ability to designate workstations to an operator, and to designate one or more camera groups to an operator for viewing and/or control.
- 6) Configuration utility shall store all changes to system, including but not limited to:
 - I. User log-ins /User log-offs
 - II. Human interface device inputs (key strokes)
 - III. External alarm commands/ Error messages
- 7) A copy of system configuration shall be stored external to the system to allow system restoration in case of hardware failure.

9.11.6. VMS User Hierarchy

- 1) MSI shall request a detailed User Prioritization List (UPL) during the project.
- 2) UPL shall enable programming of CCTV management system with agreed user prioritization.
- 3) Over and above user priority, users shall be enabled for following in varying combinations:
 - I. Image viewing
 - II. Image recording
 - III. PTZ control
- 4) In addition, control location shall be prioritized such that command control Centre has full control of all functions and priority one override over all other locations.
- 5) Within the hierarchy, each user's log-on password shall not only allow access to varying levels of system functionality, but shall provide for relative priority between users of equal access rights. Operators in above groups shall be individually allocated a priority level that allows or denies access to functions when in conflict with another operator of lower or higher priority level.
- 6) These priority levels and features they contain shall be discussed and defined with the system administrator. MSI shall allow time to carry out this exercise together with relevant configuration of groups, sub-groups, permissions and priorities.

9.11.7. VMS Recording Requirements

- 1) All images shall be recorded centrally as a background process at configurable parameters.
- 2) It shall not be possible to interrupt, stop, delay or interfere with the recording streams in any way, without the appropriate user rights.
- 3) CCTV recording system shall enable Pre and Post Event (PPE) recording, presentation and storage, initiated automatically in response to system alarm sources received by the VMS.
- 4) PPE recording clips shall be provided by the VMS and retrieved from the central video archive on the buffer storage system. This PPE stream shall be totally independent of the background recording stream provided to the central video archive such that central video archive recording, as programmed, continues under all circumstances.
- 5) Information stored shall be full real-time and full resolution from each incoming camera channel. In the absence of a trigger from a manual input or from a programmed alarm source, the PPE video recording shall be written to buffer storage on a FIFO basis.
- 6) PPE periods initiated by a single alarm occurrence shall be configurable via the VMS as

follows:

- I. Pre – 0 to 30 seconds
 - II. Post – 30 to 300 seconds
 - III. Shall be variable for each camera according to each individual alarm and the alarm type
- 7) In the event of a trigger, VMS shall ensure that the programmed sections of pre and post event video are immediately presented to the Operator to complement alarm display and simultaneously saved as an identified indexed video clip, complete with time/date stamp, in a reserved and protected area of storage system. Such PPE recording shall then be capable of retrieval via search criteria.
- 8) Once tagged and saved, the PPE video clip shall NOT be overwritten except by an operator with the required permissions i.e. it is excluded from the normal FIFO regime of the bulk storage system. Recording shall also be initiated on-demand by manual triggers from system operators e.g. keyboard key-stroke.
- 9) VMS shall support the following recording modes:
- I. Total recording - VMS shall constantly record video input. VMS shall allow for continuous recording of all video inputs
 - II. Event based recording - VMS shall record video input only in case an event has occurred
 - I. The recorder shall allow for event recording mode, recording upon an alarm, on all or some of the channels.
 - II. Each event-configured channel shall have the ability to be triggered by multiple triggers
 - III. Marked events shall include the pre and post alarm recording time.
 - IV. The user will be able to query for all events per channel, per time, per triggers, per comments and to playback the selected event.
- 10) VMS shall support following triggers to initiate a recording
- I. Scheduler - recorder will record video inputs based on a specified schedule.
 - I. VMS shall allow recording based on a time schedule for all or some video channels
 - II. VMS shall allow for multiple recording periods per day, per channel
 - III. VMS shall have option to set any available trigger in the system (VMD, TTL and/or API) to trigger the channel
 - IV. VMS shall have option for individual channel setup of pre/post-alarm recording for defined interval (e.g. up to 10 minutes pre-alarm and 30 min post-alarm recording)
 - V. VMS shall have ability to enable/disable triggers through a daily time schedule
 - II. Manual - user shall be able to initiate a manual recording upon request
 - III. VMS shall work in conjunction to the any previous alarm operations
 - IV. VMS shall allow API Triggers
 - V. All trigger information shall be stored with the video information in the VMS data set and shall be made available for video search
 - VI. VMS shall support the following recording modes:
 - VII. Total recording - VMS shall constantly record video input. VMS shall allow for continuous recording of all video inputs

- VIII. Event based recording - VMS shall record video input only in case an event has occurred
 - i. The recorder shall allow for event recording mode, recording upon an alarm, on all or some of the channels.
 - ii. Each event-configured channel shall have the ability to be triggered by multiple triggers
 - iii. Marked events shall include the pre and post alarm recording time.
 - iv. The user will be able to query for all events per channel, per time, per triggers, per comments and to playback the selected event.
- IX. VMS shall support following triggers to initiate a recording
- X. VMD (Video Motion Detection) – Video motion detection running on the edge device.
- XI. The recorder shall support VMD per video channel

9.11.8. Manual or on demand recording

- 1) Recording shall also be initiated on-demand by manual triggers from system operators e.g. keyboard key-stroke (subject to user rights).
- 2) System shall allow for an operator to initiate recording on any live stream being viewed.

9.11.9. VMS review system

VMS recording and replay management systems shall support the following features and operations:

- 1) Play back shall not interfere with recording in any way
- 2) Support either analogue cameras connected via Codecs or IP-cameras directly connected to the network
- 3) Stream live images through the network using IP Multi-cast techniques
- 4) Stream images from the Codec to the attached storage system
- 5) Store the recording stream from all cameras simultaneously with no degradation to any individual camera recorded image stream unless the system is configured by administrator to allow for change in quality
- 6) Deliver live video to VMS workstation within a period of one second from manual call up
- 7) Deliver live video to VMS workstation within a period of three seconds from automatic alarm receipt on alarm interface
- 8) Storage of each camera's images at a rate and resolution as defined in the Codec or IP camera configuration. VMS programming shall automatically vary these rates in response to time profiles, alarm inputs
- 9) Support multiple, configurable recording time schedules per camera. Each schedule shall support different recording parameters and automatically implement against configured time schedule e.g. operational and non-operational hours shall be scheduled with different recording parameters on designated cameras
- 10) Support streaming of recorded files using IP Unicast directly to hardware decoders for display on analogue monitors or software decoder when/if required
- 11) Playback multiple, synchronized recorded streams at differing speeds and frame rates
- 12) Record and playback a video stream simultaneously at differing speeds and frame rates
- 13) Time stamping of every recorded video field based upon Network Time Protocol (NTP) time

- 14) Support video streaming directly from the edge devices.
- 15) When streaming directly from the edge devices the workstation shall receive a multicast stream directly from the edge device for monitoring purposes. The recorder shall register to the same multicast group for recording
- 16) Selectable on-screen-display of time and camera title during playback
- 17) Security file lock to prevent specific recorded files from being overwritten regardless of their date and time, in addition to those records stored as PPE clips. The duration and policy for retention of such videos would be same as that of the PPE clips
- 18) Configurable granularity of video files
- 19) Generate alarm when storage medium has fallen below a user selectable threshold
- 20) Stored video files can be “downloaded” directly to DVD or WORM for replay using VMS video replay application and shall incorporate proof of authenticity
- 21) Download video records in common (e.g. AVI) file format for remote, cursory review and assessment prior to generating tamper-evident auditable copies

9.11.10. VMS Alarm Handling

- 1) Actions Associated with Alarms.
 - I. VMS shall allow associating a system action to an alarm.
 - II. Each alarm shall change the icon of the alarmed sensor indicating its alarmed state.
 - III. Each alarm shall have the capability to be assigned to individual users or to user groups (roles).
 - IV. User shall have the ability to set or filter cameras and any other sensor in the cameras/sensors list/tree according to the alarm state or that sensor.
- 2) Alarm Notification.
 - I. VMS shall support the following methods of notifying users that a video alarm has occurred:
 - i. Indicate the alarm of a camera or sensor in the main cameras/sensors list.
 - ii. Alarm video pop-up on local or external monitors.
 - iii. Audio notification may be sounded when the event occurs.
 - iv. API – Notifies a third party security system that a video alarm has occurred.
 - v. TTL/Relay – Activates a TTL/Relay to drive an external alarm device.
 - II. VMS shall support standard SNMP v3 for notifying that a maintenance alarm has occurred.
- 3) Alarm Display on Local Workstation
 - I. User shall have the ability to associate each video alarm with a pre-defined alarm page which contains a video pane layout and pre-configured cameras in live or playback mode.
 - II. User shall have the ability to configure a different alarm page for each alarm in the system.
- 4) Automatic Actions upon Alarm.
 - I. User shall have the ability to define rules to automatically execute actions upon an alarm condition.
 - II. Automatic actions upon an alarm condition shall include the following actions: Send command to sensor, Play page locally, Play page on external monitor, Display live

video, Display playback video, Close video, Move camera to PTZ preset, Start/Stop Virtual Tour, Start/Stop recording, Play a predefined sound, Send an HTTP request, Execute an external application locally on the operator workstation.

5) Alarm/Incident Workflow.

- I. User shall have the ability to define a workflow for each event.
 - i. User shall have the ability to define a procedure containing a list of tasks instructing the operator what actions to take when an alarm occurs. Other users shall be able to see the status of each task for a specific event on the respective workstation.
 - ii. The workflow shall be adaptive to the user's selections and change the remaining tasks in the workflow based on conditional tasks that present multiple options to proceed.
 - iii. The workflow shall support simple tasks that can be managed (e.g. completed) manually, as well as automatic tasks that execute an automatic action that performs a system command and/or a sensor command.
 - iv. Automatic actions executed as automatic tasks in a workflow procedure shall support creating, closing and changing incidents.
 - v. User shall have the ability to change the state of each task to: Suspend, In Progress, Complete, Cancel and Fail.
- II. User shall have the ability to acknowledge, reject or reset each alarm – after the alarm has been acknowledged all authorized users shall see the alarm status change on their respective workstations.
- III. The system administrator shall have the ability to audit user alarm actions (acknowledge /reject/reset).
- IV. User shall be able to comment an alarm.

9.11.11. VMS Integration requirements

- 1) VMS shall be integrated with the Command and Control System via SDK/API. All events and alarms that occur with the VMS and its sub systems will be available in the Command and Control System as required based on the SDK/API integration.
- 2) Either OPC or SDK shall manage interface between VMS, GUI and other City Management systems as required.
- 3) OPC or SDK shall allow the operator workstations to control the VMS irrespective of the vender chosen by duplicating all control functionality of the VMS used for normal day-to-day activities.
- 4) Alarm linking between VMS sub-systems shall be done at VMS sub-system level to, for example, call up relevant pictures to screens and move PTZ units to pre-set positions in response to alarm and activate video recordings, modifying recording parameters as necessary.
- 5) All OPC software shall be fully compliant with the OPC specification as set down by the OPC foundation. Any software or products which are not compliant shall be highlighted in the Technical Proposal return. MSI shall indicate in the technical proposal return how the OPC interface shall be implemented.
- 6) If an OPC interface cannot be provided, an alternative solution shall be provided for this data

using a standard open protocol and confirmation as to how this shall be implemented shall be provided in the technical proposal return.

- 7) If an SDK solution is provided the system shall allow reconfiguration by (City) and end users without recourse to special languages. A system SDKs shall be supplied with all required supporting software to allow the integration of the system with new devices and systems.

9.11.12. VMS System Size

VMS shall enable handling of all the cameras, on day one, as well as future scalability as may be required.

9.12. Video Analytics – Functional Specifications

Surveillance system shall have capability to deploy intelligent video analytics software on any of the selected cameras. This software shall have capability to provide various alarms & triggers. The software shall essentially evolve to automate the suspect activity capture and escalation; eliminate need of human observation of video on a 24x7 basis.

Analytics software shall bring significant benefit to review the incidences and look for suspicious activity in both live video feeds and recorded footages.

Minimum video analytics that shall be offered on identified cameras are:

- Attribute Based Search
- Loitering detection
- Improper Parking
- Camera Tampering
- Abandoned objects detection
- Unattended object
- Tripwire/Intrusion

9.13. Access Control System – Functional Specifications

Access Control System shall be deployed with the objective of allowing entry and exit to and from the premises to authorized personnel only. The system deployed shall be based on Biometric Technology. An access control system consisting of a central PC, intelligent controllers, power supplies and all associated accessories is required to make a fully operational online access control system. Access control shall be provided for doors. These doors shall be provided with electric locks, and shall operate on fail-safe principle. The lock shall remain unlocked in the event of a fire alarm or in the event of a power failure. The fire alarm supplier shall make potential free contacts available for releasing the locks in a fire condition especially for staircase and main doors. Entry to the restricted area shall be by showing a proximity card near the reader and exit shall be using a push button installed in the secure area. The system shall monitor the status of the doors through magnetic reed contacts. The system should be designed and implemented to provide following functionality:

- I. Controlled entries/ exits to defined access points
- II. Controlled entries and exits for visitors
- III. Configurable system for user defined access policy for each access point

- IV. Record, report, archive each and every activity (permission granted and / or rejected) for each access point.
- V. User defined reporting and log formats
- VI. Fail safe operation in case of no-power condition and abnormal condition such as fire, theft, intrusion, loss of access control, etc.
- VII. Day, Date, Time and duration based access rights should be user configurable for each access point and for each user.
- VIII. One user can have different policy/access rights for different access points.

9.14. Edge Analytics and Artificial Intelligence with Continuous Learning

These use cases are to be implemented using Artificial Intelligence through various cameras, sensors etc at the edge/field devices with continuous learning capabilities, Following use cases shall be part of implementation and shall have capability to integrate with common platform used for monitoring purpose (considering future and not necessary at day one):

- | | | |
|--|--|--|
| Property of Interest | | |
| i. Camera Tampering | | xviii. Municipal parking management |
| ii. Abandoned objects detection | | xix. Automatic Anomaly Detection |
| iii. Object Classification | | xx. Integrated Traffic Management System |
| iv. Tripwire/Intrusion detection | | xxi. Graffiti |
| v. Vehicle attributes Detection (Color/Make/Model) | | xxii. Vandalism |
| vi. Automatic Number Plate Detection | | Person of Interest |
| vii. Tracking vehicle across cameras | | i. Loitering detection |
| viii. Speed of car/ Vehicle | | ii. Face Recognition |
| ix. Helmet detection on two wheelers | | iii. Person tracking over network of cameras |
| x. Wrong way driving detection | | iv. Gender identification: Male or female |
| xi. Illegal turn by vehicle | | v. Hair identification: Long or short hair |
| xii. Triple Riding on 2 Wheelers | | vi. People counting |
| xiii. No Seat Belt | | vii. Person collapsing |
| xiv. Smoking in Car while driving | | viii. Incident detection: Fight (action) |
| xv. Use of Mobile Phones during driving | | ix. Person waving (gesture recognition) |
| xvi. Improper/illegal Parking | | x. Dwell time for person of interest |
| xvii. Authorized vehicle | | xi. Threat Detection |
| | | xii. Forensic Analytics |

9.15. Technical Specifications

Integrated Building Management System (iBMS)

Sr. No.	Specifications
A	<p>Solution for iBMS: Solution should provide a pre-integrated, centralized and consolidated platform for end to end management of a building, which includes Facility infrastructure (HVACs, LT Panel- AMF, DG, UPS, Fuel Tank, CCTV, Fire Alarm and suppression system). System should have the service dependency engine that allows to take intelligent decisions, as per the business needs/requirements. The tool should have the service oriented architecture layer and the mediation layer in a single plane. iBMS should be open for third party integration via (soap, xml, web service, snmp-v1, v2,v3). NO/NC ports (IO ports) and Modbus (TCP/IP&RTU) integration should be standard. For other industrial protocols, gateway integration should be available. Solution should perform the following general functions. Should be scalable with ready device certifications to accommodate new infrastructure getting added to the building</p>
1	<p>Visibility – It should get a single platform to manage the entire building and its components. The way ahead should be drilling down to the component, which is under performing / about to fail or has failed. The impact of the failed equipment on others should get highlighted. We should get a Hawkeye view to know, how are all the building components working at any point of time. So that issues are addressed as quickly as possible.</p>
2	<p>Capacity Planning - End equipment's in the building, should be set with thresholds to get an idea of how well they are rendering services to the people in the building. It should be able to proactively Identify potential area's which may need to be upgraded/downgraded (cooling, power, storage, etc.) with time. All MSI (end equipment vendors) SLA's and their respective maintenance contracts would be part of the OMS (operations and maintenance) plan.</p>
3	<p>Third Party Integration - Seamless Data Sharing to build a "Collaborative Decision Making System".</p>
4	<p>Salient Dependencies - Monitor & Control salient interdependencies between safety and security systems like: In case of fire, other than a fire alarm, we could get confirmatory information from the zonal camera. Multiple current surges in any particular zone should lead to an inspection of the electrical cables in the zone. Any sectional power failure, should help us to find the failure of the end equipment, by tracing down the LT panel SLD to the end equipment.</p>
5	<p>System with CMDB - Integrate people, process & technology. Decreasing the likelihood of downtime in the building by facilitating communication across all equipment's (part of the facility). A definite inventory management tool with a workflow system connecting responsible people, should be part of the solution.</p>
6	<p>Root-Cause Analysis - Isolate and pinpoint problem area before it impacts the building operations & business continuity while suppressing down the unwanted events.</p>
7	<p>Energy sources should always keep in check on the rated power consumption vs the power available for consumption. Since one of the big reasons for fire is higher load than the power distribution capability.</p>

