

# Request for Proposal (RFP) for Selection of System Integrator for Implementation of Nagpur Smart City Solutions

VOLUME II – Scope of Work and Requirement Specifications

Tender Ref No. **DIT/1715/CR:142/39**

Date: 30-04-2016

Directorate of Information Technology,  
Government of Maharashtra



## Table of Content

1.	PROJECT SCOPE OF WORK .....	3
1.1.	SOLUTION 1 - CITY NETWORK BACKBONE .....	5
1.1.1.	Overview.....	5
1.1.2.	Solution requirements .....	6
1.1.3.	Scope of Work .....	11
1.2.	SOLUTION 2 – NAGPUR CITY WIFI.....	22
1.2.1.	Overview.....	22
1.2.2.	Solution requirements .....	22
1.2.3.	Scope of Work .....	24
1.3.	SOLUTION 3 – NAGPUR CITY SURVEILLANCE.....	26
1.3.1.	Overview.....	26
1.3.2.	Solution requirements .....	27
1.3.3.	Scope of Work: .....	29
1.4	SOLUTION 4: NAGPUR CITY KIOSK .....	50
1.4.1	Overview.....	50
1.4.2	Solution requirements.....	50
1.4.3	Scope of work:.....	54
1.5	“SMART STRIP” .....	56
1.5.1	Overview.....	56
1.5.2	Smart Transport .....	58
1.5.3	ICT Enabled Solid Waste Management.....	61
1.5.4	Smart Lighting.....	64
1.5.5	Smart Traffic.....	66
1.5.6	Smart Parking.....	69
1.5.7	Environmental Sensors.....	72
1.6	INTEGRATED OPERATION PLATFORM (IOP).....	73
1.7	GIS MAP FOR NAGPUR CITY .....	74
1.8	OPERATION CENTRES.....	76
1.8.1	Overview.....	76
1.8.2	City Operations Center.....	77
1.8.3	Network Operations Center .....	78
1.8.3.1	Features of NOC .....	79
1.8.3.2	Services to be provided through NOC .....	79
1.8.3.3	NOC Operations Centre.....	91
1.8.3.3.1	Features of NOC .....	92
1.8.3.3.2	Services to be provided through NOC.....	92
1.8.3.3.3	NOC Operations Centre .....	104
1.9	HELPDESK.....	105
1.10	SITE PREPARATION FOR COMMAND CONTROL CENTER, SERVER ROOM, NETWORK OPERATION CENTER, CITY OPERATION CENTER & HELPDESK .....	107
2.	HANDHOLDING AND TRAINING .....	110
3.	PROJECT IMPLEMENTATION TIMELINES, DELIVERABLES AND PAYMENT TERMS .....	113
3.1	PROJECT DELIVERABLES, MILESTONES AND TIMELINES .....	114
3.2	PAYMENT TERMS AND SCHEDULE .....	117

4.	REQUIREMENT SPECIFICATIONS (TECHNICAL / FUNCTIONAL)	118
1.1	CITY NETWORK BACKBONE – (NETWORK INFRASTRUCTURE)	118
1.2	CITY WIFI SOLUTIONS	163
1.3	CITY SURVEILLANCE	183
1.4	CITY SMART KIOSK	235
1.5	“SMART STRIP”	238
1.6	COMMON INFRASTRUCTURE & SOLUTIONS	270
5.	ANNEXURES:	302
	ANNEXURE I: INDICATIVE LIST OF CITY WIFI LOCATIONS	302
	ANNEXURE II: INDICATIVE LIST OF CITY SURVEILLANCE LOCATIONS	305
	ANNEXURE III: SOLUTION REQUIREMENT - LOCATIONS:	334
	ANNEXURE IV: INDICATIVE LIST OF CITY KIOSKS LOCATIONS	335
	ANNEXURE V: PROPOSED LOCATIONS FOR ZONE AGGREGATION POINTS	336
	ANNEXURE VI: INDICATIVE BILL OF MATERIAL – (LOCATION)	338
1.	<i>City Network Backbone</i>	338
2.	<i>City Operation Centre</i>	339
3.	<i>City WIFI</i>	342
4.	<i>City Surveillance</i>	342
5.	<i>City Surveillance Command Control Center</i>	344
6.	<i>Server Room at Command Control Centre</i>	345
7.	<i>City Kiosk</i>	347
a.	<i>Self Service City Kiosk</i>	347
b.	<i>Manned City Kiosk</i>	347
8.	<i>“Smart Strip”</i>	348
1.1	<i>Smart Transport</i>	348
1.2	<i>ICT Based Solid Waste Management System</i>	348
1.3	<i>Smart Lighting</i>	349
1.4	<i>Smart Traffic</i>	349
1.5	<i>Smart Parking</i>	349
1.6	<i>Environmental Sensors</i>	350
9.	<i>Helpdesk (Command Control Center and City Operation Center)</i>	350