8	System should be capable enough to store the raw data or as polled data, for at-least for 365 days. It should also have the facility to automate the backup process or allow to take manual backup, in case if it is required.
9	System should be capable of getting supported by the administrators at different levels. The system should provide individual and group rights and privileges. Normal users may have read access only, that too only to specific areas.
10	Support for email and SMS both (integration with SMS-gateway & GSM communication).
B	Energy Management
1	System should be capable of integrating with the mains (LT panel), DG, UPS, PDU, rectifier, energy meters for continuous monitoring of its health. The battery health of the UPS would also be needed.
2	System should be able to do continuously monitor the quality of power, supplied to the electricity board and by the Generators (PF, frequency, harmonics distortion etc.), to avoid downtime.
3	System should have the feature to setup thresholds on each of the monitored energy parameter.
4	System should be able to clearly provide load trend for each rack, if need be in the building which would enable setup practical thresholds to get alerted on overload situations, to avoid any breakdown.
C	Fire Alarm System Monitoring and Management
1	Should proactively alert in case of electrical fire (short circuit or over current)
2	System should have the capability to integrate with different makes of fire alarm systems in the DCs and provide alarms generated by system on Central Dashboard.
3	System should be able to plan and process a proper evacuation plan in case of fire
4	Trigger Audio and Visual alarm
5	Co-relate with the nearest camera in the site with the zone of the FAS.
6	Switching ON of lights on the evacuation pathway.
Sr. No.	Specifications
D	Centralized Reporting & Dashboard
1	Dashboard and reporting engine should provide centralized view for the entire infrastructure (physical security, safety & energy) in the building.
2	It should provide business users with highly interactive and power-users with highly sophisticated, pixel-perfect reports.
3	It should provide Web-based interactive reporting for business users, Rich graphical report designer for power users, Parameterized reports with powerful charting, Output in popular formats: HTML, CSV, PDF.
4	It should provide Analysis to explore data by multiple dimensions such as customer, product, network and time into the hands of business users.
5	It should provide Intuitive & rich graphic designer to create customized reports, such as: DC-PUE (enables to measure how much energy is getting consumed in IT and how much in DC

	infrastructure).
6	Solution should provide a comprehensive centralized dashboard for health monitoring of DC (Infrastructure) components like: Electrical Panels, PAC, UPS, DG, Fuel etc.)
E	DG Monitoring
1	Proposed system should be able to integrate with diesel generators for measuring fuel level and run hours of the DG. System should also allow monitoring of various alarms (like: LLOP, dg on, etc.) including quality of power of the DG.
2	System should be capable to do fuel level monitoring of diesel tanks installed for gensets in the DC/DR building, to have a proactive estimation of fuel availability.
3	<p>Parameters - Generator and Fuel Supply Automation</p> <ul style="list-style-type: none"> ▪ Mains Fail ▪ DG On ▪ DG Failed to start / DG Failed to stop ▪ DG Fuel Level Low ▪ High Water Temperature / High Coolant Temperature ▪ Low Battery Voltage ▪ Low Lube Oil Pressure(LLOP) ▪ Automate Fuel Supply Process to reduce fuel consumption cost.

Integrated Operation Platform (IOP)				
Sr. No.	Item	Minimum Requirement Description	Compliance (Yes / No)	Deviations / Remarks
IOP.001	General Requirements	IOP shall be open architecture based, highly scalable and able to integrate multiple disparate systems seamlessly on a common platform		
IOP.002	General Requirements	IOP system shall provide a real time Common Operating Picture (COP) of the area involving all agencies using a simple GUI		
IOP.003	General Requirements	<p>Some of incidents that IOP responds to include but are not limited to the following:</p> <ul style="list-style-type: none"> · Hazards / Calamities: Natural, Man-made, Environmental · Epidemics (Health) · Transportation (Road, Rail etc) · Public Utility (Water, Electricity, Street Lighting, Solid Waste Management) · Public Safety (Crime, Law & Order) 		
IOP.004	General Requirements	System shall integrate with various emergency response services such as Ambulance, Fire, Disaster Management Systems, etc.,		

IOP.005	General Requirements	System shall integrate with various social media applications such as Facebook, Twitter etc., and provide intelligent dashboard functions as required		
IOP.006	General Requirements	System shall support various sensors like Cameras, GPS, Voice devices (Analog & Digital), Storage devices, Sensor inputs from other applications/ systems		
IOP.007	General Requirements	System should provide tool to define/create any event/rule based Standard Operating Procedure (SoP) for decision making by optimizing the time to resolution for emergency and crisis situations		
IOP.008	General Requirements	IOP platform shall provide a dashboard functionality to manage workflows by integrating information from different agencies and systems to facilitate responsive decision making		
IOP.009	General Requirements	IOP platform should provide a cross-agency collaboration tool to support instant communication between various user groups and authorities via sms and email		
IOP.010	General Requirements	IOP platform should facilitate training mechanism		
IOP.011	Location Requirements	Platform shall have a GIS based map to provide the location detail		
IOP.012	Location Requirements	Multiple layer maps to be supported as required for various applications		
IOP.013	Location Requirements	GIS maps to comply OGC standards		
IOP.014	Location Requirements	Maps to support Drag & Drop functionality of various sensors at any given point of time		
IOP.015	Location Requirements	Map functionality to provide search options on basis of events, sensors, time etc.,		
IOP.016	Location Requirements	GIS to support addition/removal of sensors/ systems on need based		
IOP.017	Location Requirements	Map to support event based response actions for decision making in case of any emergency / critical situation		
IOP.018	Location Requirements	GIS based application to support Role based authentication for effective management of the system		
IOP.019	Realtime Requirements	CCTV feeds to be viewed on the Map in case of any event triggers		
IOP.020	Realtime Requirements	System to provide instant threat/event management based on the triggers generated		
IOP.021	Realtime Requirements	System shall provide view and availability of various systems/ sensors on the map at any given time		

IOP.022	Realtime Requirements	System shall facilitate communication between various agencies and personnel to address the situations		
IOP.023	Realtime Requirements	System shall support tracking of real time devices integrated		
IOP.024	Realtime Requirements	System shall trigger alerts for any of the sensors/ applications		
IOP.025	Incident Response	System shall facilitate setting the priority of the event and enable triggering the incidents automatically		
IOP.026	Incident Response	System shall allow setting up multiple triggering rules per incident type		
IOP.027	Incident Response	System shall enable associating response procedures to incident types. The associated procedures should be available for selection to operators upon manual incident creation.		
IOP.028	Post Incident Requirement	Shall have a recording mechanism that includes all the activities such as voice, telephony, Location, triggers etc., including the operator activities for analysis		
IOP.029	Post Incident Requirement	Shall have an event reconstruction functionality to give a complete overview of the synchronous events in the timeframe		
IOP.030	Post Incident Requirement	Shall provide a facility to export all the event scenario as a playable media file		
IOP.031	Post Incident Requirement	System shall support sorting and filtering the list of incidents		
IOP.032	Assets Management	System should present the operator with a logical tree that contains devices from different types		
IOP.033	Assets Management	System shall allow searching the device tree by device name or device type		
IOP.034	Assets Management	System shall indicate the device type by an icon		
IOP.035	Assets Management	System should display a pop-up for a device with its details		
IOP.036	Health Management	System should be able to monitor of both physical servers and system components (e.g. services, plug-ins) including CPU/Memory/Disk utilization and network connectivity performance		
IOP.037	Web Intelligence	System should have a tool for monitoring websites and social networks like twitter, facebook, google+, whatsapp (data for whatsapp shall be provided by GoUP) any publicly accessible web site for topics of interest over time from multiple sources in one platform.		
IOP.038	Web Intelligence	System should allow capability to analyse, corelate		

		and represent the subject-matter under investigation.		
IOP.039	Web Intelligence	System should periodically query web sites and should be able to log-in to the sites if needed, given proper credentials.		
IOP.040	Web Intelligence	System should allow Incoming data to be processed, analysed, filtered and matched against the defined requirements		
IOP.041	Web Intelligence			
IOP.042	Web Intelligence	It should allow all the data in the system to be accessible by role based mechanism		
IOP.043	Web Intelligence	System should support technology like BIG Data platform to enable easy search, filter and handle massive amounts of social data thereby transforming data to intelligence		
IOP.044	Web Intelligence	System should be used to integrate data from existing databases and data gathered from the web about entities like people, organizations, groups, concepts etc. as well as the relationships between them.		
IOP.045	Web Intelligence	Should provide notifications to multiple agencies and departments (on mobile) that a new intelligence has been gathered through open source/social media.		
IOP.046	Web Intelligence	System should have the capability of employing pre-existing knowledge (such as found in internal databases) as Ontology of the system, improving knowledge extraction and PIR (Priority Intelligence Requirements) matching across the board.		
IOP.047	Web Intelligence	System should be able to correlate the external data (structured and unstructured) with internal data from multiple internal databases and then should be able to initiate SOP. Should be able to identify the critical information and should be able to link it to an existing SOP or a new SOP should be started.		
IOP.048	Web Intelligence	System should be able to search across data from different silos, across many data types (new items, blog postings, people, tweets, and more)		

Video Wall for Command and Control Centre

Sr. No.	Item	Minimum Requirement Description	Compliance (Yes / No)	Deviations / Remarks
VWCCC.001	General	Video Wall and Controller from the same make is preferred		
VWCCC.	Video	26 Cubes (LED Based projection) -10X2 for Command Control		

002	wall	Centre -3X2 for Police Control Room		
VWCCC.003	Technology	Single chip DLP Technology		
VWCCC.004	Resolution	1920x1080		
VWCCC.005	Brightness	240 Cd/m ² or better		
VWCCC.006	On-screen contrast	1,200,000:1 (dynamic) or better		
VWCCC.007	Display technology	DLP rear projection with DMD Chip		
VWCCC.008	Colour gamut	>15 mill		
VWCCC.009	Brightness uniformity	>90% or better		
VWCCC.010	Screen	180° viewing angle screen		
VWCCC.011	Screen Gap	Less than 1 mm at ambient temperature in Control room		
VWCCC.012	Colour stability	Self-calibration with advanced colour sensor		
VWCCC.013	Dimensions	Diagonal: 50 "		
VWCCC.014	Light source	LED - 6x redundancy		
VWCCC.015	Light source	> 60,000h Typical usage mode		
VWCCC.016	lifetime	> 80,000h Economy usage mode		
VWCCC.017	Operating Conditions	10°C-40°C, 80% humidity (Non-Condensing)		
VWCCC.018	Input voltage	90 – 240 V, 50-60Hz		
VWCCC.019	Signal input/output	Single I link DVI in / Single link DVI out		
VWCCC.020	Direct Ethernet	IP control		

	access			
VWCCC.021	Graphical user interface	All settings and operational parameters		
VWCCC.022	Third party interface	Should be open to third party interface		
VWCCC.023	Warranty	5 years		

Video Wall Controller:

Sr. No.	Item	Minimum Requirement Description	Compliance (Yes / No)	Deviations / Remarks
VIWCO.001	Display controller	Controller to be able to control maximum number of inputs		
VIWCO.002	Redundant Controller	Controller should be based on the latest architecture.		
VIWCO.003	Platform	Windows 7 Professional (64 bit) or higher		
VIWCO.004	Processor & RAM	i7 with 3 GHz or higher processor & Minimum 16 GB		
VIWCO.005	Chassis Type	19" Rack mount industrial chassis		
VIWCO.006	Network	2 Network Ports		
VIWCO.007	Resolution Support	1920 x 1080 or higher		
VIWCO.008	RSS Feed	Controller should be able to show the RSS feed as required		
VIWCO.009	Ticker	There should be a possibility in the controller to create user defined multiple tickers. It should also be possible to place these tickers anywhere on the wall		
VIWCO.010	Scalability	System should be able to add additional inputs as required in the future		
VIWCO.011	Control	System should have capability of Monitoring & Control with various applications on different network through single Operator Workstation. It shall be possible to launch, change		

		layouts in real time using Tablet		
VIWCO.0 12	Fans	Chassis should have minimum 2 fans for adequate cooling		
VIWCO.0 13	Redundancy	Redundant Hot Swappable HDD in RAID 1 Configuration & Power Supply		
VIWCO.0 14	Keyboard & Mouse Extension	Keyboard and Mouse along with mechanism to extend them to 20 m operator desk from display controller to be provided		
VIWCO.0 15	24 x 7 operation	Controller shall be designed for 24 x 7 operation		
VIWCO.0 16	Others	Video Wall and the Controller should be of the same make to ensure better performance and compatibility		
VIWCO.0 17	OEM Certification	All features and functionality should be certified by the OEM. The Display Modules, Display Controller & Software should be from a single OEM.		
Video Wall Management Software				
Sr. No.	Item	Minimum Requirement Description	Compliance (Yes / No)	Deviations / Remarks
WMS.001	General Requirements	Software should be able pre configure various display layouts and access them at any time with a simple mouse click or based on timer		
WMS.002	General Requirements	Software should enable users to see desktop of graphics display wall remotely on any PC connected with Display Controller over the Ethernet and change the size and position of the various windows being shown.		
WMS.003	General Requirements	Wall management software shall be having interoperability with Video management system.		
WMS.004	General Requirements	Wall management software may be centrally Server based or local controller based architecture.		
WMS.005	General Requirements	Software should enable various operators to access the display wall from the local keyboard and mouse of their workstation connected with the Display Controller on the Ethernet		
WMS.006	General Requirements	Software should copy screen content of PC connected on the Ethernet with the Display Controller to be shown on the Display wall in scalable and moveable windows in real time		

		environment.		
WMS.007	General Requirements	Wall management software should enable system integrators to integrate it with their Software.		
WMS.008	General Requirements	Wall Control software shall perform health monitoring that allows timely detection of faults, a. Wall health, b. Cube health, c. Cube IP-address, d. Brightness		
WMS.009	General Requirements	Wall Control Software shall allow commands on wall level or cube level or a selection of cubes: a. Switching the entire display wall on or off. b. Fine-tune colour of each cube		
WMS.010	General Requirements	Log file functions		

Video Wall Management Software				
Sr. No.	Item	Minimum Requirement Description	Compliance (Yes / No)	Deviations / Remarks
WMS.011	Client & Server based Architecture	Should support Multiple clients / Consoles to control the Wall layouts		
WMS.012	Collaboration	Software should be able to share layouts comprising of multiple sources with workstations / Displays over LAN/WAN for remote monitoring		
WMS.013	Scaling	Software should enable user to display multiple sources (both local & remote) up to any size and anywhere on the display walls (both local & remote).		
WMS.014	Display	Software should be able to create layouts & launch them as and when desired		
WMS.015	Remote Control	Display Wall and sources (both local & remote) should be controlled from Remote PC through LAN without the use of KVM Hardware.		
WMS.016	Layout Management	Should support for Video, RGB, DVI, Internet Explorer, Desktop Application and Remote Desktop Monitoring Layouts		
WMS.017	Support of Meta Data	Software should support display of Alarms		
WMS.018	Authentication	Software should provide at least 2 layer of authentication		
WMS.019	Scenarios	Software should be able to save/load desktop layouts from Local/remote machines		
WMS.020	Layout	All the Layouts can be scheduled as per user convince.		