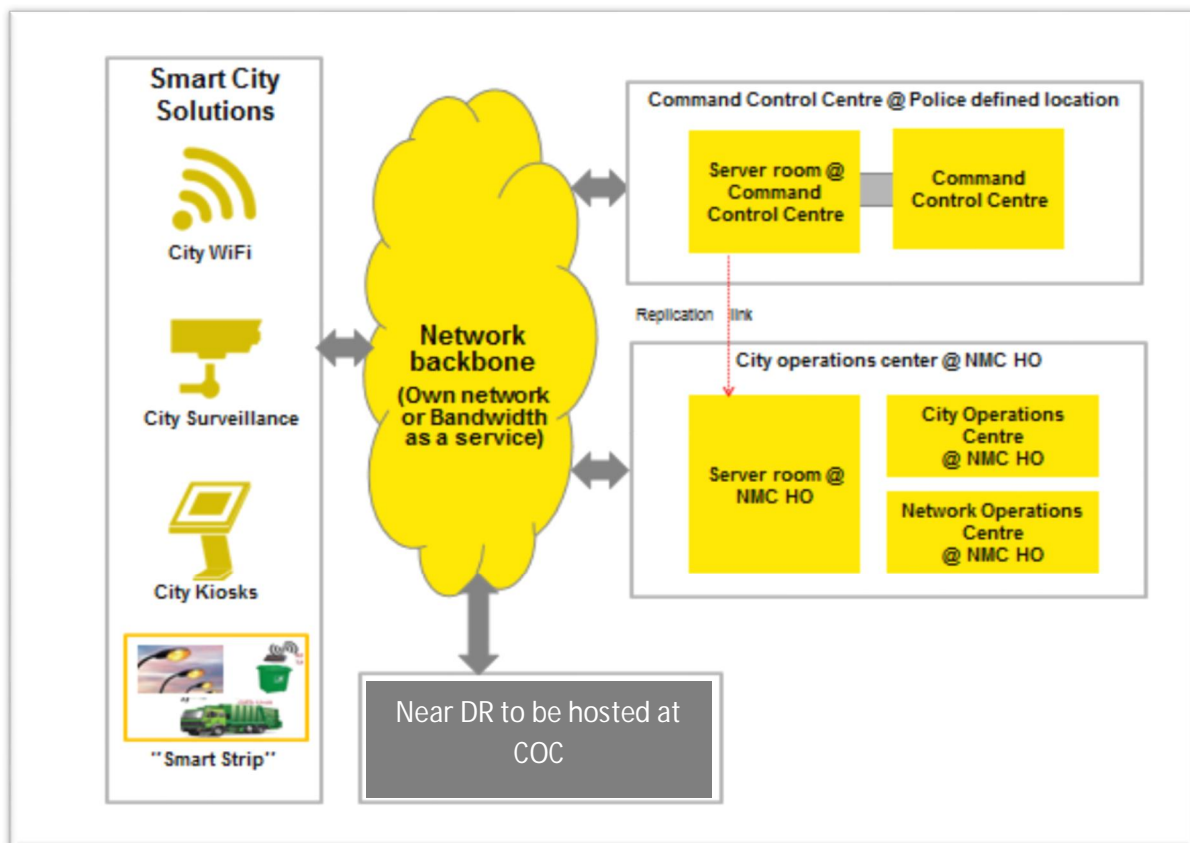
## 1. Project Scope of Work

Key foundation components for Nagpur Smart City considered in this RFP are:

#	Component	Rationale
1.	City Network Backbone	<ul style="list-style-type: none"> <li>• Build a robust and sustainable city-wide network connectivity</li> <li>• Ensure sufficient network capacity for current and future requirements of the city</li> </ul>
2.	City WiFi	<ul style="list-style-type: none"> <li>• Internet connectivity for the for general public to ensure economic development and increased digital inclusion</li> <li>• Improved wireless internet connectivity to support public safety and delivery of municipal corporation services</li> </ul>
3.	City Surveillance	<ul style="list-style-type: none"> <li>• Further strengthening of : <ul style="list-style-type: none"> <li>○ City-wide surveillance</li> <li>○ Technology use for prevention of crime</li> <li>○ Improved response time and post-incident management</li> <li>○ Traffic management</li> <li>○ Crowd management</li> </ul> </li> </ul>
4.	City Kiosk	<ul style="list-style-type: none"> <li>• Improve and widen service delivery to citizens of Nagpur</li> <li>• Provide any-time services to citizens of Nagpur with limited access to mobile devices</li> </ul>
5.	"Smart Strip"	<ul style="list-style-type: none"> <li>• Area based smart interventions as a prototype model</li> </ul>

Future smart city initiatives shall leverage these foundation components to provide services to citizens of Nagpur. Scope of work for the aforementioned components is detailed out in the subsequent sections.

**Diagrammatic representation of SI's scope of work:**



As shown in the diagram the key components with scope of work are:

1. Component 1: City Network Backbone
2. Component 2: City WiFi
3. Component 3: City Surveillance
4. Component 4: City Kiosk
5. Component 5: "Smart Strip"
6. Command Control Center for Surveillance along with Server room and Helpdesk
7. City Operations Centre along with Server room, Network Operation center and Helpdesk

SI shall be responsible to carry out the detailed survey for each of the solution component requirement in order to finalize infrastructure requirement, network bandwidth requirement, operational & administrative challenges etc. and shall submit detailed Site Survey Report and Project Execution Plan to the Purchaser or its designated agency/department.

The subsequent sections detail out the solution and scope with respect to each of the solution component. The SI shall note that the activities defined within scope of work mentioned are indicative and may not be exhaustive. SI 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.

## **1.1. SOLUTION 1 - City Network Backbone**

### **1.1.1. Overview**

With technology being a key driver for implementation of smart city initiatives across the city of Nagpur, a robust network is one of the key foundational requirements on which future ICT based 'Smart' initiatives shall be designed and built. Accordingly, purchaser has decided to establish a city wide network backbone infrastructure that shall act as the backbone for effective implementation of smart city initiatives across city of Nagpur.

The provisioned network backbone infrastructure shall be designed in a manner which shall be capable to carry all the key services that shall be implemented in due course under smart city initiatives. The purchaser wishes to implement a dedicated and secure fiber network backbone to be established across Nagpur city.

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

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

The network backbone is expected to help Nagpur build a converged network, bringing together different city management vertical solutions on a single foundational network infrastructure. The converged network shall facilitate information exchange between resources and applications across different domains. It is proposed to be an end-to-end platform enabling delivery of varied services for citizens. Key objectives envisaged are to provide:

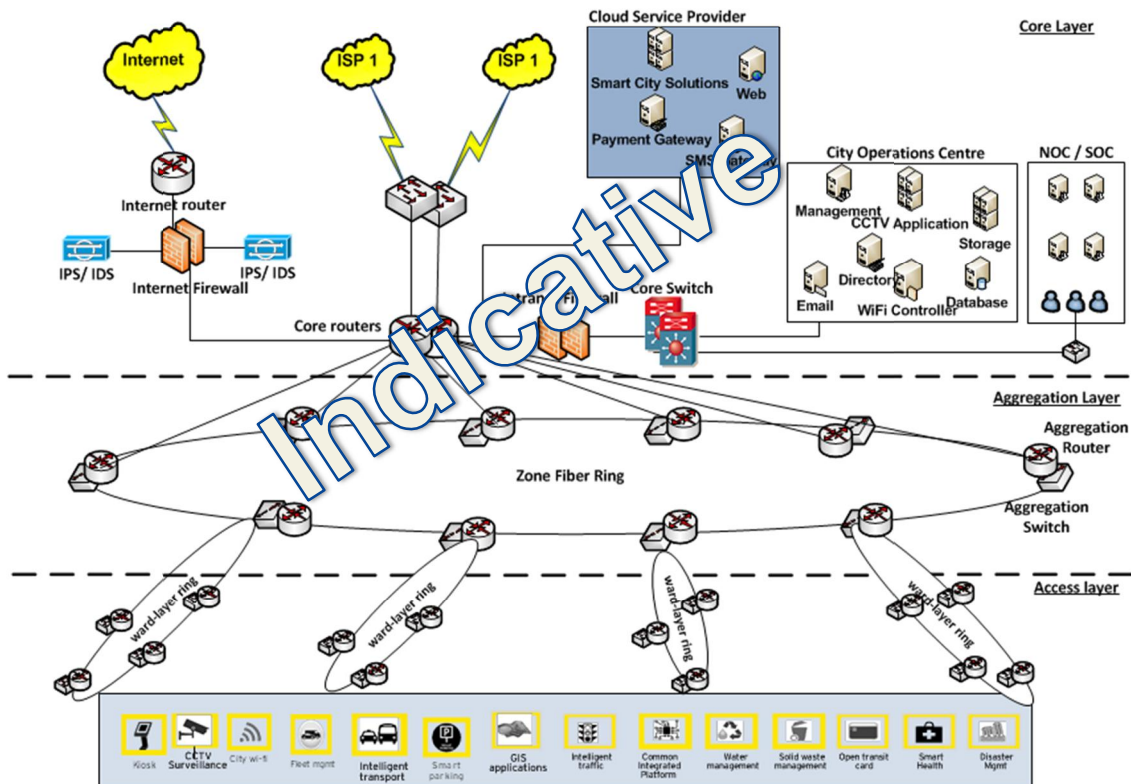
- a. IP connectivity that shall enable the citizens to avail varied services under smart city initiatives
- b. Wired and wireless, scalable, and highly secure network platform
- c. Data management framework to help enable data collection, organization, and sharing
- d. Adoption and usage of distributed compute and storage services, location services, and security services