0	Scheduler			
WMS.02 1	Layout Scheduler	Software should support auto launch of Layouts according to specified time event by user		
WMS.02 2	User friendly	Software should be user friendly		
WMS.02 3	OEM Certification	All features and functionality should be certified by OEM. Display Modules, Display Controller & Software should be from a single OEM.		

Video Management System – VMS				
Sr. No.	Item	Minimum Requirement Description	Compliance (Yes / No)	Deviations / Remarks
VMS.0 01	General Requirements	VMS shall work on ONVIF Open Platform catering to all the security needs of the city		
VMS.0 02	General Requirements	VMS shall be open to any ONVIF IP cameras integration so that it would be able to cater future requirements of the project		
VMS.0 03	General Requirements	VMS shall support interoperability of IP cameras from multiple vendors		
VMS.0 04	General Requirements	MSI shall clearly mention in their proposal the brands and models integrated into VMS		
VMS.0 05	General Requirements	VMS system shall be compatible to single and multiple processor servers. The server processor & hardware shall be optimized in all cases.		
VMS.0 06	General Requirements	VMS system shall cluster the processing & memory load across several machines. The failure of any one server in the solution shall not cause a failure in the entire system.		
VMS.0 07	General Requirements	System shall allow the frame rate, bit rate and resolution of each camera to be configured independently for recording.		
VMS.0 08	General Requirements	System shall support H.265, H.264 and MJPEG compression formats for all IP cameras connected to the system.		
VMS.0 09	General Requirements	VMS shall support high availability of recording servers. A failover option shall provide standby support for recording servers with automatic synchronization to ensure maximum uptime & minimum risk of lost data.		
VMS.0 10	General Requirement	VMS software shall have multicast and multi-streaming support. It shall have the ability to take a snapshot from any		

	s	online live camera and export to a standard graphic file format.		
VMS.0 11	General Requirement s	VMS shall support archiving for optimizing recorded data storage through unique data storage solutions by combining performance and scalability with cost efficient long-term video storage.		
VMS.0 12	General Requirement s	Video Management System shall incorporate intuitive map functions allowing for multi layered map environment. The map functionality shall allow for the interactive control of the complete surveillance system, at-a-glance overview of system integrity, and seamless drag-and-drop integration with video wall module option.		
VMS.0 13	General Requirement s	System should support Maps integration with below features; i. Click on an indicator on the map and drill down to additional linked maps. ii. Zoom into the map iii. To “drag & drop” a camera or any other sensor from the map area to a video window or to click on a camera to start viewing it in a pop-up window. iv. Add cameras to the map images. v. The map supported formats shall be: BMP, GIF, JPG, PNG and TIFF		
VMS.0 14	General Requirement s	Video Management System shall incorporate fully integrated matrix functionality for distributed viewing of any camera in the system from any computer with the client viewer.		
VMS.0 15	General Requirement s	VMS shall be ONVIF compatible		
VMS.0 16	General Requirement s	VMS shall be scalable to support minimum 5000 or more cameras, which can be added into the system by only addition of software licenses and servers		
VMS.0 17	General Requirement s	It shall be possible to integrate VMS into the Command & Control system. In that respect bidders shall provide their SDK/API (or any other integration means) libraries and documentation to ensure a seamless integration with any other system.		
VMS.0 18	General Requirement s	VMS shall be open to any standard storage technologies integration.		
VMS.0 19	General Requirement s	VMS shall already support Storage system from multiple vendors.		
VMS.0 20	General Requirement	VMS shall provide the ability to save any event that was tagged as an alarm (video motion detection, video loss or		

	s	input) received, to be saved in a manner in which it cannot be overwritten.		
VMS.0 21	General Requirement s	VMS shall be open to any video wall system integration		
VMS.0 22	General Requirement s	VMS shall offer possibility to integrate external Video Analytics systems.		
VMS.0 23	Distributed Architecture	It shall be possible to access VMS without installing dedicated client software (e.g. through the use of common web browser such as Internet Explorer...)		
VMS.0 24	Distributed Architecture	VMS shall be designed to offer a full IP based distributed architecture		
VMS.0 25	Distributed Architecture	VMS shall have the capability to handle software clients (operators) connected in different locations on the same network.		
VMS.0 26	Distributed Architecture	Simultaneous quantity of operators per location shall not be limited		
VMS.0 27	Management	VMS shall store the system's configuration in a relational database, either on the management server computer or on the network.		
VMS.0 28	Management	VMS shall authenticate user access, user rights and privileges of all operators through Active Directory		
VMS.0 29	Management	Access rights and privileges shall consist in but not limited to a. Visibility of devices, live view, playback, AVI/ MP4 export, JPEG export, database export, sequences, smart search, input status, output control. b. PTZ control, PTZ priority, PTZ pre-set control c. Smart/Remote Client, live playback/setup, status API, service registration API and d Privileges for the map feature		
VMS.0 30	Management	Registration of the system shall allow for on line activation and off line activation of licenses		
VMS.0 31	Management	The system shall support automatic failover for Recording Servers. This functionality shall be accomplished by one Failover Server as a standby unit for max 10 servers that shall take over, if one of a group of designated Recording Servers fails. Recordings shall be synchronized back to the original Recording Server once it is back online		
VMS.0 32	Management	VMS shall operate in multicast / unicast / bandwidth throttling protocol to minimize the network bandwidth		
VMS.0 33	Multicasting	VMS shall support video streams up to at least 25fps		
VMS.0	Multicasting	Monitoring module shall allow for continuous monitoring of		

34		the operational status and event-triggered alarms from servers, cameras and other devices.		
VMS.0 35	Monitoring Module	The Monitoring module shall provide a real-time overview of alarm status or technical problems while allowing for immediate visual verification and troubleshooting.		
VMS.0 36	Monitoring Module	Module shall include flexible access rights and allow each user to be assigned several roles where each shall define access rights to cameras.		
VMS.0 37	Monitoring Module	Viewing live video from cameras on the surveillance system with Playback recordings from cameras on the surveillance system, with a selection of advanced navigation tools, including an intuitive timeline browser.		
VMS.0 38	Monitoring Module	The system shall allow views to be created which are only accessible to the user, or to groups of users based on different layouts optimized for 4:3 and 16:9 display ratios. It should be able to create and switch between an unlimited number of views and able to display video from up to 25 cameras from multiple servers at a time.		
VMS.0 39	VMS Storage	It shall be possible to schedule recording and archiving by a recurrence pattern (daily, weekly, specific time and dates) and by specific time ranges (all day, time range, daytime, night time)		
VMS.0 40	VMS Storage	It shall be possible to schedule recording on per camera basis (Continuous, manual or motion based)		
VMS.0 41	VMS Storage	VMS shall allow the control of the amount of used disk space.		
VMS.0 42	VMS Storage	It shall be possible to protect specific video streams against any deletion and for any time		
VMS.0 43	Log Management	system log shall be searchable by Level, Source and Event Type.		
VMS.0 44	Log Management	Alert Log records alerts triggered by rules (searchable by Alert type, Source, Event type)		
VMS.0 45	Management	system shall have smart recording wherein no recording or recording at lower frame rate is done when there is no movement. The VMS shall be able to record higher-quality video and shall reduce fps when not in use during VAS. night time.		
VMS.0 46	Management	System should support recording management to view the recordings available on a camera's local storage device (such as an SD card), and copy them to the server.		
VMS.0 47	Management			
VMS.0 48	Management	System should support Clip/Playback Management—Use Clip/Playback Management to view and download video files		

		that are stored on the server.		
VMS.0 49	Management	No of operators shall not be software licenses dependent. In case of emergency, threats, natural catastrophe the control room shall be able to reconfigure the VMS by adding more operators without any Contractor's intervention.		
VMS.0 50	Management	Security Platform shall have strong security mechanism such as the use of advance encryption, digital certificates and claims-based authentication to ensure that only authorized personnel have access to critical information, prevent man-in-the-middle attacks, and that the data is kept private.		

Video Content Analytics				
Sr. No.	Item	Minimum Requirement Description	Compliance (Yes / No)	Deviations / Remarks
VAS.001	General Requirements	System shall be a real-time video analytics engine that utilizes advanced image processing algorithms to turn video into actionable intelligence.		
VAS.002	General Requirements	System shall provide configurable detection zones and lines to detect events of interest, Detection zones define an area of interest and Detection lines define a perimeter instead of a region.		
VAS.003	General Requirements	System shall facilitate creating multiple zones and lines in a single scene to trigger various alerts		
VAS.004	General Requirements	System shall allow configuration of applicable rules and manage them.		
VAS.005	General Requirements	System shall also enable editing Zones and lines to desired shape or size.		
VAS.006	General Requirements	Triggers generated by the applied rules shall provide visual indicators to identify the event. Such as a yellow coloured target changing the colour to red on event		
VAS.007	General Requirements	System shall enable masking of areas which interfere detection zones in other areas of the scene		
VAS.008	General Requirements	System shall enable detecting rules in the defined areas (zones/ lines)		
VAS.009	General Requirements	System shall provide a functionality for configuring timelines for various events such as abandoned object, camera tampering etc		
VAS.010	General Requirements	System shall be able to filter large amounts of video and focus on human attention appropriately		
VAS.011	General Requirements	System shall have Automated PTZ camera control/preset for zooming in on interesting events like motion Detection etc.		

		as picked up by Camera without the need for human intervention.		
VAS. 012	General Requirements	VCA shall provide secured feeds with encryption for data authenticity		
VAS. 013	General Requirements	VCA shall be able to, vehicle parked in defined zones etc.,		
VAS. 014	General Requirements	System shall have a report generation functionality to provide inputs on various instances of events triggered in the system		
VAS. 015	General Requirements	VCA should allow to add, edit, delete or disable and enable Policies.		
VAS. 016	Features	Definable and available triggers should be for citywide surveillance, system needs to have capability to deploy intelligent video analytics software on any of selected cameras. Software should have capability to provide various alarms & triggers. solution should offer following triggers:		
		1) Parking Violation		
		2) Wrong Direction		
		3) People loitering		
		4) Camera Tampering (In case this is an inherent feature of the camera, this may not be provided as a separate line item in VA)		
		5) Unattended Object		
		6) Crowd detection		
		7) Attribute Based Search		
		a. Track a specific person across several surveillance cameras. The application shall allow access to all relevant associated VMS recordings with following		
		b. Search initiators:		
		o VMS recorded content;		
		o Photographic images i.e. System shall also provide the option to initiate such search just by clicking on the image of a human during video playback;		
		o Artificial sketch builder allowing selection of various attributes i.e. body color, body figure, Hair styles, Texture and color of cloths, various accessories i.e. Spectacles, Shoes, bag/suitcase, Tie etc.		
		c. When initiating a query by VMS recorded content, the operator shall be able to		

		initiate the query for a specific VMS video channel and time range in order to get results of extracted individual's thumbnails from the image database that was generated in real-time by the analytics application.		
		d. The application shall support a list of at least 20 different textures types.		
		e. The application shall support map images and GIS maps.		
		The application users shall be integrated with the VMS users and user privileges shall be derived from the VMS.		
VAS. 017	General Requirements	Motion Detection component that automatically detects moving objects in the field of view of a camera & is capable of filtering movement in configurable directions & movement due to camera motion (e.g. from wind)		
VAS. 018	General Requirements	System shall have a sophisticated rule-based engine with powerful analytics capabilities that provides automatic event notification,		
VAS. 019	Log Management	System should have a proper MIS system for recording of various video analytics as per need. There should be provisions for acknowledging the events with remarks in the system itself & print out of a period specific list can be taken for recording purpose.		

IP Telephony - Core Telephony System:				
Sr. No.	Item	Minimum Requirement Description	Compliance (Yes / No)	Deviations / Remarks
IPTCS.001	Converged communication	Converged communication System with ability to run BRI/PRI, IP on the same platform using same software.		
IPTCS.002	Centralized database	System should have capability to manage centralize database of all the users. CLI facility for all users should be provisioned from day one. System should support centralized web based administration.		
IPTCS.003	Protocol	System should support SIP Protocol and SIP based end points/IP Phones.		
IPTCS.004	Login	System should allow users to log in from any IP Phone using his username and password and it will transfer all his existing facilities to that IP phone.		
IPTCS.005	Architecture	System should be based on server gateway		

		architecture to facilitate distributed architecture with central call control. The external server should be on Open Source / Linux operating system.		
IPTCS.006	Call control system	voice network architecture and call control functionality should support all types of IP phone Call control system should be fully redundant solution and should provide 1:1 redundancy. The solution must provide geographical redundancy by separating call control servers over LAN and WAN.		
IPTCS.007	Standby configuration	Support active – active / active – standby configuration. The interruption-free switchover from active to standby control must take place without existing two-way voice connections being interrupted including Failure of Fibre Optic Cable, call control server, etc.		
IPTCS.008	Software version	System software version offered should be latest release as on date of supply of IPPBX as available globally.		
IPTCS.009	IPv6	Solution should be implemented on IPv6.		
IPTCS.010	Call Admission Control	System should support Call Admission Control.		
IPTCS.011	Web based administration	Solution should have inbuilt as well as web based administration for call processing/call control. Should also support HTTPS for management.		
IPTCS.012	Alerts	Solution should provide alert notifications for troubleshooting performance.		
IPTCS.013	Troubleshooting	Solution should support secure GUI / CLI (HTTPS and TCP) to troubleshoot system		
IPTCS.014	Monitoring	Solution should allow monitoring of system in real-time on a set of preconfigured parameters. Solution should provide management tool to monitor system performance, device status, device discovery, etc		
IPTCS.015	Role based access	Management platforms should allow configuration of role based access of the system to multiple users like administrator etc. it should also allow to set the authority and their rights in the system.		
IPTCS.016	BHCC/BHCA Rate	role based access should be capable to have =>2,00,000 BHCC/BHCA Rate.		
IPTCS.017	Signalling encryption	Solution should support signalling encryption by Transport Layer Security (TLS) and media encryption using Secure Real-Time Transport Protocol (SRTP)		

IPTCS.019	Broadcasting	Solution should allow Broadcasting of voice, text messages using XML based application to one to many (minimum 40 or more) on desk phone/ IP phone.		
IPTCS.020	Voice and video facility	Solution should support voice and video facility for all. However, video facility will be enabled for selective users only.		
IPTCS.021	Voice Gateway	<ul style="list-style-type: none"> ▪ Voice Gateway should be distributed at 2 locations: Location-1 should have minimum 20 PRI physical ports & Location-2 should have minimum 10 PRI physical ports ▪ Voice gateway should have internal redundant power supply and should support for E1, QSIG, PRI, etc. ▪ Voice gateway should support SIP Trunk from day one. ▪ Voice gateway should have adequate number of DSP channels to support non-blocking architecture. ▪ Voice gateway should be provided with Dual Ethernet Port for redundancy. 		
IPTCS.022	Multiple Device Configuration	User should be allowed to configure his multiple communication devices like desk phone, mobile, laptop, desktop on a single extension number. It should also allow transfer/resume of ongoing audio and video call from one device to another configured device seamlessly. Solution should allow user wise enablement/configuration of STD, ISD facility.		
IPTCS.023	System Architecture	<ul style="list-style-type: none"> ▪ Server should be with Latest processor based architecture. ▪ Server and Gateway should not be in the same Unit sharing the same Active ▪ Backplane/ Motherboard (to prevent total failure of entire system during Motherboard failure) ▪ Server must have remote-access capability over standard PSTN / IP networks for maintenance. ▪ Support security features like Real-time Media Encryption, Malicious Call Trace, etc. ▪ 128-bit encryption of voice between servers and gateways 		
IPTCS.024	Partitioning	Solution must support logical / tenant partitioning.		