## 1.1.2. Solution requirements

### 1.1.2.1. Functional design

The overall functional design of network backbone is indicative in nature and is envisaged to be implemented in a three tiered architecture as depicted below.

The 3-tier architecture as below is indicative and the SI is required to prepare its own architecture in the technical bid.



The envisaged layers of the City Network Backbone are:

- Core Layer:** The Core layer forms the backbone of the entire network which consists of Compute, storage, application, links and connectivity to be established at the City Operations Centre. This layer shall enable all applications hosted at City Operations Centre to be accessed over the backbone for consumers and users. Core layer shall form the point of aggregation for all the traffic coming from the Zone layer and beyond.
- Aggregation Layer – Zone Level:** The aggregation layer is envisaged at Zone level. The traffic coming from respective wards shall get aggregated at the Zone level. Ring architecture is proposed to be formed to establish the required redundancy. The aggregation layer shall further connect to the Core layer for forwarding the traffic to the Core layer.
- Access Layer –Ward Level:** The Access layer shall be formed at the wards of NMC. All the wards in the respective zone shall form individual rings to establish redundancy.

There can be multiple rings within the respective zone. e.g. if there are 10 wards in a given zone, then two rings comprising of 5 wards each can be created. These two rings shall ultimately connect to the respective zone (PoP). The access layer shall enable the smart city solutions to connect to the network backbone. The aggregation switch of the respective smart city solution shall tap on the respective access layer devices.

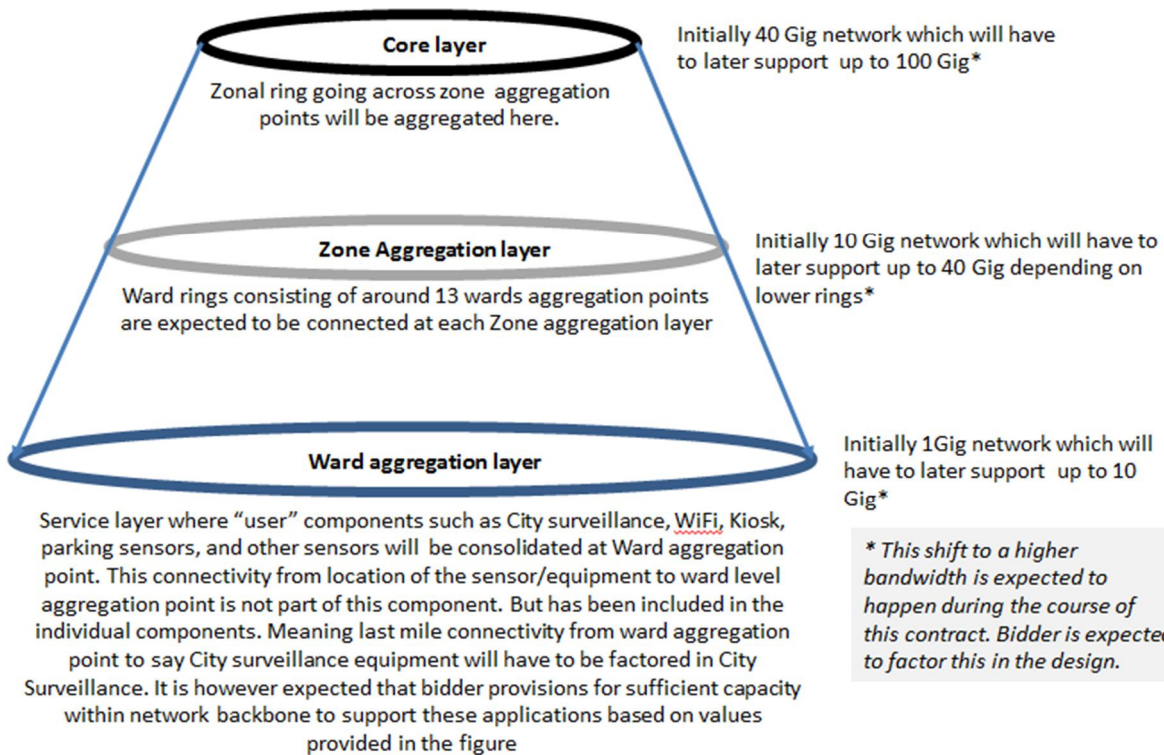
- d. **Services Layer – Smart City Solution Level:** The Service layer shall be formed at various locations within the wards of NMC. The service layer shall enable the smart city solutions such as City Surveillance, City WiFi, City Kiosk, Street lighting, Smart parking, etc. to connect to the network backbone. The aggregation switch of the respective smart city solution shall connect on the Access layer devices to connect to the network backbone.

Various locations for deployment of above layers:

#	Item	Deployment location
1	Core layer	At NMC head office
2	Aggregation layer	Identified aggregation point as mentioned in ANNEXURE V. These are mostly NMC zonal offices and tentatively identified government office buildings.  A Minimum of 10 such aggregation points are being considered. SI may estimate and propose the number of aggregation points.
3	Access layer	Aggregation points to be identified by SI based on network load and geographical coverage.  A Minimum of 10 rings for access layers to be considered by SI. These may overlap in order to provide required redundancy.
4	Services layer	The services layer is considered to be the edge locations/area where the smart city solutions shall be deployed like: <ul style="list-style-type: none"> <li>• City WiFi</li> <li>• City Surveillance</li> <li>• City Kiosk</li> <li>• “Smart Strip”</li> </ul>



Below diagram provides in brief the overall network requirements:



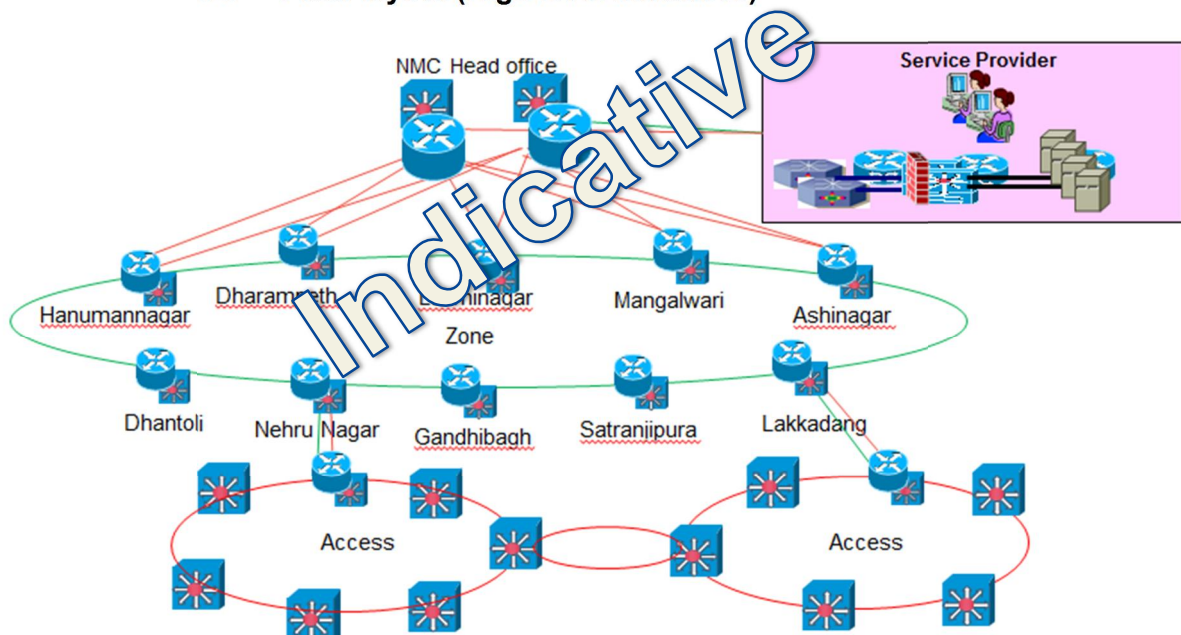
Key services which shall be provisioned under various layers:

1. Monitoring and Management – The management and monitoring layer shall be provisioned centrally from core layer. Centralized management of infrastructure resources shall be implemented in core, aggregation layer, zonal layer and ward layer. All key services that shall be provisioned for the users such as –
  - a. City Wi-Fi
  - b. CCTV surveillance
  - c. City Kiosk
  - d. “Smart Strip”
  - e. All other Smart City initiatives
2. Network Operation Center (NOC): The NOC shall consist of two layered:
  - a. Core layer: This shall monitor all the infrastructure devices (Router, switches, firewall, bandwidth etc.) that are kept in core layer, aggregation layer along with key services that shall be provisioned in due course
  - b. Aggregation layer: The aggregation layer shall help in monitoring the issues related to fiber, network, infrastructure implemented at zone layer and ward layer
3. Configuration and change management: Configuration shall be managed from core layer for all the devices on the network
4. The proposed solution shall be scalable in nature to host all key services under smart city
5. The proposed solution shall have redundancy built at each layer
6. The proposed solution shall be capable to allow enough redundancy built at fiber as

well as at infrastructure level

7. The proposed solution shall be ready to scale up both horizontally and vertically
8. The proposed solution shall be ready in all respect where it is envisaged by NMC to make use of this infrastructure under different revenue models under its long term vision.
9. The solution shall meet demands of bandwidth needs for all the procured and planned smart city solutions
10. The solution shall easily integrate with WiFi subsystem that shall be connected on the same backbone infrastructure.
11. The solution shall be ready in all aspects to host FTTX model in near future to provide voice, video and data services over fiber

#### 1.1.2.2. Fiber layout (High level Indicative)



Fiber backbone infrastructure is an important component of the entire smart city initiative that shall enable the delivery of all the key and important services to be made available to its citizens with seamless access. Network backbone infrastructure shall comprise of dark fiber, setting of various point of presence (PoP) that shall be established across city and cover all zones and wards. The fiber shall be further utilized at access / ward layer for services to be enabled as and when required.

Key requirements that need to be fulfilled by the SI while carrying the activities are provided as below:

#### 1. Route Survey & Network Design Preparation:

- a. The SI shall prepare the route map & network design and submit the final route maps and network design to the purchaser.
- b. The SI are advised to make a detailed survey and familiarize themselves with the soil and terrain so that the rates quoted takes all factors into consideration.

#### 2. Fiber Implementation:

- a. Supply, delivery to site, unloading, storing and handling of 24 Core Fiber drums along with fittings and associated items as required.

- b. All fittings, accessories and associated works for proper and safe installation of fiber assets to be taken into consideration by the SI
- c. Laying, jointing, live line installation, testing and commissioning of all optical fiber and its accessories
- d. Training of Engineers / linesmen, both in supplier's premises and at site, in the installation, operation and maintenance of the optical fiber cables.
- e. The estimated fiber optic cable length requirements are indicated in the Bill of Material (BoM) and reflected in the Price Schedule.

Note: The SI shall be paid for the actual quantity supplied and installed at site. The measurement for quantity to be paid shall be based on horizontal route length of the optical fibre cable (OFC) laid and the price quoted by the SI.

### **3. Core Backbone**

- a. The core backbone shall be established using 24 Core Optical Fiber Cables.
- b. The core architecture shall be established maintaining high level of redundancy and no single point of failure
- c. Two cores in each laid OFC shall be redundant for future scalability and maintenance activity.
- d. The maximum fiber distance between Core and Zone layer shall not exceed 8 Kms or beyond.
- e. Adequate loop of 10 to 15 meters of OFC shall be kept loose on junctions wherever applicable.
- f. There shall not be more than one Splice, Joint closures installed between two (2) locations, during hand over of Network to Purchaser.
- g. All the 24 cores shall be spliced & joined in the Core Backbone.
- h. The colour code shall be uniformly followed across the Core ring, zonal aggregation ring & ward ring.