		Ensure that Logical Partitioning implemented properly in the new solution, so that the toll bypass does not happen and deployed solution meets government regulations		
IPTCS.025	System Features:	Call Diverting, Call Bridging, Call waiting, Call log on IP Phone Call Conference, Click to Dial, Auto Call Forwarding, Speaker facility, Speed dial feature, Recorded Announcement, Authorization Code, Boss secretary feature support, Direct Inward Dialling, Direct Outward Dialling, Music on Hold (Programmable), Authorization code based long distance dialling, Abbreviated Dial, Calling line identification, Calling party name identification, Station Volume controls, call Transfer, Hunt Groups, Dial Plan Partitioning, Hotline, Different/distinctive Ringing tone, extension Mobility or equivalent, Automatic Route Selection, Least Cost Routing, Alternate Route Selection, Movable Extension Number, Uniform & Flexible Numbering Plan-up to 6 Digit, Message-waiting indicator (MWI), External outgoing, Parallel ringing, Add-on conference, call park and pickup, Speed Dial, call back (busy, no reply, etc.), Multiple line appearances per phone, call status per line, Auto Call Disconnection, on hook dialling, Hands free calling, Class of Restriction, Integrated announcement.		
IPTCS.026	Integration:	<ul style="list-style-type: none"> ▪ MSI shall be responsible for publishing necessary/required APIs in REST 2.0 and JSON formats for integration (Back and forth) for of proposed solution and facilitating integration activity with Active Directory & Microsoft outlook extension ▪ Publishing necessary/required API plug-in for other e-Governance applications which should allow features such as Click to call, Audio & video calls from the application itself. 		
IPTCS.027	Soft Agent/Client:	<ul style="list-style-type: none"> ▪ Solution should provide voice & video calling through PC/Desktop, laptop, mobile users with soft clients/agent. ▪ Solution should allow calling from web, PC/Desktop, laptop, Mobile. For PC, mobile ▪ Provide mobile app/client for logging. ▪ soft client should be available on various 		

		<p>operating systems like Windows (for Desktop/Laptop is should support Windows 7 onwards), Mac, iOS and android (for Mobile client should support at least 80% user coverage).</p> <ul style="list-style-type: none"> ▪ Desktop Client should have soft phone capability & support video calls with HD 720p capability. ▪ Support single sign on (SSO) functionality. ▪ Dial pad and other basic feature keys for ease of operation. ▪ Common supported status should be available, busy, idle, away etc. ▪ Provide SSH and HTTPS access to management platform for enhanced security. 		
IPTCS.028	Conferencing:	<ul style="list-style-type: none"> ▪ Support one to one, one to many audio and video conferencing facility. ▪ Allow addition, dropping of users during the conferencing. ▪ Allow users to join on going, scheduled video conference call as an audio participant support voice conferencing between internal users to external party. ▪ support at least audio codecs G.711, G.729, G.722 and video codecs H.264/ H.265. ▪ Lock / Password protected meeting to prevent unauthorized participant joining session. ▪ Allow share/Transfer of document (presentations, reports, desktop based applications etc.) using soft client/agent during the VC. 		

IP Telephony - Video IP Phone Device				
Sr. No.	Item	Minimum Requirement Description	Compliance (Yes / No)	Deviations / Remarks
IPVID.001	Display	7" capacitive touchscreen, 1280 x 800 WXGA resolution		
IPVID.002	Audio	Wideband audio through handset, headset and speakerphone, Full-duplex speakerphone		
IPVID.003	Video	Full HD 1080p HD video, Video displayed on built-in 7" touchscreen or on external monitor, External monitor output provides simultaneous display of video conferencing and PC (via HDMI in) with Picture-in-Picture support, Variable window size / position		

IPVID.004	Camera	1080p30fps resolution, Detachable, f2.0 lens for superior low light performance, Field of View (H) up to 70°, Focus range from 40 cm (15.7") to 3 m (9.8'), Privacy shutter, Manual tilt for optimal eye level positioning, Integrated or external display mount, Activity LED		
IPVID.005	Handset	DECT 6.0 cordless handset with answer, volume, and mute controls, Optional wired handset		
IPVID.006	Physical Buttons & Status Indicators	Dial pad, Volume up/down, Audio mute with LED status, Camera block with LED status, Speakerphone with LED status, Headset with LED status, Incoming call / message waiting LED status, Capacitive touch buttons with LED status for home, contacts, communication app, call history and back/previous		
IPVID.007	Connectors / Ports	RJ45 Gigabit Ethernet PoE LAN, RJ45 Gigabit Ethernet PC, USB dedicated camera, USB 2.0 for high-powered charging (up to 1.5 A), USB 2.0 for headset, keyboard, mouse, USB 2.0 Micro AB, HDMI out for external monitor, HDMI in for PC input, RJ9 analog handset, RJ9 analog headset, 48 V AC power supply, microSD card slot (future support)		
IPVID.008	Physical Security	Kensington security slot		
IPVID.009	Storage	8 GB eMMC flash memory		
IPVID.010	Memory	2 GB RAM		
IPVID.011	Power	802.3af SPPoE, 15.4 W, 802.3at PoE, 25.5 W, 110-220 V AC, 50-60 Hz, 30 W		
IPVID.012	Environmental	Operating temperature: 0°C to 40°C (32°F to 104°F), Relative humidity: 10% to 90% non-condensing		
IPVID.013	Connectivity	Latest version Ethernet, Wi-Fi & Bluetooth		
IPVID.014	Network Protocols	SIP, DHCP, DNS, LLDP, UDP, TCP, TLS, HTTP/HTTPS, RTP/SRTP, RTCP/SRTCP, NTP, 802.1x, VLAN, 802.1p Layer 2 QoS, DSCP Layer 3 QoS		
IPVID.015	Security	Wired network, 802.1x EAP-TLS, Wi Fi network, WEP, WPA/WPA2 PSK, EAP-PEAP (MSCHAPV2, GTC), EAP-TLS, EAP-TTLS (MSCHAP, MSCHAPV2, GTC), EAP-PWD, Data Encryption, HTTPS file download, Exchange ActiveSync with HTTPS, HTTPS browser support, Aura SIP AES-256 encryption, Secure remote SIP connectivity		

IP Telephony - Voice IP Phone device				
Sr. No.	Item	Minimum Requirement Description	Compliance (Yes/No)	Deviations / Remarks
IPVO.001	Display	64 x 128 pixel, black & white, white backlight		
IPVO.002	Keypad	Navigator: 4 way navigation + OK + Cancel, Function Keys: On/Off hook, Dial Pad, mute with Led, volume keys +/-, hands-free with Led, 2 personal Keys/Led, redial, info & message with LED, Alphabetic Keyboard, programmable keys with Led, Paper Label & soft keys		
IPVO.003	Connectivity	RJ-45 LAN: Gigabit Ethernet 10/100/1000, RJ-45 PC through 10/100/1000 Gigabit Ethernet Switch, RJ-9 connector for corded handset, RJ-9 connector for Alphabetic Keyboard, Dedicated 3,5 mm jack headset port, RJ-11 connector for external ringer & audio active envelop indicator, 2 mm Jack Plug for external AC/DC power adapter, SATA connector for Add-on module connection,		
IPVO.004	Power	Power over Ethernet Class 2, Optional Transformer: 100 V AC to 240 V AC/48 V DC		
IPVO.005	Audio	Comfort Handset, Hearing Aid Compatible, Full-duplex speakerphone, Acoustic echo cancellation, Wideband, Voice Activity Detection, comfort noise generation		
IPVO.006	Network	DHCP & static IP – Manual/dynamic host configuration protocol (DHCP) network setup QoS support - Q tagging (VLAN), Layer 3, TOS, DSCP, and QoS Tickets AB/LLDP-MED client (automatic VLAN acquisition, PoE management, inventory information) Energy Efficient Ethernet support		
IPVO.007	Security	Authentication: Message Digest 5 (MD5)/TLS: For authentication, customer certificates management (with centralized deployment), Denial of service (DoS) attack protection: Flooding, ARP Spoofing protection Transport: TLS 1.2/1.0 and SRTP - Encryption and authentication of the signalling traffic; Encryption of media traffic.		
IPVO.008	Languages	Multi-language support menu for use in Uttar Pradesh, India		
IPVO.009	Environmental Conditions	Operating Temperature: -5°C to +45°C, Relative humidity: 5% to 95%, Storage/Transportation Temperature: -25°C/+70°C, IEC 60529 (IP Class: IP 22)		

Monitoring Workstations/Desktop:				
Sr. No.	Item	Minimum Requirement Description	Compliance (Yes / No)	Deviations / Remarks
MONW.001	Processor	Latest generation 64bit X86 Quad core processor(3Ghz) or better		
MONW.002	Chipset	Latest series 64bit Chipset		
MONW.003	Motherboard	OEM Motherboard		
MONW.004	RAM	Minimum 8 GB DDR3 ECC Memory @ 1600 Mhz. Slots should be free for future upgrade. Minimum 4 DIMM slots, supporting up to 32GB ECC		
MONW.005	Graphics card	Minimum Graphics card with 2 GB video memory (non- shared)		
MONW.006	HDD	2 TB SATA-3 Hard drive @7200 rpm with Flash Cache of 64GB SSD. Provision for installing 4 more drives.		
MONW.007	Media Drive	NO CD / DVD Drive		
MONW.008	Network interface	10/100/1000 Mbps autosensing on board integrated RJ-45 Ethernet port.		
MONW.009	Audio	Line/Mic IN, Line-out/Spr Out (3.5 mm)		
MONW.010	Ports	Minimum 6 USB ports (out of that 2 in front)		
MONW.011	Keyboard	104 keys minimum OEM keyboard		
MONW.012	Mouse	2 button optical scroll mouse (USB)		
MONW.013	PTZ joystick controller (with 2 workstations in CCC)	<ul style="list-style-type: none"> ▪ 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 		
MONW.014	Monitor	22" TFT LED monitor, Minimum 1920 x1080 resolution, 5 ms or better response time, TCO 05 (or higher) certified		
MONW.015	Certification	Energy star 5.0/BEE star certified		
MONW.016	Operating System	64 bit pre-loaded OS with recovery disc		
MONW.017	Security	BIOS controlled electro-mechanical internal chassis		

7		lock for the system.		
MONW.01 8	Antivirus feature	Advanced antivirus, antispysware, desktop firewall, intrusion prevention (comprising of a single, deployable agent) which can be managed by a central server. (Support, updates, patches and errata for the entire contract/ project period)		
MONW.01 9	Power supply	SMPS; Minimum 400-watt Continuous Power Supply with Full ranging input and APFC. Power supply should be 90% efficient with EPEAT Gold certification for the system.		

Network Laser Colour Printer:

Sr. No.	Item	Minimum Requirement Description	Compliance (Yes / No)	Deviations / Remarks
NLCP.001	Print Speed	Black: 15 ppm or above on A3, 24 ppm or above on A4 Colour: 8 ppm or above on A3, 12 ppm or above on A4		
NLCP.002	Resolution	600 X 600 DPI		
NLCP.003	Memory	Min. 8 MB or more		
NLCP.004	Paper Size	A3, A4, Legal, Letter, Executive, custom sizes		
NLCP.005	Paper Capacity	250 sheets or above on standard input tray, 100 Sheet or above on Output Tray		
NLCP.006	Duty Cycle	25,000 sheets or better per month		
NLCP.007	OS Support	Linux, Windows 2000, Vista, 7, 8, 8.1		
NLCP.008	Interface	Ethernet Interface		

Fixed Dome Camera for Indoor Surveillance:

Sr. No.	Item	Minimum Requirement Description	Compliance (Yes / No)	Deviations / Remarks
FDCIS.00 1	Video Compression	H.264		
FDCIS.00 2	Video Resolution	1920x1080		
FDCIS.00 3	Frame rate	25 fps in all resolutions		
FDCIS.00 4	Image Sensor	1/4" / 1/3" Progressive Scan CMOS		
FDCIS.00 5	Lens Type	Varifocal, C/CS Mount, IR Correction		
FDCIS.00 6	Lens	Fixed IRIS 2.8-10mm, F1.7, 10x digital zoom		
FDCIS.00	Minimum	0.9 lux		

7	Illumination			
FDCIS.008	Image settings	Compression, colour, brightness, sharpness, contrast, white balance, exposure control, backlight compensation, rotation		
FDCIS.009	Protocol	HTTP, HTTPS, FTP, SMTP, RTSP, RTP, TCP, UDP, RTCP, DHCP, UPnP, QoS, IPV4, IPV6		
FDCIS.010	Security	Password Protection, IP Address filtering, User Access Log		
FDCIS.011	Operating conditions	0 to 50°C		
FDCIS.012	Casing	Tamper Resistant casing for Indoor Environment		

KVM Module:				
Sr. No.	Item	Minimum Requirement Description	Compliance (Yes / No)	Deviations / Remarks
KVMM.001	KVM Requirement	Keyboard, Video Display Unit and Mouse Unit (KVM) for the IT Infrastructure Management at Data Centre		
KVMM.002	Form Factor	19" rack mountable		
KVMM.003	Ports	minimum 8 ports		
KVMM.004	Server Connections	It should support both USB and PS/2 connections.		
KVMM.005	Auto-Scan	It should be capable to auto scan servers		
KVMM.006	Rack Access	It should support local user port for rack access		
KVMM.007	SNMP	The KVM switch should be SNMP enabled. It should be operable from remote locations		
KVMM.008	OS Support	It should support multiple operating system		
KVMM.009	Power Supply	It should have dual power with failover and built-in surge protection		
KVMM.010	Multi-User support	It should support multi-user access and collaboration		

Online UPS:				
Sr. No.	Item	Minimum Requirement Description	Compliance (Yes / No)	Deviations / Remarks
ONUPS.0	Capacity	Adequate capacity to cover all above IT Components		

01		at respective location		
ONUPS.0 02	Output Wave Form	Pure Sine wave		
ONUPS.0 03	Input Power Factor at Full Load	>0.90		
ONUPS.0 04	Input	Three Phase 3 Wire for over 5 KVA		
ONUPS.0 05	Input Voltage Range	305-475VAC at Full Load		
ONUPS.0 06	Input Frequency	50Hz +/- 3 Hz		
ONUPS.0 07	Output Voltage	400V AC, Three Phase for over 5 KVA UPS		
ONUPS.0 08	Output Frequency	50Hz+/- 0.5% (Free running); +/- 3% (Sync. Mode)		
ONUPS.0 09	Inverter efficiency	>90%		
ONUPS.0 10	Over All AC- AC Efficiency	>85%		
ONUPS.0 11	UPS shutdown	UPS should shutdown with an alarm and indication on following conditions 1) Output over voltage, 2) Output under voltage, 3) Battery low, 4) Inverter overload, 5) Over temperature, 6) Output short		
ONUPS.0 12	Battery Backup	30 minutes in full load		
ONUPS.0 13	Battery	VRLA (Valve Regulated Lead Acid) SMF (Sealed Maintenance Free) Battery		
ONUPS.0 14	Indicators & Metering	Indicators for AC Mains, Load on Battery, Fault, Load Level, Battery Low Warning, Inverter On, UPS on Bypass, Overload, etc. Metering for Input Voltage, Output Voltage and frequency, battery voltage, output current etc.		
ONUPS.0 15	Audio Alarm	Battery low, Mains Failure, Over temperature, Inverter overload, Fault etc.		
ONUPS.0 16	Cabinet	Rack / Tower type		
ONUPS.0 17	Operating Temp	0 to 50 degrees centigrade		
ONUPS.0 18	Managemen t Protocol	SNMP Support through TCP/IP		

DG Set:				
Sr. No.	Item	Minimum Requirement Description	Compliance (Yes / No)	Deviations / Remarks
DGS.001	General Specifications	<ul style="list-style-type: none"> ▪ Auto Starting DG Set mounted on a common base 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 		
DGS.002	Engine	Radiator cooled, multi cylinder, 1500 RPM diesel engine, with electronic/manual governor and electrical starting arrangement complete with battery, conforming to BS5514/ ISO 3046/ IS 10002		
DGS.003	Fuel	High Speed Diesel (HSD)		
DGS.004	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.		
DGS.005	AMF (Auto Main Failure) Panel	<p>AMF Panel fitted inside the enclosure, with the following: It should have the following meters/indicators</p> <ul style="list-style-type: none"> ▪ Incoming and outgoing voltage / Current in all phases ▪ Frequency, KVA and power factor ▪ Time indication for hours/minutes of operation ▪ Fuel Level in fuel tank, low fuel indication ▪ Emergency Stop button ▪ 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 		
DGS.006	Acoustic Enclosure	<ul style="list-style-type: none"> ▪ 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). ▪ Enclosure must be weather resistant powder coated, with insulation designed to meet latest MOEF/CPCB norms for DG sets, capable to withstand Hyderabad climate. The enclosure must have ventilation system, doors for easy access for maintenance, secure locking arrangement, complete and 		
DGS.007	Fuel Tank Capacity	It should be sufficient & suitable for containing fuel for minimum 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.		
--	--	--	--	--

Structured Cabling Components:				
Sr. No.	Item	Minimum Requirement Description	Compliance (Yes / No)	Deviations / Remarks
SCC.001	Standards	ANSI TIA 568 C for all structured cabling components		
SCC.002	OEM Warranty	OEM Certification and Warranty of 15-20 years as per OEM standards		
SCC.003	Certification	UL Listed and Verified		

Electrical cabling component:				
Sr. No.	Item	Minimum Requirement Description	Compliance (Yes / No)	Deviations / Remarks
ECC.001	Standards	All electrical components shall be design manufactured and tested in accordance with relevant Indian standards IEC's		

10. Cyber Security Requirement – Smart City Framework

As per the letter issued by National Security Council Secretarial, New Delhi, it is mandated to follow norms and regulations of Cyber Security for Smart City Model Framework. A bidder must provide compliance to each of the below mentioned points:

1. The generic architecture of smart city generally consists of four layers- a sensing layer a communication layer a data layer and application layer, and these four layers are overseen by the smart city security system, Architecture of information Technology systems deployed in Smart city need to be open interoperable and scalable.
2. The reference architecture of information Technology (IT) infrastructure in Smart city suggested by National Institute of Standards and Technology (NIST) serves as a common starting point for system planning while promoting interoperable functional building blocks, which are required in a smart city.
3. The message exchange between various applications in the smart city should be fully encrypted and authenticated. Any application outside the Data Center (DC) should talk to the application hosted in the datacenter through only predefined APIs.
4. While it is necessary to converge multiple infrastructure into one Central platform for ease of management it is mandatory that such applications hosted in the central data centre support tenancy with adequate authentication and role based access control mechanism for each tenant pertaining to their respective infrastructure.
5. In multi-tenant architecture there should be provision for flow of normalized data only to respective tenant partition (s) in a predefined manner with adequate authentication and encryption mechanism.
6. The Smart city architecture should be capable of managing heterogeneous data which would be continuously communicated through numbers devices following different protocols, in order to ensure that the flow of data between devices does not run into latency issues, appropriate protocols need to be deployed so as to minimize latency. The following communication protocols could be used for the different layers for data flow.
7. Between applications and back end system, HTTP, SQL, FTP, SNMP, SOAP, XML, SSH, SMTP, Between back end systems and field devices message Queue Telemetry Transport (MQTT)XMPP, RESTful HTTP Constrained Applications protocol (CoAP) SNMP, IPV4/6, BACnet LON works Low power Wide Area Network (Lora) Fixed, 4G/5G Wi-fi Wimax, 2G/3G from field devices, Zigbee Olp, ETSI LTN IPV4/6,6 LowPAN ModBus Wi-fi-802, 15.4 enOcean LoRA, RFID NFC Bluetooth, Dash7 Fixed ISM & Short range banks
8. Data Layer (Termed as city Digital platform/fabric) should be capable of communicating with various types of sensors/ device and their management platforms/applications for single /multiple services irrespective of software and application they support. Data exchange between various sensors and their management applications must strictly happen through this layer. Thus making it one true source of data abstraction, normalization correlation and enable further analysis on the same adequate security checks and mechanisms as described in later points to be deployed to protect data layer from data confidentiality Breach and unauthorized access.
9. The entire information Technology (IT) infrastructure deployed as part of Smart city should follow standards like ISO- 27001, ISO- 22301, ISO 37120, ISO 3712, ISO 27017, ISO 27018, BSIS

- PASS 180 BSI PAS 181, BSI PAS 182 for Wi-Fi access – PEAP(Protected Extensible Authentication Protocol), 3rd Generation Partnership Project (3GPP) Etc, As appropriate.
10. Application Program interfaces (APIs) should be published and the IT System be running on standard protocols like JSON/XML or REST etc.
 11. 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 system to generate false alarms of sabotage the system.
 12. Wireless broadband plan and architecture for the specific city may be prepared detailing the existing fiber system and other supporting infrastructure so as appropriately interfacing another or citywide wireless network.
 13. All sensors deployed as part of IT and IT based system in the Smart Cities should talk only to the authorized wireless network and do not hook on to the rogue networks the guidelines to secure Wi-Fi network as published by Department of Telecom must be followed
 14. 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.
 15. All traffic from the sensors in the Smart city to the application servers should be encrypted Secure Socket Layer (SSL) and authenticated prior to sending any information. The data at rest and in Transit must be encrypted.
 16. Authentication of sensors in the Smart City Should happen at the time provisioning the sensors and adding them into the system and should be based on physical characteristics' of the sensors like MAC ID, Device ID etc.
 17. Sensors deployed in solution to set up Smart City Should be hardened device with the ability to be upgraded remotely for firmware through encrypted image files.
 18. As various use multiple protocols to communicate with the underlying network with varied security capability the system allows provisioning necessary. Authentication and encryption sat the gateway or the nearest data aggregation level if the sensor is notable to do the same.
 19. The Sensors or edge device deployed in Smart city should not have any physical interface for administration Monitoring of system and networks should be undertaken remotely.
 20. The sensors deployed in Smart City should be of low power consumption and should work on self-sufficient power sources.
 21. All devices and system deployed in Smart City should be hardened and have the ability to be upgraded remotely for firmware through encrypted image files with authentication mechanism to complete the operation.
 22. All the sensors in the Smart city should connect to a completely separate network.
 23. The Data center should be segmented into multiple zones with each zone having a dedicated functionality e.g. all sensors for one operational domain can connect to the data center in one zone, and the internet facing side of the data center should be in another zone.
 24. The Internet facing part of the data center should have a Demilitarized zone where all the customers' application servers would be located that are customers facing. Only these serves can assess the data from the actual utility applications servers on predefined ports.

25. The Customer application servers should be accessed only by the web server that is hosted in a different zone of the data center.
26. The following should be implemented in the data Centre – Firewalls, Intrusion detection & intrusion prevention system, Web Application Firewalls, Behavioral Analysis system for anomaly detection, correlation engine, Denial of Service prevention device, Advanced persistent Threat Notification mechanism, federated identity and access management system etc.
27. Security information and Event Management (SIEM) monitoring on all smart city Networks devices and sensors to identify malicious traffic.
28. All application and apps will undergo static and dynamic security testing before deployment and be tested with respect to security on a regular basis at least once in a year.
29. All applications and Apps deployed as part of Smart city be hosted in India.
30. The said architecture provide.
31. Automatic and secure updates of software and firmware etc
32. All system and devices should provide auditing and logging capabilities
33. Ensure vendor Compliance to remove any backdoors, undocumented and hard cored accounts.
34. End to End solution should be provided with annual end to end service availability of 99,999 percent. The end to end service agreement should be in place for minimum period of five years from the data or operation of the systems.
35. Appropriate terms may be set up to monitor cyber incidents and mitigation of same.
36. All the information on incidents be shared regularly with Indian computer Emergency response Team (CERT-in) and ICIIPC (National Critical information Infrastructure Protection Centre) and take help to mitigate and recover from the incidents.

11. Testing and Acceptance Procedures

Testing and quality assurance in software development is more rigorous since each component has to be more reliable, if it is to be reused. A system is tested at various stages of development and deployment. For example, each component is tested as a unit for checking the correctness of its own code. The component shall be tested with its dependent components. After final release of the entire set of components, system is tested for the correctness of system functionality. The components shall be tested in simulated production load for performance and load analysis. The MSI along with consortium partners shall be responsible for the testing processes such as **planning** (includes preparing test plans and defining roles and their responsibilities), **preparation** (consists of preparing test specification, test environment and test data) and **execution** (includes testing at various levels like unit level, integration level, system level and production).

11.1. Test Plan

Test plans are prepared for each phase of testing. The initial test plan is created during the Project Planning phase. The initial test plan describes who performs which type of testing and when. Ideally master test plan covers all types of test i.e. from unit testing to production testing. The MSI along with consortium partners is expected to submit the test plans to ASCL for approval. Any changes made to the test plan during the project life cycle should be communicated to ASCL for approval.

Test plans should contain following items:

- Roles and responsibilities of test team
- Approach to testing
- Function testing
- Security testing
- User Interface and reports testing
- Concurrency testing
- Performance and Load testing
- Test Scenarios along with entry and exit criteria
- Test specifications
- Suspension and resumption criteria

11.2. Test scenarios

The MSI along with consortium partners should prepare test scenario for each business scenario. A test scenario when executed should fulfil a business requirement as per the scope of business functionality. Test scenarios shall include following:

- Test Specification - During the test specification phase, the test cases are specified. It consists of description of the input, process to be executed and a prediction of output results.
- Test Environment - Component developer does unit testing and integration testing. Integration testing can be delegated to a specialized testing group. Each of the members in the testing group is provided with testing environment according to his/her role and responsibilities. Following is sample testing environment for testing:
 - A workstation

- A set of tools and applications required on workstation like access to user interface, browser etc.
- Access to centralized document database (where all the project related documents are maintained)
- Access to testing tools and defect logging tools
- Access to the central database or repository for development and unit testing (this database contains sample test data)
- Access to deployed components
- Test Data - Test data is prepared for testing at each stage. The test data should be prepared in such a way that it covers basic path and every alternate path of the code. The basic path and alternate paths are prioritized to capture relevant data. Tools can also be used to generate test data.

11.3. Test Execution

The following testing steps are usually employed in the project lifecycle. The MSI along with consortium partners expected to follow these steps.

Unit Testing: In unit testing, each piece of code has to be rigorously tested. At this stage testing is done according to the priority of path of code. All the test results are logged in the defect logging tools. After completion of testing, code is corrected for defect logs. This process is iterative till criteria for successful testing is reached.

Integration Testing: Upon completion of unit testing, integration testing begins. The purpose is to ensure distinct components of the application still work in accordance to customer requirements. Test sets will be developed with the express purpose of exercising the interfaces between the components. This activity is to be carried out by the Test Team. Integration test will be termed complete when actual results and expected results are either in line or differences are explainable/acceptable based on client input.

Incremental Integration Testing: Continuous testing of an application as new functionality is added.

System Testing: System testing is performed when all the components are delivered to central repository prior to the release of the software. The testing is done on priority basis of business processes. All the defects are logged and assigned to respective component owners. The component and unit testing shall be performed after the correction of code. However, it may depend on size and type of individual test specifications. Impact analysis is useful to narrow down testing efforts by identifying critical test cases affected due to code change.

Pre-Production Testing: Pre-Production testing is done simulating the production load. Test data is either prepared or generated from the tools. This testing is used to evaluate performance, load capacity and concurrency. Load testing tools can also be used for this purpose. Following special type of testing are done during Pre-production Testing Phase:

Regression Testing: The objective of regression testing is to ensure software remains intact. A baseline set of data and scripts will be maintained and executed to verify changes introduced during the release have not “undone” any previous code. Expected results from the baseline are compared to results of the software being regression tested. All discrepancies will be highlighted and accounted for, before testing proceeds to the next level.

Performance Testing: Although performance testing is described as a part of system testing, it can be regarded as a distinct level of testing. Performance testing will verify the load, volume, and response times as defined by requirements.

Load Testing: Testing an application under heavy loads, such as the testing of a web site under a range of loads to determine at what point the systems response time degrades or fails.

Installation Testing: Testing full, partial, or upgrade install/uninstall processes. The installation test for a release will be conducted with the objective of demonstrating production readiness. This test is conducted after the application has been migrated to the client’s site. It will encompass the inventory of configuration items (performed by the application’s System Administration) and evaluation of data readiness, as well as dynamic tests focused on basic system functionality. When necessary, a sanity test will be performed following the installation testing.

Security/Penetration Testing: Testing how well the system protects against unauthorized internal or external access, willful damage, etc. This type of testing may require sophisticated testing techniques.

Recovery/Error Testing: Testing how well a system recovers from crashes, hardware failures, or other catastrophic problems.

Acceptance Testing: During the test scenarios definition, for each of the business scenario, an acceptance criterion is defined. Acceptance criteria include expected behavior of the s/w component and the expected results (data). Expected results form a part of the Exit Criteria. In addition to expected result and behaviors, some conditions are also specified in the exit criteria. They can be:

- Number of bugs to be discovered for a functional module. This depends on size of the functionality and is an indicator of amount of testing done. If any medium or low-priority errors are outstanding - the implementation risk must be signed off as acceptable by ASCL and Lead Partner along with consortium partners
- All High Priority errors from System Test must be fixed and tested by MSI along with consortium partners needs to get the acceptance criteria approved from ASCL for all the functional components of the system. The Acceptance Criteria for each release into production environment will be agreed upon by MSI along with consortium partners in consultation with ASCL prior to release from Testing to production environment. After installation, if any bug is reported or there is non-compliance to requirements then a proper procedure should be followed. End-user should report (“Change Request”) to his/her supervisor about the bug that will in turn get forwarded to Project Manager (PM). PM will forward the List of change request to Lead Partner along with consortium partners. After the bug is fixed, it should be reflected in the production copy after testing it.

Performance Testing: The MSI has to test and demonstrate the operational performance requirement as per specification after completion of entire scope. This will be part of acceptance testing. The system will be taken over by owner only after successful operational performance testing. The MSI has to arrange necessary hardware / software to demonstrate the performance testing. MSI should note that ASCL can appoint a third party agency for conducting any part of above testing procedures (in addition to the testing carried out by the bidder).

11.4. Testing, Commissioning & Successful Operation

The scope includes testing and commissioning & implementation of all equipment, sub-systems and systems of the project and putting them into successful technical & commercial operation. The scope shall include but not limited to the requirements given elsewhere in the specification. The MSI shall be responsible to provide all necessary testing and commissioning personnel, tools/kits, test equipment etc.

12. Handholding and Training

To strengthen the staff, structured capacity building programs shall be undertaken for multiple levels in the organizational hierarchy like foundation process/ soft skills training to the staff for pre-defined period. Also, refresher trainings for Command Control Centre/City Operation Staff and designated Authorities & Police staff shall be a part of Capacity Building. It is important to understand that training needs to be provided to each and every staff personnel of such operation centres. These officers shall be handling emergency situations with very minimal turnaround time.

- 1) MSI shall prepare and submit detailed Training Plan and Training Manuals to ASCL /authorized entity for review and approval.
- 2) 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.
- 3) MSI shall be responsible for necessary demonstration environment setup of all ICT solutions in this RFP to conduct end user training. End user training shall include all the equipment including but not limited to all the applications and infrastructure at Operation centres, data centres & field Locations. End user training shall be conducted at a centralized location or any other location as identified by ASCL with inputs from MSI.
- 4) 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.
- 5) MSI shall impart operational and technical training to internal users on solutions being implemented to allow them to effectively and efficiently use the surveillance system.
- 6) MSI shall prepare the solution specific training manuals and submit the same to Authority for review and approval. Training Manuals, operation procedures, visual help-kit etc. shall be provided in English language.
- 7) MSI shall provide training to selected officers of ASCL covering functional, technical aspects, usage and implementation of the products and solutions.
- 8) 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.
- 9) An annual training calendar shall be clearly chalked out and shared with ASCL along with complete details of content of training, target audience for each year etc.
- 10) MSI shall update training manuals, procedures manual, deployment/Installation guides etc. on a regular basis (Quarterly/ Biannual) to reflect the latest changes to the solutions implemented and new developments.
- 11) MSI shall ensure that training is a continuous process for the users. Basic computer awareness, fundamentals of computer systems, basic, intermediate and advanced application usage modules shall be identified by MSI.
- 12) 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 MSI.
- 13) Time Schedule and detailed program shall be prepared in consultation with ASCL and respective authorized entity (Police). 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.

- 14) MSI is required to deploy a Master Trainer who shall be responsible for planning, designing and conducting continuous training sessions.
- 15) Training sessions and workshops shall comprise of presentations, demonstrations and hands-on mandatorily for the application modules.
- 16) ASCL shall be responsible for identifying and nominating users for the training. However, MSI shall be responsible for facilitating and coordinating this entire process.
- 17) MSI shall be responsible for making the feedback available for the Authority/authorized entity to review and track the progress, in case, after feedback, more than 30% of the respondents suggest that the training provided to them was unsatisfactory or less than satisfactory then the MSI shall re-conduct the same training at no extra cost.

12.1. Types of Trainings

Following training needs is identified for all the project stakeholders:

12.1.1. Basic IT training

This module shall include components on fundamentals of: Computer usage, Network, Desktop operations, User admin, Application installation, Basic computer troubleshooting etc.

12.1.2. Functional Training

Basic IT skills, Software Applications (City Operation Centre and Command & Control Centre), Networking, Hardware Installation, Centralized Helpdesk, Feed monitoring

12.1.3. Administrative Training

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

12.1.4. Senior Management Training

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

12.2. Post-Implementation Training

Refresher Trainings for the Senior Management, Functional/Operational training and IT basics for new operators, Refresher courses on System Administration, Change Management programs.