### **4. Zonal Aggregation Backbone – Ring Topology**

- a. The Aggregation rings shall be established using 24 Core Optical Fiber Cables.
- b. The Zonal Aggregation architecture shall be formed using ring topology.
- c. Two of the cores in each OFC shall be redundant for future scalability and maintenance activity. These two spare cores at Zonal Aggregation Backbone shall not be used for any other purpose apart from the stated.
- d. Adequate loop of 10 meters of OFC shall be left on junction wherever applicable.
- e. There shall not be more than one Splice Joint closures installed between two aggregations points during hand over of Network to Purchaser.
- f. All the 24 cores shall be spliced & joined in the Zonal Aggregation Backbone ring.
- g. The maximum fiber distance between Zone layer shall not exceed 12 Kms

### **5. Ward (Access) Backbone – Ring Topology**

- a. The Ward rings shall be constructed using 24 Core Optical Fiber Cables.
- b. Multiple Ward rings shall be created for the zones that ward is falling under for eg. If there are 10 wards in a zone, two rings of 5 wards shall be created.
- c. The Ward Aggregation architecture shall be formed using ring topology.

- d. Two cores in each OFC shall be redundant for future scalability and maintenance activity and these cores at the Ward Backbone ring shall not be used for any other purpose apart from the stated.
- e. Adequate loop of 10 to 15 meters of OFC shall be left on junction wherever applicable.
- f. There shall not be more than one Splice Joint closures installed between two aggregations points during hand over of Network to Purchaser.
- g. All the 24 cores shall be spliced & joined in the Ward Backbone ring.
- h. The access layer shall be extended using the lit fiber which shall be used to allow all the key services to pass through the network backbone. The access point, CCTV surveillance system etc. shall be plugged into lit fiber to enable the services for users.

### **1.1.3. Scope of Work**

#### **1.1.3.1. Planning and designing of Network backbone architecture**

##### **1.1.3.1.1. Site survey and studying of available infrastructure**

- a. SI shall carry out site survey of locations as identified for implementing various smart city initiatives mentioned in the RFP and also potential locations for future initiatives based on discussion with relevant stakeholders.
- b. NMC owns approximately 550 km duct across the city. SI is expected to study existing fiber duct provisioned for NMC across various locations, available in hard copy contracts and prepare implementation / drawings for every location under this scope.
- c. List of NMC zone offices have been included.
  - i. In order to optimize the existing infrastructure facilities and to ensure cost effective project execution, it is necessary to scan the building at the NMC zone offices where the OFC can be terminated along with relevant IT equipment's. For this purpose, the following order of preference shall be followed :-
    - Housing of the optic fiber equipment in NMC zone office building
    - Housing of the optic fiber equipment in government owned building
    - Housing of the optic fiber equipment in privately owned premises on wayside (these locations have to be approved by NMC)
    - Route through which the fiber cable shall run through the building in a secure manner
  - ii. However, the recourse to utilize any of the above mentioned alternative shall be made subject to the following :-
    - Expenditure on addition/alternation necessary to make the room suitable for housing the optic fiber equipment shall be much less than cost of construction of new rooms at the appropriate site for Optic fiber equipment.
    - The total area shall be sufficient to accommodate the layout required.
    - The location of building to be considered in a manner which is close to the cable route to avoid extra cable length.
    - Power supply is made available and preferably standby power is also available.
    - The site shall be higher than highest flood level of that place.

- iii. In case the existing building for wayside location is not available, a new optic fiber equipment building for wayside location shall be decided with the following considerations.
  - Site shall be close to the key locations identified for smart city initiatives.
  - Staff quarters and other residential building/restaurants, tea stalls shall not be close by
  - Site shall be at an appropriate ground level
  - Site in between roads to be avoided
  - Preferably the site shall be on the same side of the road as the route of optic fiber cable
  - Consideration for road access to site
  - Sufficient open space is available for storage of the equipment
  - Security of the equipment shall be the ownership of the SI at the respective site.
- d. Ground Probing Radar (GPR) may be used to identify the cable duct path and the proposed aggregation points.
- e. For maintenance purposes, 5% additional pipe provision may be considered for estimation.
- f. Indicative measurement of lengths of cable route along with the details of rail / road crossings, culverts, causeways etc. may be recorded in the detailed survey register. The probable location of joints, terminations and leading-in may also be decided and marked on the road map.
- g. Based on the assessment undertaken, SI shall undertake a detailed and comprehensive network architecture development of the entire Smart City solution covering all the locations in Nagpur, IT and physical infrastructure in line with the overall objective and requirements of the project. SI shall identify the space required for setting up the network infrastructure at each of the location.
- h. SI shall be required to undertake the GIS based survey to design the OFC route planning and network topology and share the same with the purchaser. SI can make use of the publicly available data and tools such as Google Maps, ArcGIS, NIC developed maps etc.
- i. The network architecture development exercise shall cause development of the following:
  - i. Detailed WAN and Network architecture covering all locations
  - ii. Detailed Fiber layout along with details of fiber to be laid by using existing NMC fiber ducts or by laying new Fiber ducts
  - iii. Detailed Network solution and deployment architecture covering the central infrastructure at Central Command Centre, City Operations Centre, IT architecture for City Surveillance, City WiFi, City Kiosk, "Smart Strip" etc.
  - iv. Solution required for managing / monitoring the complete Network Backbone.
  - v. Detailed information security architecture to ensure data privacy as well as security
- j. SI shall prepare a Network architecture that includes all of the above along with other design elements like data standards, technology standards, interoperability standards, security architecture and other such guidelines / standards as shall be required for developing a state of the art Smart City solution. This shall be prepared in active consultation with purchaser.

- k. SI shall factor inclusion of various Govt. offices and their location, bandwidth requirements, security, LAN/WAN protocols, network topology for each of the Smart City solution its utilization and allocation of bandwidth etc. shall be taken care of at the time of designing the overall network architecture.
- l. SI shall also consider the terrain, topography, climatic conditions etc. while designing the network architecture.
- m. The Network Architecture once approved shall be base lined either in part or in whole and the purchaser shall institutionalize the processes for Architecture Change management to undertake any change in the respective location, as required during the contract phase.
- n. The roles and responsibilities of the SI team to undertake this work during the contract period shall be clearly defined for the duration of the contract period.
- o. Designing IP Address Schema
  - i. The SI shall design suitable IP Schema for the entire Network Backbone including Central Command Centre, City Operations Centre, Zone offices, ward locations, smart city solutions and interfaces to external systems/ network. The SI shall ensure efficient traffic routing irrespective of link medium.
  - ii. The SI shall maintain the IP Schema with required modifications from time to time within the scope of the project.