13. Project Implementation Timelines & Deliverables

ASCL intends to implement the project in phased manner approach, distributed in three phases as mentioned below:

13.1. Phase I – T + 2 months (T is the date of signing of the contract with MSI)

13.1.1. Study & Reporting Activities:

A	Phase I: Mobilization and Design	D + 2 months
1	Resource Mobilization	D + 1 months
2	Detailed Project Study for all ICT solution: a) Detailed Survey of identified Sites, Network and Power Requirements b) Hardware and Software Deployment plans c) Detailed Project Plan including Operations management, Contract management, Risk Management, Information Security and Business Continuity d) FRS, SRS, SDD Documents for all work streams & components	D + 2 months

13.2. Phase II – T + 6 months

B	Phase II: Supply, Installation, Testing & Go Live	D + 6 months
1	Data Center and Disaster Recovery Site	D + 5 Months
2	City Communication Network	D + 2 Months
3	Geographical Information System for City	D + 4 Months
4	Adaptive Traffic Signals and Management System	D + 4 Months
5	Intelligent Traffic Management Systems	D + 4 Months
6	CCTV and Surveillance Based System for City	D + 4 Months
7	Environment Sensors	D + 4 Months
8	ICT Enabled Solid Waste Management	D + 6 Months
9	Integrated City and Command Control Centre (ICCC) for ASCL	D + 6 Months
10	Existing Integration Components	D + 6 Months

13.3. Phase III – T + 9 months

C	Phase III: Testing & Go Live		T + 9 Months
1	Functional Testing	Compliance Report	T + 8 Months
2	Load and Performance Testing	Compliance Report	T + 8 Months
3	Failover and Rollback Testing of DC and DR Sites	Compliance Report	T + 8 Months
4	User Acceptance Testing	-	T + 9 Months
5	Go Live	-	T + 9 Months

13.4. Phase IV – T1 + 60 months (T1 is the date of Go Live of all application)

D	Phase IV: Operations & Maintenance phase for a period of 60 months from the date of Go Live		
1	Operation & Maintenance	SLA Compliance Report	Every Quarter

14. Payment Terms and Schedule

- 1) Request for payment shall be made to ASCL in writing, accompanied by invoices describing, as appropriate, services performed, required documents submitted pursuant to general conditions of contract and upon fulfilment of all obligations stipulated in the Contract.
- 2) Due payments shall be made promptly by ASCL, generally within sixty (60) days after submission of an invoice or request for payment by MSI
- 3) The currency for payment to MSI under this Contract shall be Indian Rupees (INR) only. All remittance charges shall be borne by MSI.
- 4) In case of disputed items, the disputed amount shall be withheld and shall be paid only after settlement of the dispute.
- 5) Any penalties/ liquidated damages, as applicable, for delay/ non-performance, shall be deducted from the due payments of the respective milestones.
- 6) Taxes, as applicable, shall be deducted, as per prevalent rules and regulations

Payments to MSI, after successful completion of target milestones (including specified project deliverables), shall be made as under:

Sr. No.	Scope of Work	Timelines	Payment
A	Phase I		
1.	Advance	On resource mobilisation	10% of contract value
2.	Upon finalization SRS, FRS & SDD	T+2 Months	As completed 10% of contract value
B	Phase II		
3.	On Supply, Installation and Commissioning of each component	T + 6 Months	As completed 20 % of contract value of each component
C	Phase III		
4.	After 3 Months Testing & Go Live of all components	T + 9 Months	As completed 20% of contract value of each component
D	Phase IV		
5.	Operations & Maintenance of 60 months from the date of Go Live	T1 + 60 Months	40% of Contract Value in equal quarterly instalments to be paid over a period of 60 months
Note:	<ul style="list-style-type: none"> • <i>T is the date of signing of contract</i> • <i>T1 is the date of Go Live.</i> 		

15. Annexures

15.1. Annexure 1: Junctions for Intelligent and Adaptive Traffic Signals

S.No.	List of Junctions
1	Agra Cantt Railway Station
2	Amar Singh Gate (Red Fort)
3	Bhagwan Talkies
4	Bhogi Pura Chauraha
5	Bijlighar Chauraha
6	Bodhla Chauraha
7	Collectorate Tiraha
8	Entry point inner ring road Fatehabad road
9	Hariparvat Chauraha
10	Itmad Ud Daulha Tiraha
11	Phool Sayyad Chauraha
12	Purani Mandi Chauraha
13	PWD Club Chauraha
14	Rambaugh Chauraha
15	Sai Ka Takiya Chauraha
16	Shahdra Chouraha, Bajrang Petrol Pump, Entry Point
17	Shamshan Ghat Chauraha
18	Sikandra Tiraha
19	Soor Sadan Tiraha
20	St Johns Chauraha
21	Subhash Park Tiraha
22	Taj View Tiraha
23	Targhar Chauraha
24	TDI Mall
25	Waterworks Junction
26	100Ft Kalindi Road
27	100Ft Tiraha PS Shah Ganj, Fatehpur Entry Point
28	Agra College Tiraha
29	Amar Hotel Tiraha
30	Belanganj Chauraha
31	Chimman Puri Chauraha
32	Deewani Tiraha, New Agra
33	Dhakran Chauraha
34	Gurudwara Cut
35	Idgah Chauraha
36	Kalakriti Tiraha
37	Kargil Petrol Pump Tiraha
38	Khandhari Chauraha

39	Kothi Meena Chauraha
40	Loha Mandi Chauraha
41	Madina Tiraha
42	Maruti Estate Chauraha
43	Nalband Chauraha
44	Nammer Chauraha
45	Pratapura Chowk
46	Raja Mandi Chauraha
47	RBS Chauraha
48	Rooi Ki Mandi Chauraha
49	Sadar Bazaar Road
50	Sadar Bhatti
51	State Bank Tiraha
52	Sultan Ganj Ki Pulia
53	University Gate Khandari Campus
54	Victoria Park Tiraha
55	Fauwara Tiraha
56	Gadha Pada Chauraha
57	Ghatia Azam Khan Chowk (Kinari Bazaar Chowk)
58	Guru Agrasen Chowk (Raja Ki Mandi Railway Station)
59	Haathi Ghat Chowk
60	Paliwal Chowk
61	Ram Nagar Ki Pulia Chauraha
62	Saket Tiraha

15.2. Annexure 2: Intelligent Traffic Management System with General Surveillance

S.No.	List of Junctions	Only ANPR	ANPR + RLVD	No Helmet	Wrong Way	Illegal Parking
1	Amar Singh Gate (Red Fort)	Y	N	N	N	N
2	Bhagwan Talkies	-	Y	Y	N	Y
3	Bijlighar Chauraha	N	Y	Y	Y	Y
4	Bodhla Chauraha	-	Y	Y	N	N
5	Collectorate Tiraha	-	Y	Y	Y	N
6	Entry point inner ring road Fatehabad road	-	Y	Y	N	N
7	Hariparvat Chauraha	-	Y	Y	Y	N
8	Itmad Ud Daulha Tiraha	-	Y	Y	N	Y
9	Kerawali Tiraha, Runakta, Entry Point	Y	N	N	N	N
10	Keriya More, Sarai Khawaja,Entry Point(Traffic)	Y	N	N	Y	N
11	Nunihai Tiraha	Y	N	N	N	N
12	Panchkuia	Y	N	N	N	N
13	Purani Mandi Chauraha	-	Y	Y	Y	Y
14	PWD Club Chauraha	-	Y	Y	Y	N
15	Rambaugh Chauraha	-	Y	Y	Y	Y
16	Sai Ka Takiya Chauraha	-	Y	Y	Y	N
17	Shahdra Chouraha, Bajrang Petrol Pump,Entry Point	-	Y	Y	N	Y
18	Shamshan Ghat Chauraha	Y	N	N	N	N
19	Sikandra Tiraha	-	Y	Y	N	N
20	Soor Sadan Tiraha	-	Y	Y	Y	N
21	St Johns Chauraha	-	Y	Y	Y	N
22	Subhash Park Tiraha	-	Y	Y	Y	N
23	Taj View Tiraha	-	Y	Y	Y	N
24	Targhar Chauraha	-	Y	Y	N	N
25	TDI Mall	-	Y	Y	N	N
26	Tedhi Baghiya, Entry Point	Y	N	N	Y	Y
27	Waterworks Junction	-	Y	Y	N	Y
28	100Ft Tiraha PS Shah Ganj, Fatehpur Entry Point	Y	N	N	N	N
29	Agra College Tiraha	-	Y	Y	Y	N
30	Deewani Tiraha, New Agra	-	Y	Y	N	N
31	Dhakran Chauraha	-	Y	Y	Y	N
32	Gurudwara Cut	Y	N	N	Y	Y
33	Idgah Chauraha	-	Y	Y	Y	Y
34	Kargil Petrol Pump Tiraha	Y	N	N	N	N
35	Khandhari Chauraha	-	Y	Y	Y	N

36	Loha Mandi Chauraha	Y	N	N	N	N
37	Maruti Estate Chauraha	-	Y	Y	N	N
38	Nalband Chauraha	-	Y	Y	N	N
39	Pratapura Chowk	-	Y	Y	N	N
40	Raja Mandi Chauraha	-	Y	Y	N	N
41	State Bank Tiraha	-	Y	Y	N	N
42	Sultan Ganj Ki Pulia	-	Y	Y	Y	Y
43	University Gate Khandari Campus	-	Y	Y	N	N

S.No	List of Junctions	Phase	Count of Cameras					General Surveillance	
			Requirement for Only ANPR Cameras	Requirement for ANPR + RLVD Cameras		Requirement for No Helmet Camera	Requirement for Illegal Parking	Fix Camera	PTZ Camera
				ANPR Cameras	RLVD Cameras				
1	Amar Singh Gate (Red Fort)	1	4	-	-	-	-	2	1
2	Bhagwan Talkies	1	-	8	4	8	4	8	2
3	Bijlighar Chauraha	1	-	5	5	5	5	-	2
4	Bodhla Chauraha	1	-	4	4	4	-	-	1
5	Collectorate Tiraha	1	-	5	3	5	-	-	1
6	Entry point inner ring road Fatehabad road	1	-	3	3	3	-	-	1
7	Hariparvat Chauraha	1	-	8	4	8	-	-	1
8	Itmad Ud Daulha Tiraha	1	-	4	3	4	3	-	1
9	Kerawali Tiraha, Runakta, Entry Point	1	3	-	-	-	-	-	1
10	Keriya More, Sarai Khawaja, Entry Point(Traffic)	1	4	-	-	-	-	-	-
11	Nunihai Tiraha	1	3	-	-	-	-	-	1
12	Panchkuia	1	5	-	-	-	-	2	2
13	Purani Mandi Chauraha	1	-	4	4	4	4	-	1
14	PWD Club Chauraha	1	-	8	4	8	-	-	1

15	Rambaugh Chauraha	1	-	8	4	8	4	8	2
16	Sai Ka Takiya Chauraha	1	-	6	4	6	-	-	1
17	Shahdra Chouraha, Bajrang Petrol Pump, Entry Point	1	-	5	3	5	3	4	2
18	Shamshan Ghat Chauraha	1	4	-	-	-	-	-	1
19	Sikandra Tiraha	1	-	5	3	5	-	-	1
20	Soor Sadan Tiraha	1	-	6	3	6	-	-	1
21	St Johns Chauraha	1	-	7	4	7	-	-	1
22	Subhash Park Tiraha	1	-	5	3	5	-	-	1
23	Taj View Tiraha	1	-	5	3	5	-	-	1
24	Targhar Chauraha	1	-	6	4	6	-	-	1
25	TDI Mall	1	-	5	3	5	-	-	1
26	Tedhi Baghiya, Entry Point	1	3	-	-	-	3	-	2
27	Waterworks Junction	1	-	6	4	6	4	8	2
28	100Ft Tiraha PS Shah Ganj, Fatehpur Entry Point	2	4	-	-	-	-	-	1
29	Agra College Tiraha	2	-	5	3	5	-	-	1
30	Deewani Tiraha, New Agra	2	-	4	2	4	-	-	2
31	Dhakran Chauraha	2	-	4	2	4	-	-	1
32	Gurudwara Cut	2	4	-	-	-	4	-	1
33	Idgah Chauraha	2	-	4	4	7	4	-	1
34	Kargil Petrol Pump Tiraha	2	3	-	-	-	-	-	1
35	Khandhari Chauraha	2	-	6	4	6	4	6	2
36	Loha Mandi Chauraha	2	4	-	-	-	-	-	1
37	Maruti Estate Chauraha	2	-	4	2	2	-	-	1
38	Nalband Chauraha	2	-	6	4	6	-	-	1
39	Pratapura Chowk	2	-	6	4	6	-	-	1
40	Raja Mandi Chauraha	2	-	5	3	5	-	-	1
41	State Bank Tiraha	2	-	5	3	5	-	-	1

42	Sultan Ganj Ki Pulia	2	-	4	4	4	4	8	2
43	University Gate Khandari Campus	2	-	6	3	6	-	-	1
TOTAL		41		172	110	173	46	46	52

Only Surveillance at Traffic Junctions

S.No.	List of Junctions	Traffic Signals	Fix Camera	PTZ Camera
1	Agra Cantt Railway Station	Y	-	2
2	Bhogi Pura Chauraha	Y	4	1
3	Phool Sayyad Chauraha	Y	-	1
4	100Ft Kalindi Road	Y	-	1
5	Amar Hotel Tiraha	Y	1	1
6	Belanganj Chauraha	Y	-	2
7	Chimman Puri Chauraha	Y	-	1
8	Kalakriti Tiraha	Y	-	1
9	Kothi Meena Chauraha	Y	-	1
10	Madina Tiraha	Y	-	1
11	Nammer Chauraha	Y	-	1
12	RBS Chauraha	Y	-	1
13	Rooi Ki Mandi Chauraha	Y	4	1
14	Sadar Bazaar Road	Y	-	-
15	Sadar Bhatti	Y	1	1
16	Victoria Park Tiraha	Y	-	1
17	Fauwara Tiraha	Y	-	1
18	Gadha Pada Chauraha	Y	-	1
19	Ghatia Azam Khan Chowk (Kinari Bazaar Chowk)	Y	-	1
20	Guru Agrasen Chowk (Raja Ki Mandi Railway Station)	Y	-	1
21	Haathi Ghat Chowk	Y	-	1
22	Paliwal Chowk	Y	-	1
23	Ram Nagar Ki Pulia Chauraha	Y	-	1
24	Saket Tiraha	Y	-	1
TOTAL			10	25

15.3. Annexure 3: CCTV for City Surveillance System

Sr No	Junction Name	Area/Thana	No of Arms	No of Fixed Box camera	No of PTZ Camera
1	Hing Ki Mandi Tiraha	Kotwali	3	3	1
2	Rawatpada Tiraha	Kotwali	3	3	1
3	Roxy Cinema Tiraha	Kotwali	3	3	1
4	Fubbara Tiraha Kotwali	Kotwali	3	3	1
5	Seth Gali Tiraha	Kotwali	3	3	1
6	Kashmiri Bazaar Tiraha	Kotwali	3	3	1
7	Sindhi Bazar Tiraha	Kotwali	3	3	1
8	City station Tiraha	Kotwali	3	3	1
9	Tilak bazar Chouraha	Kotwali	4	4	1
10	Roshan Mohalla Choraha	Kotwali	4	4	1
11	Nalla Mahavir Pulia Tiraha	Kotwali	3	3	1
12	Subhash Bazar Tiraha	Kotwali	3	3	1
13	Lohargali Tiraha	Kotwali	3	3	1
14	Fubbara Tiraha Kinari Bazaar	Kotwali	3	3	1
15	Chaubey Ji Ki Fatak	Kotwali	2	2	1
16	Seb Ka Bazaar Tiraha	Kotwali	3	3	1
17	Johari Bazaar Tiraha	Kotwali	3	3	1
18	Emergency Tiraha	MM Gate	3	3	1
19	Purani Emergency Tiraha	MM Gate	3	3	1
20	Kaliwadi Chauraha	MM Gate	4	4	1
21	Collectorate Gate	NAI Ki Mandi	3	3	1
22	Vishwa Vidyalay Main Gate	HARI PARVAT	3	3	1
23	Paliwal Main Gate	HARI PARVAT	3	3	1
24	Sahyog Vatika Main Gate	HARI PARVAT	3	3	1
25	Vishwa Vidyalay Main Gate (Chouraha)	HARI PARVAT	4	4	1
26	Wazirpura	HARI PARVAT	3	3	1
27	Big Bazaar	HARI PARVAT	4	6	1
28	GG Nursing Home	HARI PARVAT	3	3	1
29	Sanjay Talkies	HARI PARVAT	3	3	1
30	LIC Building	HARI PARVAT	4	3	1
31	Vikash Bhawan	HARI PARVAT	5	5	1
32	Kapda Market	HARI PARVAT	3	3	1
33	Max Mall	HARI PARVAT	4	4	1
34	SBI Zonal Karyalay	HARI PARVAT	4	4	1
35	Shoe Market	NAI Ki Mandi	4	4	1
36	Guffa Baar Parking	HARI PARVAT	3	3	1
37	ICICI Bank Parking	HARI PARVAT	3	3	1
38	Pratik Center Parking	HARI PARVAT	3	3	1
39	Delhigate Chauraha	HARI PARVAT	4	4	1
40	Hanuman Chouraha	HARI PARVAT	4	4	1

41	Diwani Chauraha	NEW AGRA	4	7	3
42	Radhakrishna Choraha	HARI PARVAT	4	4	1
43	Abhinandana Tiraha	HARI PARVAT	3	3	1
44	Vijaynagar Chowki	HARI PARVAT	4	4	1
45	Shah market	HARI PARVAT	2	6	1
46	Anjaana Market	HARI PARVAT	0	4	1
47	Opposite Thirrah Khandari Chemps in front of University Gate	HARI PARVAT	3	3	1
48	Langde Ki Chowki Chauraha	HARI PARVAT	4	4	1
49	Char Khamba Chauraha	HARI PARVAT	4	4	1
50	Ratanpura Chauraha	HARI PARVAT	4	4	1
51	Chauraha Ganda Nala (near Bijar Nagla)	HARI PARVAT	4	4	1
52	Masta Ki Bagichi Chauraha	HARI PARVAT	4	4	1
53	Sanjay Palace	HARI PARVAT	2	6	1
54	DhuliaGanj Chauraha	HARI PARVAT	4	4	1
55	Hanuman Temple Chouraha	HARI PARVAT	4	4	1
56	Church Road Suresh Chandra Chandra Dinesh Chandi in front of the showroom	HARI PARVAT	4	4	1
57	Bhagwaan Talkies Chauraha	NEW AGRA	4	4	1
58	Shakya Market	NEW AGRA	2	2	1
59	Tejnagar mode	NEW AGRA	3	3	1
60	Hydel Chauraha	NEW AGRA	4	4	1
61	Central Bank cut	NEW AGRA	3	3	1
62	Shriram Check	NEW AGRA	4	4	1
63	Shreeji Guest House Cut	NEW AGRA	3	3	1
64	Agarwal Hospital Cut	NEW AGRA	3	3	1
65	Janak Park Chauraha	NEW AGRA	4	4	1
66	Aadarsh Nagar Mode	NEW AGRA	3	3	1
67	Agarwal Seva Sadar Tiraha	NEW AGRA	3	3	1
68	Hiralal Halwai Tiraha	NEW AGRA	3	3	1
69	Waterworks from Chairla to the guest house on the road to Bulkeshwar	NEW AGRA	3	3	1
70	Chandi Chowki Chauraha	NEW AGRA	4	4	1
71	Shakti Market Chauraha	NEW AGRA	4	4	1
72	Shalimar Extenson Chairah	NEW AGRA	4	4	1
73	Subhash Nagar Chairah	NEW AGRA	4	4	1
74	Dayalbauh Road (Nagla Padi Road)	NEW AGRA	3	3	1
75	Chitalamata Temple Garden JPNagar Mode	NEW AGRA	3	3	1
76	Mau Road Nirbhaya Nagar Terraha Mode	NEW AGRA	3	3	1
77	Lions Colony Mode Madhusudan Motors	NEW AGRA	3	3	1
78	Near NH-2 Gupta Overseas	NEW AGRA	3	3	1
79	Dayalbagh Road Sabzi Mandi Choraha	NEW AGRA	4	4	1

80	Dayalbagh Road Post Office (Tiraha)	NEW AGRA	3	3	1
81	Abulula Tiraha	NEW AGRA	3	3	1
82	Abulula's Pulia	NEW AGRA	3	3	1
83	HI-2 slope before Dia Komplex	NEW AGRA	3	3	1
84	Bhagwan Talkies Flyover (Parking Stand)	NEW AGRA	3	3	1
85	Sultanganj's Puliyya Fly Aover Mughal Road	NEW AGRA	4	4	1
86	Manoj Dhaba Tiraha Dayalbagh Road	NEW AGRA	3	3	1
87	Near Mughal road Chor Road	NEW AGRA	3	3	1
88	Union Bank Dayalbagh Road	NEW AGRA	3	3	1
89	Nagla budi chirahah	NEW AGRA	4	4	1
90	Kalyani Height K Samne	NEW AGRA	3	3	1
91	Sanjivani Tiraha 100Ft Road	NEW AGRA	3	3	1
92	BOI Cut 100 Ft Road	NEW AGRA	3	3	1
93	Service road cut near Omex Mal	NEW AGRA	3	3	1
94	Diwani Chauraha (Mandir k Paas)	NEW AGRA	3	3	1
95	Badawar House	NEW AGRA	3	3	1
96	Kendriya Hindi Sasthan	HARI PARVAT	4	4	1
97	Charchit Chauraha Shastripuram	SIKANDRA	4	4	1
98	Kailash Mode Guru	SIKANDRA	3	3	1
99	Kailas Mandir	SIKANDRA	3	4	1
100	Bhavna State Mode	SIKANDRA	3	3	1
101	Gurdwara cut	SIKANDRA	3	3	1
102	Kirawali Tiraha	SIKANDRA	3	3	1
103	Sikandra Sabzi Mandi	SADAR	2	4	2
104	Sultanpura chirahah	SADAR	4	4	1
105	Mustafa Quarter (Bhappa Chawlai Tiraha)	SADAR	3	3	1
106	Shahid nagar terrah	SADAR	3	3	1
107	Bhagat Murthy Chairla	SADAR	4	4	1
108	Safoota chirahaha	SADAR	4	4	1
109	Outside railway cant station	SADAR	2	4	1
110	Rajpur bagiya	SADAR	2	2	0
111	Takkar Road Tiraha	SADAR	3	3	1
112	Ukhra Pulia	SADAR	3	3	1
113	Madhunagar	SADAR	4	4	1
114	BD Jain Inter College Campus	SADAR	2	2	0
115	Nand Tackies Chairah	SADAR	4	4	1
116	R. M. O Choraah	SADAR	4	4	1
117	Allabakh Chirahah	SADAR	4	4	1
118	Kotli Bagchi Semari Taj Chorrah	SADAR	4	4	1
119	Rajeshwar Temple	SADAR	2	2	1
120	Eklavya Stadium	SADAR	2	3	1
121	Cariappa chirahah	SADAR	4	4	1

122	Veeragana Jhalkarvi Chairah	TAJ GANJ	4	4	1
123	Basai chirah	TAJ GANJ	3	3	1
124	Double Tree Y Hilton Chorahah	TAJ GANJ	4	4	1
125	Vibhav Nagar Chauraha	TAJ GANJ	4	4	1
126	ADA Heights	TAJ GANJ	2	3	1
127	Todra Chowki Tiraha	TAJ GANJ	3	3	1
128	Canara Bank Crossroads Idgah	RAKABGANJ	3	3	1
129	Mayur Talkies Railway Colony Thiraha Idgah	RAKABGANJ	3	3	1
130	Railway Station Idgah Colony	RAKABGANJ	3	3	1
131	Gostwali Gali		3	3	1
132	Idgah Katgarh Terraha		3	3	1
133	Mohanpura turn corp compound		2	2	1
134	Ravli Mandir Terrah		3	3	1
135	Ghoulpur house		3	3	1
136	Petrol pump intersection baluganj		2	3	1
137	Chauki Baluganj Chauraha		4	4	1
138	Targhar Chauraha baluganj		4	4	1
139	Chilagarh Chauraha baluganj		4	4	1
140	Auliya Tiraha		3	3	1
141	Sai Ki Takiya Chauraha		4	4	1
142	Dhaulpur House Raipur Terraha		3	3	1
143	Red Fort Terah Man Gate		2	2	0
144	Victoria Park Terrahae		3	3	1
145	Chhalkara Devi cremation ground crossing		4	4	1
146	Yamuna Kinara Road		3	3	1
147	Fort railway station		3	3	1
148	Bhairo Temple Chandappan Alleyaha Biography Mani Mandi		3	3	1
149	Garib Nagar Tiraha		3	3	1
150	Patel Nagar Kali Mata Temple Krishna Kaloni Thiraha Biography Mandi		3	3	1
151	Motiganj Market Division		3	3	1
152	Kala Mahal Peepal Mandi		3	3	1
153	Stretchy Bridge		3	3	1
154	Ambedkar Pool (Below)		3	3	1
155	Bijlighar Dhuliaganj		4	4	1
156	Gudgi Chauraha (Mansoor Khan)		4	4	1
157	BP Oil Mill		3	3	1
158	Naya Pool Tiraha		4	4	1
159	Royal cut Tiraha		3	3	1
160	Niraich near Bhatia Petrol Pump		3	3	1

161	Nunihai in front of the Dauji Misthan		3	3	1
162	Saufhuta road in front of RB degree college		3	3	1
163	Roshan Mohalla Tiraha		3	3	1
164	Subhash bazar		3	3	1
165	Peepalwala Tiraha		3	3	1
166	Hotel Lalas		3	3	1
167	Haathi Gate Tiraha		3	3	1
168	Mahaveer Nala Mode Meera Hussaini		3	3	1
169	Near Mahavir Nalla temple		3	3	1
170	Mantola Terahaha		3	3	1
171	Barfwali Lane		4	4	1
172	Mutwir Masjid Terah Pipal Mandi		3	3	1
173	Naubasta Chairah	LOHA MANDI	4	4	1
174	Besan Basti Chaaraha	LOHA MANDI	4	4	1
175	Telipada Terahaha	LOHA MANDI	3	3	1
176	Pirabahabuddin Choraha	LOHA MANDI	4	4	1
177	Madia Katra Chairla	LOHA MANDI	4	4	1
178	Kidwai Park Chirahah	LOHA MANDI	4	4	1
179	Rajamandi Chairah	LOHA MANDI	4	4	1
180	St. Jans Chairah	LOHA MANDI	4	4	1
181	Panchkuya Chirahah	LOHA MANDI	4	4	1
182	Jaipur House	LOHA MANDI	0	4	1
183	Baldevganj Sarafa Bazar	LOHA MANDI	2	2	1
184	Lohamandi Main Market	LOHA MANDI	4	4	1
185	Arya Samaj Temple Chirah Jaipur House	LOHA MANDI	4	4	1
186	Tota Ka Taal Tiraha	LOHA MANDI	3	3	1
187	Syedpada Tiraha	LOHA MANDI	3	3	1
188	Alamganj police check post	LOHA MANDI	2	2	0
189	Alamgunj police check old	LOHA MANDI	2	2	0
190	Avadhपुरi Terrah	JAGDISHPURA	4	4	1
191	Jeevan jyoti thiraha	JAGDISHPURA	3	3	1
192	Pratap Nagar Chairahah	JAGDISHPURA	3	4	1
193	Tempo Station Sector 7 Tiraha Housing Development Colony	JAGDISHPURA	3	3	1
194	Bichपुरi naharpur	JAGDISHPURA	4	4	1
195	Jeevan Jyoti Hospital Housing Development	JAGDISHPURA	2	3	1
196	Vinayak Hospital Housing Development	JAGDISHPURA	3	3	1
197	Moti Hospital Bidla Bychपुरi Road	JAGDISHPURA	3	3	1
198	Sadar Tehsil Tiraha	Shahganj	3	4	1
199	Shahganj Chairahah	Shahganj	4	4	1
200	Speed color lab Chauraha	Shahganj	4	4	1

201	Panchkuya near GIC School Gate	Shahganj	2	2	0
202	C News Terra	Shahganj	3	3	1
203	Shivaji Nagar	Shahganj	2	2	0
204	Alok Nagar Chairah	Shahganj	4	4	1
205	Saket Chairah	Shahganj	3	3	1
206	COD Terra	Shahganj	3	3	1
207	Shakargadh ki Pulia	Shahganj	3	3	1
208	Pruthvinath Fatak Police Chowki	Shahganj	2	2	0
209	Rajiv Talkies Tiraha	Shahganj	3	3	1
210	12 Khamba Double Fatak	Shahganj	2	2	0
211	12 Khamba Single Fatak	Shahganj	3	3	1
212	Arjun Nagar Tiraha	Shahganj	3	3	1
213	Arjun Nagar near Shishu Bharti School Mode	Shahganj	1	2	0
214	Ajit Nagar Tiraha	Shahganj	3	3	1
215	Malpura Terrah	Shahganj	3	3	1
216	Kamalakhah Dargah Gate	Shahganj	2	3	1
217	Niripura thiraha jaganar road	Shahganj	3	3	1
218	CNG Petrol Pump Sarai Khwaja	Shahganj	3	3	1
219	Idgah chirahah	Shahganj	3	3	1
220	Dayalu Porshad Mode Nagla Chauya	Shahganj	3	3	1
221	Vayubihar Tiraha	Shahganj	3	3	1
222	Shah Market Tiraha	HARI PARVAT	2	6	1
223	Ayodhayakunj Tirahah	Shahganj	3	3	1
224	Shah Market Nehru Nagar Tiraha	HARI PARVAT	3	3	1
225	Shashtri Puram Chouraha	Sikandara	0	4	1
226	Shahganj Chouraha	Shahganj	4	4	1
227	Shastri puram ROB Chouraha	Sikandara	0	4	1
228	Roosi Ki Mandi Chauraha	Shahganj	0	4	1
229	Kariappa Chouraha	Rakabganj	4	0	1
230	Shankar Gargh puliya tiraha	Shahganj	0	3	1
231	Subhash murti Chauraha	Tajganj	4	0	1
232	Malpura Nahar Chouraha	Shahganj	4	0	1
233	Rohta Neher Chauraha	Shahganj	4	0	1
234	Amar hotel Tiraha	Tajganj	3	1	1
235	Loha Mandi Chauraha	Laha mandi	4	0	1
236	Kerawali Tiraha, Runakta, Entry Point	Sikandara	3	0	1
237	Victoria Park Tiraha	Rakabganj	3	0	1
238	Madiya Katra Tiraha	Hari parvat	3	0	1
239	Delhi Gate	Hari parvat	4	0	1
240	State Bank Tiraha	Rakabganj	3	0	1
241	New Nyayalaya Deewani, New Agra	New Agra	2	1	1
242	Barrier Gate SN Medical College	MM Gate	4	1	1

243	ISBT	Hari parvat	0	12	2
244	Bhawna Tower	Sikandara	3	0	1
245	Idgah Railway Station	Rakabganj	3	0	1
246	Maruti State Chouraha	Jagdishpura	4	0	1
247	SN Medical College, SBI Gate	MM Gate	2	2	1
248	Rajpur Chungi	Tajganj	3	0	2
249	Kalakriti tiraha	Tajganj	3	0	1
250	Nyayala Gate, Cemetary	New Agra	2	1	1
251	Agrsen Murti Tiraha	Tajganj	3	0	1
252	Belanganj Chauraha	Chhatta	4	0	2
253	Chimman Puri Chauraha	Mantola	3	0	1
254	Sadar Bhatti	Nai Ki Mandi	4	1	1
255	Nunihai Tiraha	Aetma-ud-daulha	3	0	1
256	Chhipitola Chouraha	Rakabganj	4	0	1
257	Baluganj Chouraha	Rakabganj	5	0	2
258	University Gate Khandari Campus	Hari parvat	3	0	2
259	Jivani Mandi	Chhatta	4	0	2
260	Basai tiraha	Tajganj	3	0	2
261	Patholi nehar Chauraha	Shahganj	4	0	2
262	G.P.O chauraha	Sadar	4	0	2
263	Trydent tiraha	Tajganj	3	0	2
264	Mankameshwar Tiraha	Kotwali	3	0	2
265	Pani Ki Tanki, Ghatia Azam Khan, Sanjay Palace	Hari parvat	3	0	2
266	100ft, Shamshabad Rd, Entry Point	Shahganj	3	0	2
267	Fatehabad Road/Tohra Chowki Tiraha	Tajganj	3	0	2
268	Shah Market , Tiraha	Hari parvat	3	0	2
269	Shah Market, Nehru Nagar Tiraha	Hari parvat	3	0	2
270	DayalBagh, Radhaswami Temple	New Agra	2	0	2
271	SSP Residence Office		3	2	2
272	Main Market Kamla Nagar	New Agra	4	0	2
273	Kamla Nagar Chouraha	New Agra	4	0	2
274	Dhulia Ganj Chauraha	Kotwali	4	0	2
275	Fauwara Chouraha	Kotwali	4	0	2
276	Madina Tiraha	Mantola	3	0	2
277	Meera Husaeni Chouraha	Mentola	4	0	2
278	Amar Pura Chouraha	Jagdishpura	4	0	2
279	Karbala/Motilal Nehru Road Chouraha Near University	Hari parvat	4	0	2
280	Awas Vikas chowki k Paas	Jagdishpura	3	0	2
281	Awas Vikas Sector 8	Jagdishpura	3	0	2
282	Karkunj Chouraha	Sikandara	4	0	2