#### **1.1.3.1.2. Preliminary fiber route survey**

- a. Preliminary survey shall be carried out for finalizing the drawing for the route of optical fiber cable as part of project planning and execution. Following main items of work shall constitute this survey:
- b. Selecting the route in general
- c. Deciding the number of drop and insert locations
- d. Deciding the size and assessing the length of cable required
- e. Working out the requirement of circuits that are to be provided in the cable
- f. Working out the requirements of heavy tools and plants depending upon nature of the territory, availability of roads alongside etc.
- g. Assessing the special problems of the section such as type of soil, long cuttings, new embankments, water logged areas, types of major bridges, major yards
- h. Collecting details of the existing telecommunication facilities and the additional requirements due to electrification and preparing tentative tapping diagrams
- i. Assessing the number of road crossings and other protective works required to be done
- j. Avoiding as far as possible laying of cable too close to a newly built road
- k. Avoiding the toe of the embankment adjacent to the cultivated fields
- l. Avoiding burrow pits and areas prone to water logging
- m. Avoiding heavily fertilized soils containing acids, electrolytes and decomposable organic materials promoting bacterial activity
- n. Avoiding proximity to chemical, paper and such other industries which discharge chemically active affluent
- o. Avoiding large rock cuttings, routes of existing cables and areas difficult to approach
- p. Deciding carefully the cable route approaches to cable huts to avoid built up areas including those areas where building, etc. are likely to come up in future

- q. Determining composition of the soil which may affect corrosion, etc. on the cable and special protection required for cable
- r. Working out requirement of transport vehicles like jeeps, lorries, motor trolleys, etc. for execution of the work
- s. Avoiding side of the alignment which is likely to be affected due to addition/alteration of earth work/supply structures

#### **1.1.3.1.3. Preparation of cable route plan and tapping diagrams**

The cable route plan shall indicate the route with respect to the main road, that is, whether the route along the main road is on both side and right side of the main road when facing a particular direction in case of single line section.

#### **1.1.3.1.4. Selection of the Cable Route**

Generally the terrain conditions on the two sides of the road vary to such an extent that the cable route on one side of the road has a distinct advantage over that on the other side. While operating on the principle, it shall be borne in mind that frequent track crossings are not desirable.

In addition to the above, the following also need consideration:

- a. Avoiding underground structures, signalling cables, power cables, pipe lines, etc.
- b. Avoiding laying of cable on the side of the drains in built up areas which are generally difficult to lay
- c. Taking the cable route preferably through the bed of small culverts where water does not accumulate instead of taking it over the culverts
- d. Avoiding termites/rodents infected areas
- e. Identification of site locations for zone and ward level aggregation points
- f. SI shall assist NMC in preparing the MoU's with respective Govt. departments, Municipalities for using space for identified zone and ward level aggregation points

#### **1.1.3.2. Fiber laying**

- a. SI shall employ industry leading practices for laying of fiber for existing NMC owned ducts and new ducts.
- b. It shall be the responsibility of SI to get all the necessary permission(s) for fiber laying including the Right of Way. NMC shall provide all the necessary support for getting such permissions.
- c. Before carrying out the actual fiber/duct laying process, the SI is encouraged to carry out a detailed survey based on the outcomes of the preliminary survey carried out earlier. The purpose of the detailed survey is to undertake closer study of various existing telecommunication facilities to work out exact requirement of materials required for different items of work to finalize all the drawings and site plans required for the execution of work as also to examine the details collected during preliminary survey and to offer necessary changes/modifications, if any.
- d. The following are the main items of work that shall constitute the detailed survey:
  - i. Closely examining the proposed cable route and prepared cable route plans
  - ii. Siting of cable hut buildings and preparation of site plans

- iii. Siting and preparation of site plans for buildings required for the execution of the work, as offices at different stations, store go-downs
- iv. Siting of areas for loading/unloading of cable drums and siding facilities for the EMVs (Engineering Materials Vehicles) for the project
- v. Preparation of the material schedule required for different protective works
- vi. Arranging isolated components circuits to be provided in the cable
- vii. Investigation of special problems, if any, of the section and finding out proposed solution thereof
- e. On Ducted Routes: Optical fiber cables may be laid through the existing ducts wherever the concrete ducts are available. As far as possible the cable may be diverted to the new ducts laid subsequently. When the cables are laid in ducts, no particular depth is prescribed. End of the ducts shall be properly sealed and necessary protection by way of W.I. pipe / RCC pipe shall be provided at the entry and exit of the duct till the cable is buried to a depth of 1.5 m. The above is applicable in town or any other ducts laid cross country
- f. On Non-Ducts Routes: PLB pipe laying shall be done as per the approved detailed survey report
- g. SI is expected to put in practices for precaution against damage by Termites & Rodents. In the rodent prone areas, Optical Fiber cable joint closures shall be applied with BHC 10% dust (Benzene Hydro chloride 10%) to prevent rodent & termite damage. The method suggested is "BHC" 10% dust of 1 kg shall be mixed in an approximate 2 kg of sand and applied around the optical fiber cable joint enclosures
- h. Cable laying is proposed either by traditional Cable pulling method or by Cable blowing method
- i. To reduce the friction between the cable and HDPE, a suitable lubricant may be continuously applied with a sponge to the cable surface during pulling. The standard lubricants with low frictional coefficient may be used. User of Telecom Duct may be adopted. Telecom Duct is an advanced pre-lubricated duct system. Lubricants are built in to a durable polymer base. Duct has a low coefficient of friction and the built in lubricants do not diminish with age. SI is expected to choose the industry leading practices while carrying out the mentioned tasks.
- j. Following types of techniques shall be used for splicing of fibers:-
  - i. Mechanical Splice - This is done by aligning the axis of the two fibers to be joined and physically hold them together.
  - ii. Fusion Splicing - This is done by applying localized heating (i.e. by electric arc or flame) at the interface between the butted, pre-aligned fiber end, causing them to soften and fuse together.
- k. Mechanical splicing shall be used for temporary splicing of fibers or where fusion splicing is impractical or undesirable.
- l. At all other location and during initial installation of optic fiber cable, fusion splicing shall be adopted.
- m. Purchaser may choose to carry out an acceptance test for fiber that has been laid. In either case, SI is expected to carry out an independent review of the fiber/duct that has been laid for the purpose of creating network backbone. Such inspection reports shall be submitted as supporting documents while raising invoices. Purchaser may ask the SI to carry out this sample test from a third party agency. Cost of such test shall be borne by the SI.



- n. In case any deficiencies are observed in the laying of fiber/duct by SI, SI is expected to promptly correct the same at no extra cost to the purchaser
- o. For attending faults, etc. special kits shall be used for opening of the joint
- p. SI shall be liable to pay any penalties imposed while carrying out work. Purchaser or any of its representatives shall have no liability arising from penalties including but not limited to penalties for causing inconvenience to the public, penalty for cutting/damaging the old cable of NMC or other providers, penalty for damaging any other utilities, among others
- q. Termination joint for optic fiber cable is provided in the cable hut for terminating the outdoor optic fiber cable of both the sides, splicing through fibers, connecting fibers to pigtails for connection to optical line terminal equipment, etc. SI shall choose appropriate procedure for installation of termination joint box based on the type of joint enclosure. The installation manual shall contain the step by step procedure for installation.
- r. After the cable is laid and splicing is complete, measurements in the below proforma shall have to be prepared and maintained.

Section		Distance	Cable length	Fiber No	Loss in dB		Remarks
From	To				1310nm	1550nm	

The end to end loss shall not exceed 0.25db/Km at 1550 nm and 0.40 db/Km at 1310 nm

### 1.1.3.3. Network backbone infrastructure management

#### 1.1.3.3.1. Commencing network backbone infrastructure management including handover to purchaser and maintenance team

List of items to be handed over to purchaser / designated authority before handing over the respective section / location for maintenance of optical fiber communication system

- a. The Cable Route Plan in electronic form (in kml file format on a CD) preferably using AUTOCAD and Google maps. Distances from fixed reference structures like centre of track, OHE mast, bridges, culverts, etc. shall be indicated in the route plan for easy reference in future.
- b. The Fiber Distribution Plan
- c. Measurements of Optical Parameters that includes sectional losses splice wise losses, records of dispersion measurements (in case of long haul systems) shall be handed over to the maintenance organization.
- d. SI shall prepare maintenance schedule for fiber optic system. Reports on adherence to the maintenance schedule shall be submitted as part of SLA compliance along with

quarterly invoices. This maintenance which shall include but not be limited to following areas:

- iii. Power supply equipment
  - Main. of Charger and In/Out voltages and currents
  - Checking of fuses and terminations
  - Check of Earthing
- iv. Optical fiber cable
- v. Cable route
  - Integrity of cable route
  - Protective works on bridges & culverts
  - Cable route markers
  - Earthing of sheath of cable
- vi. Periodical line-up consisting of
  - Tx/Rx optical power
  - Pulse mask for all digital interfaces
  - G821/G823 tests on 64KBPS/2MBPS for 10 days
  - Loss measurement with optical source & power meter
  - Measurement of order wire performance circuits.

#### **1.1.3.3.2. NOC operations**

The SI shall ensure adherence to the following prerequisites:

- a. All the devices that are installed by the SI shall be Simple Network Management Protocol ('SNMP') enabled and the SI shall centrally and remotely monitor and manage the devices on a 24x7x365 basis.
- b. SI shall provide on-site comprehensive maintenance of the entire IT / Non-IT Infrastructure and their components supplied with a provision of onsite spares on 24x7x365 basis after successful execution and acceptance by purchaser.
- c. SI shall operate and maintain the Network infrastructure (Active / Passive / Physical) as per well-defined Standard Operating Procedures.
- d. SI to establish and implement leading practices of IT service Management like Information Technology Infrastructure Library (ITIL), International Organization for Standardization (ISO)/IEC 20000 standard that shall promote the adoption of an integrated approach to effectively deliver managed services to meet the requirements of purchaser.
- e. SI shall identify all assets and document the importance of these assets. The asset inventory shall include all the information necessary in order to recover from a disaster, including type of assets, format, location, backup information, license information etc.
- f. SI shall undertake scheduled and ad hoc maintenance (on need basis) and operations like configuration backup, patch management and upgrades
- g. SI shall establish basic tools for IT management to undertake health check monitoring, troubleshooting etc. for all Network operations
- h. SI shall establish access control mechanism and shift wise attendance management system

- i. The system spare parts/ services as and when required and complete maintenance of the system in future shall be supported for a period of not less than the contract duration from the date of acceptance of the system / Go Live.
- j. The SI shall ensure that all resident engineers are certified (of the OEMs of the network components) and are provided at City Operations Centre for 24/7 operations.
- k. Typical Network Infrastructure Management Services at all locations shall include:
  - i. SI shall ensure that the network is available 24x7x365 as per the prescribed SLAs
  - ii. SI shall provide services for management of network environment to maintain performance at optimum levels.
  - iii. SI shall be responsible for attending to and resolving network failures and snags
  - iv. SI shall support and maintain overall network infrastructure including but not limited to MAN/LAN passive components, routers, switches, Firewalls', IPS/IDS, Load Balancers etc.
  - v. SI shall Configure and backup network devices including documentation of all configurations
  - vi. SI shall provide information on performance of Ethernet segments, including capacity utilization and error statistics for the segment and the top-contributing hosts, MAN / WAN links and routers
  - vii. SI shall create required facilities for providing network administration services including administrative support for user registration, creating and maintaining user profiles, granting user access and authorization, providing ongoing user password support, announcing and providing networking services for users.
  - viii. SI shall provide a single-point-of-contact for requesting any service. The Network Administrator shall respond to the initial request from the user groups within the agreed service levels and service coverage hours.
  - ix. SI shall provide support as required to assist in hardware and software problem isolation and resolution in the LAN/WAN/MAN environment.
  - x. SI shall perform LAN/WAN/MAN problem determination.
  - xi. SI shall communicate changes affecting the LAN/WAN/MAN environment.
  - xii. SI shall maintain LAN/WAN and MAN configuration data.
  - xiii. SI shall be responsible for polling / collecting of network devices security logs from all the systems. All these logs shall be made available to the Enterprise Management System (EMS) solution
  - xiv. SI shall ensure smooth routing of network traffic to the envisaged DC/DR site in case of disaster / drill.
- l. Security Administration and Management Services:
  - i. Management of security environment of the entire network infrastructure to maintain performance at optimum levels.
  - ii. Address ongoing needs of security management including, but not limited to, monitoring of various devices / tools such as firewall, intrusion detection, content filtering and blocking, and vulnerability protection through implementation of proper patches and rules.
  - iii. Maintain an updated knowledge base of all the published security vulnerabilities and virus threats for related software and microcode, including, but not limited to, operating systems, security solutions, network solutions, etc.
  - iv. Ensure that patches / workarounds for identified vulnerabilities are patched / blocked immediately.

- v. Respond to security breaches or other security incidents and coordinate with respective OEM in case of a new threat is observed to ensure that workaround / patch is made available for the same.
- vi. Maintenance and management of security devices, including, but not limited to maintaining firewall services to restrict network protocols and traffic, detecting intrusions or unauthorized access to networks, systems, services, applications or data, firewalls, servers, desktops from viruses.
- vii. Operating system hardening through appropriate configuration and patch updates on a regular basis.
- viii. Physical & Environmental Security at locations
- ix. Ensure that all network hubs and switches (including already available equipment) are secured and are enabled only when required by authorized employees.
- x. Perform reactive and preventive maintenance exercise
- xi. Monitor the environmental controls for security of network equipment, cabling security and IT hardware management.
- xii. Ensuring that the security policy is maintained and updates to the same are made regularly as per ISO 27001, BS 7799 and BS 15000 guidelines.