283	Gadha Pada Chouraha	Hari parvat	3	0	2
284	Kinari Bazar tiraha	Kotwali	3	0	2
285	SSP Residence Office		2	0	2
286	Panchvati chauraha	Tajganj	3	0	2
287	Re-trit tiraha	Tajganj	3	0	2
288	Bagh Farjana chauraha	Hari parvat	4	0	2
289	Hanuman Mandir chauraha	Hari parvat	4	0	2
290	St. poal tiraha	Hari parvat	3	0	2
291	Shaket Tiraha	Shahganj	4	0	2
292	Free Ganj	Chhatta	3	0	2
293	Yamuna View Park	Rakabganj	2	0	2
TOTAL				790	326

15.4. Annexure 4: Emergency Panic Button with Public Addressing System

S.No.	List of Junctions	Public Addressing System with Emergency Panic Button
1	Amar Singh Gate (Red Fort)	1
2	Bhagwan Talkies	1
3	Bijlighar Chauraha	1
4	Bodhla Chauraha	1
5	Collectorate Tiraha	1
6	Entry point inner ring road Fatehabad road	1
7	Hariparvat Chauraha	1
8	Itmad Ud Daulha Tiraha	1
9	Kerawali Tiraha, Runakta, Entry Point	1
10	Keriya More, Sarai Khawaja, Entry Point(Traffic)	1
11	Nunihai Tiraha	1
12	Panchkuia	1
13	Purani Mandi Chauraha	1
14	PWD Club Chauraha	1
15	Rambaugh Chauraha	1
16	Sai Ka Takiya Chauraha	1
17	Shahdra Chouraha, Bajrang Petrol Pump, Entry Point	1
18	Shamshan Ghat Chauraha	1
19	Sikandra Tiraha	1
20	Soor Sadan Tiraha	1
21	St Johns Chauraha	1
22	Subhash Park Tiraha	1
23	Taj View Tiraha	1
24	Targhar Chauraha	1
25	TDI Mall	1
26	Tedhi Baghiya, Entry Point	1
27	Waterworks Junction	1
28	100Ft Tiraha PS Shah Ganj, Fatehpur Entry Point	1
29	Agra College Tiraha	1
30	Deewani Tiraha, New Agra	1
31	Dhakran Chauraha	1
32	Gurudwara Cut	1
33	Idgah Chauraha	1
34	Kargil Petrol Pump Tiraha	1
35	Khandhari Chauraha	1
36	Loha Mandi Chauraha	1
37	Maruti Estate Chauraha	1
38	Nalband Chauraha	1



39	Pratapura Chowk	1
40	Raja Mandi Chauraha	1
41	State Bank Tiraha	1
42	Sultan Ganj Ki Pulia	1
43	University Gate Khandari Campus	1

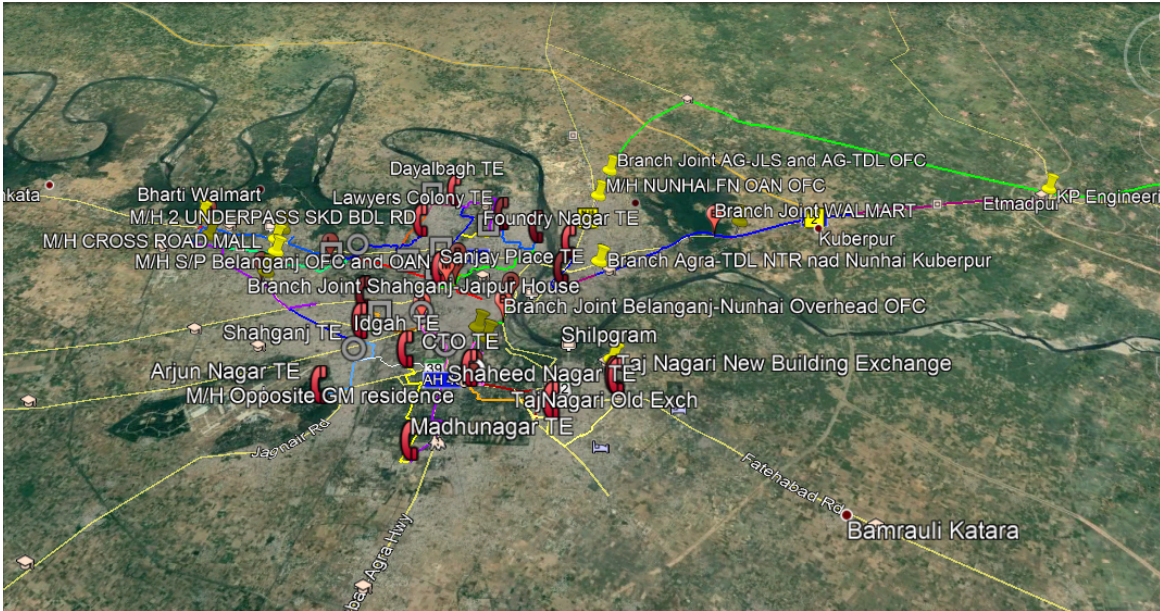
15.5. Annexure 5: Environment Sensors

S.no	Location	Type of Monitoring
1	Rajdeep Bhawan, NH2, Transport Colony	Urban Monitoring
2	Sanjay Place, Civil Lines,	Urban Monitoring
3	Rambagh, Ramnagar Colony, Civil Lines,	Urban Monitoring
4	Shri Mahabaleshwar Mandir, Babu Gulab Rai Marg,	Urban Monitoring
5	Moti Katra, Mantola	Urban Monitoring
6	Namner, Rakabganj	Urban Monitoring
7	Phulatti Bazar, Rawatpara	Urban Monitoring
8	Raja Mandi, Mantola	Urban Monitoring
9	Rajpur Chungi, Indrapuram	Urban Monitoring
10	Sadar Bazar, Agra Cantt,	Urban Monitoring
11	Shahganj	Urban Monitoring
12	Shiv Nagar, Naripura	Urban Monitoring
13	Nai ki Mandi, Mantola	Urban Monitoring
14	Tajganj	Urban Monitoring
15	Dalihal, Paktola, Tajganj	Urban Monitoring
16	Dhandhupura	Urban Monitoring
17	Kaserat Bazar, Tajganj	Urban Monitoring
18	Vibhav Nagar	Urban Monitoring
19	Indrapuram, Tajgan	Urban Monitoring
20	Defence Estate	Urban Monitoring
21	Jodha Bai Ka Roza	Urban Monitoring
22	Shanti Nagar, Ashok Nagar	Urban Monitoring
23	Dhuliya Ganj, Mantola	Urban Monitoring
25	Mandi Said, Civil Lines	Urban Monitoring
26	Model Town, Idgah Colony	Urban Monitoring
27	Agra Fort, Rakabganj	Urban Monitoring
28	Agra Fort-1, bhogipura	Urban Monitoring
29	Delhi Gate, SH 39, Agra Fort	Urban Monitoring
30	Chhipitola Rd, Rakabganj	Urban Monitoring
31	Sadar Bhatti, Dhawlikar	Urban Monitoring
32	Ghatiya Chauraha, Chilli Int Rd, Mandi Said	Urban Monitoring
33	Lajpat Kunj, Civil Lines	Urban Monitoring
34	Dharmapuri, Forest Colony	Taj Mahal Monitoring
35	Taj Museum	Taj Mahal Monitoring
36	Maa Sarawali Mandir	Taj Mahal Monitoring
37	Great Gate	Taj Mahal Monitoring
38	The Garden, Taj Mahal	Taj Mahal Monitoring
39	The Mosque-Kau Ban	Taj Mahal Monitoring

15.6. Annexure 6: OFC Network Availability

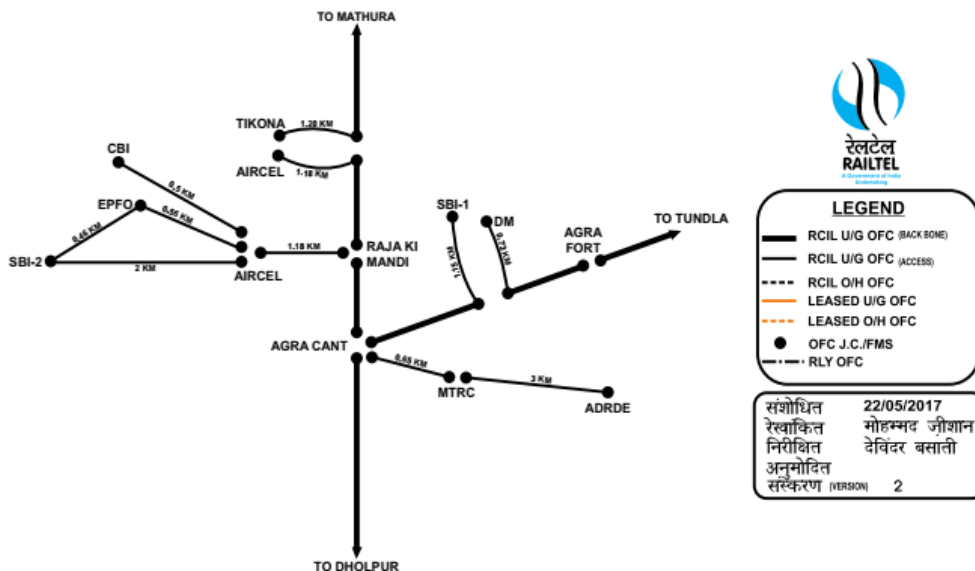
Please find the Optical Fiber availability in Agra from BSNL and Railtel in trailing. There are also various other operators (Telecom and Local MSO) who have optical network availability and MSI may approach directly.

BSNL Network



Railtel Network

**दिल्ली टेरिटरी आगरा सिटी (उत्तरी क्षेत्र)
OFC CONNECTIVITY**



15.7. Annexure 7: List of Police Stations and Chowkis

All the police stations and chowkis need to be connected over the network and shall be well equipped with desired peripherals to support the analytics and also receive events/alarms for immediate response with local monitoring and visuals.

SR NO	POLICE STATIONS	PERSON IN CHARGE	POLICE CHOWKI
1	KOTWALI	SONVIR SINGH	FOLATI
2	KOTWALI	SUESH KUMAR SAGAR	SIEB BAZAAR
3	KOTWALI	CANDRIS GUTAM	PAYI
4	KOTWALI	SUDIR SINGH	RAVAT PADA
5	KOTWALI	RAKISH KUMAR	HIG KE MANDI
6	NAIE KE MANDI	SANTOSH KUMAR	DIVIGAN
7	NAIE KE MANDI	MANOJ KUMAR	COLLECTORATE
8	M.M GETA	RAHUL KUMAR	AMARGENC
9	M.M GETA	SATISH CHAND	KHIKI KALE KHAN
10	M.M GETA	SUDIR KUMAR	DIVIGAN
11	HARI PARVAT	SRIKAHNSH	KHANDARI
12	HARI PARVAT	RAKISH KUMAR	NAHRU NAGAR
13	HARI PARVAT	DINESH KUMAR	T.P.NAGAR
14	HARI PARVAT	CHANDVIR SINGH	RING ROAD
15	HARI PARVAT	HARIND MALIK	SANJAY PALIS
16	HARI PARVAT	ASUVANI KUMAR	PALIVAL
17	HARI PARVAT	KRAPAL SINGH	DELHIGATE
18	HARI PARVAT	PUSPIND KUMAR	HATIYA AJAM
19	HARI PARVAT	ROSANLAL	JILA GIL
20	NEW AGRA	RAGWIND SINGH	BALKISWAR
21	NEW AGRA	RAJKUMAR	KAMLA NAGAR
22	NEW AGRA	OMPRAKASH SINGH	AMAR VIHAR
23	NEW AGRA	GANVIR SINGH	BRAJ BIHAR
24	NEW AGRA	MUKESH SHARMA	DIVISION
25	NEW AGRA	YOGENDRA	DAYAL BAGH
26	NEW AGRA	MANOJ KUMAR	DIWANI
27	SIKANDRA	ARVIND KUMAR	SHASTRIPURAM
28	SIKANDRA	PRAMOD KUMAR	FACTORY AREA
29	SIKANDRA	ARUN KUMAR	RONAKTA
30	SIKANDRA	RAJ KUMAR YADAV	PEEPAL MANDI
31	CHATTA	BHARAT BHUSHAN	BHATTI
32	CHATTA	RAJESH KUMAR	KUDRI MANSOOR KHAN
33	CHATTA	CHANDRA PAL SINGH	DIVISION
34	CHATTA	AMIT KUMAR	JEEVANI MANDI
35	CHATTA	AVNEESH TYAGI	BELANGANJ
36	MANTOLA	RAMKRISHNA	DIVISON
37	MANTOLA	BORENDRA SINGH	SUBHASH BAZAAR

38	AETMA-UD-DAULHA	SANJAY KUMAR SHARMA	TRANS YAMUNA
39	AETMA-UD-DAULHA	VINOD KUMAR YADAV	MANDI SAMITI
40	AETMA-UD-DAULHA	NITYANDRA PANDEY	FOUNDRY NAGAR
41	AETMA-UD-DAULHA	JATINDRA PRASAD	DIVISION
42	AETMA-UD-DAULHA	VIRENDRA KUMAR	LUNIHAI
43	SADAR	NEERAJ SINGH	SAUDAGAR
44	SADAR	RAJEEV KUMAR	LAL KURTI
45	SADAR	SUKHVEER SINGH	FACTORY LINE
46	SADAR	YOGENDRA KUMAR	BINDOO KATRA
47	SADAR	GYANENDRA SOLANKI	CANT
48	SADAR	PRASHANT TYAGI	SHAHEED NAGAR
49	RAKABGANJ	CHANDRASHEKHAR GAUTAM	BALUGANJ
50	RAKABGANJ	NARENDRA SHARMA	FORT
51	RAKABGANJ	VINOD KUMAR	IDGAH
52	RAKABGANJ	ARVIND	TORA
53	TAJGANJ	BHUVNESH KUMAR DIXIT	EKTA
54	TAJGANJ	YOGENDRA KUMAR YADAV	NEETIBAGH
55	TAJGANJ	ARVIND KUMAR	VIBHAV NAGAR
56	TAJGANJ	ANUP SAROJ	TAJ MAHAL DEPOT
57	TAJGANJ	RAJEEV KUMAR	DIVISON
58	TAJGANJ	MANOJ PAWAR	JAIPUR HOUSE
59	TAJGANJ	ANUJ MALIK	GOKULPURA
60	LOHA MANDI	ASHOK KUMAR	RAJA MANDI
61	LOHA MANDI	RAJEEV KUMAR	ALKA POORI
62	LOHA MANDI	NAVEEN KUMAR	AWAAS VIKAS
63	LOHA MANDI	PRADEEP KUMAR	DIVISION
64	LOHA MANDI	MAHESH YADAV	BODHLA
65	JAGDISPURA	RUPENDRA MISHRA	BICHPURI
66	JAGDISPURA	NADEEM	AWADHPURI
67	JAGDISPURA	SHIV BHAN SINGH	KEDAR NAGAR
68	JAGDISPURA	NITYANAND PANDEY	KHERIA
69	JAGDISPURA	DINESH SHARMA	SARAI KWAJA
70	JAGDISPURA	PUSHPENDRA KUMAR	PRATHVINATH
71	SHAHGANJ	VEGH RAM	DIVISION
72	SHAHGANJ	RAJEEV KUMAR GAUTAM	PATHAULI