#### **1.1.3.4. Other expectations from SI**

1. SI shall engage early in active consultations with DIT GoM, NMC, Nagpur 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.
2. Study the existing fiber duct layout and existing network to understand the existing technology adopted in each of the following areas (not limited to):
  - i. City WiFi
  - ii. Surveillance Infrastructure – CCTV Cameras, Data communication, monitoring, control room and Infrastructure
  - iii. City Kiosk
  - iv. “Smart Strip”Other Smart City initiatives envisaged
3. SI shall assess existing infrastructure’s current ability to support the entire solution and integrate the same with the proposed solution wherever applicable and possible
4. SI shall judiciously evaluate the resources and time planned for undertaking the current state assessment, given the overall timelines and milestones of the project.
5. SI shall be responsible for supply of all the Products/equipment such as optical fiber cable, Network, Hardware, Software, Devices, etc. as specified in the Bill of Materials included in the RFP and their appropriate quantity & capacity. This shall meet the technical Specifications as per the Network Backbone design approved by purchaser.
6. SI shall be responsible for supply of passive components specified in the Bill of Materials section of the RFP viz. Housings, Fiber Patch Cords, Racks etc. Civil work required for the site shall be undertaken by the SI.
7. Validate / Assess the re-use of the existing infrastructure if any at NMC site
8. Supply, Installation, and Commissioning of entire solution at all the locations.
9. SI shall provide the bandwidth required for operationalizing each smart city initiative till the time purchaser’s own fiber is laid by the SI as part of the scope of

- work of this RFP. The bandwidth requirement shall be analysed and procured by the SI at its own cost / risk.
10. SI shall Install and commission connectivity across NMC HO, Zonal office, Ward locations, Central Command Centre, City Operations Centre, etc.
  11. SI shall establish high availability, reliability and redundancy of the network elements to meet the Service Level requirements.
  12. SI shall be responsible for planning and design of the access network architecture (access controllers, backhaul connectivity, routers, switches, etc.) to meet the technical, capacity and service requirements for all smart city initiatives.
  13. SI shall be responsible for upgradation, enhancement and provisioning additional supplies of network (including active / passive components), hardware, software, etc. as requisitioned by purchaser.
  14. SI shall ensure that the infrastructure provided under the project shall not have an end of life within 24 months of signing the contract or within 12 months of acceptance of the infrastructure, whichever is later.
  15. SI shall ensure that the end of support is not reached during the concurrency of the contract
  16. SI shall ensure compliance to all mandatory government regulations as amended from time to time.
  17. The SI shall ensure that all the peripherals, accessories, sub-components required for the functionality and completeness of the solution, including but not limited to devices, equipment, accessories, patch cords (fiber), cables, software, licenses, tools, etc. are provided according to the requirements of the solution.
  18. NMC shall not be responsible if the SI has not provisioned some components, sub-components, assemblies, sub-assemblies as part of Bill of Materials in the RFP. The SI shall have to provision these & other similar things to meet the solution requirements at no additional cost and time implications to purchaser.
  19. All the software licenses that the SI proposes shall be perpetual software licenses along with maintenance, upgrades and updates for the currency of the contract. The software licenses shall not be restricted based on location and purchaser shall have the flexibility to use the software licenses for other requirements if required.
  20. The SI shall ensure there is a 24x7 comprehensive onsite support arrangement for duration of the contract with all the OEMs for respective components. The SI shall ensure that all the Original Equipment Manufacturers have an understanding of the service levels required by purchaser. SI is required to provide the necessary back-to-back contract agreements with the OEMs as part of the scope for technical evaluation.
  21. Considering the criticality of the infrastructure, SI is expected to design the solution considering the RFP requirement of no single point of failure with high level of redundancy and resilience to meet the network uptime requirements.
  22. SI shall be responsible for periodic updates & upgrades of all equipment, cabling and connectivity provided at all locations during the contract period.
  23. SI shall be responsible for setting up / building / renovating the necessary physical infrastructure including provisioning for network, power, rack, etc. at all the locations.
  24. SI is expected to provide following services, including but not limited to:
    - i. Provisioning hardware and network components of the solution, in line with the proposed NMC requirements

- ii. Size and propose for network devices (like Router, switches, security equipment including firewalls, IPS / IDS, IPSec routers, etc. as per the location requirements with the required components/modules, considering redundancy and load balancing in line with RFP.
- iii. Provide warranty for all the IT / Non-IT hardware assets procured to comply with the requirements of this RFP.
- iv. Size and provision the WAN bandwidth requirements across all locations considering the application performance, data transfer, DR and other requirements for smart city initiatives.
- v. Size and provision the internet connectivity for Service Provider network and Network Backbone.
- vi. Size and provision for bandwidth as a service for operations of City WiFi, City Kiosk, CCTV surveillance and “Smart Strip” till operationalization of network backbone
- vii. Liaise with service providers for commissioning and maintenance of the links.
- viii. Furnish a schedule of delivery of all Central IT/Non-IT Infrastructure items
- ix. All equipment proposed as part of this RFP shall be rack mountable.
- x. NMC may at its sole discretion evaluate the hardware sizing document. SI needs to provide necessary explanation for sizing to the purchaser
- xi. Complete hardware sizing for the complete scope with provision for upgrade
- xii. Specifying the number and configuration of the racks (size, power, etc.) that shall be required at all the locations.
- xiii. The SI shall provide for all required features like support for multiple routing protocols, congestion management mechanisms and Quality of Service support.
- xiv. The SI shall ensure that all active equipment (components) are Simple Network Management Protocol (SNMP) V3 compliant and are be available for maintenance/management through SNMP from the date of installation by a Network Monitoring System.

## **1.2. SOLUTION 2 – Nagpur City WiFi**

### **1.2.1. Overview**

In a society with a high demand for digital connectivity “on the move”, there is an increasing demand for public WiFi services to be made widely available. Understanding this need, purchaser intends to provide public Wi-Fi services at identified locations across Nagpur city. These locations shall include Market Places, Government Offices, Recreation Spots such parks & lakes, Educational Institutes, Holy places etc.

The citywide public WiFi shall leverage City Network Backbone (which shall be made available across Nagpur city). The SI shall extend the last mile connectivity through City Network Backbone to City WiFi locations over fiber. The SI shall install access points and lay the fiber cabling at identified locations along with implementation of access points and provide maintenance support to purchaser or its authorized entity. The selection of access points shall be done on the basis of density of users, geographical coverage and in consultation with purchaser or its designated agency.

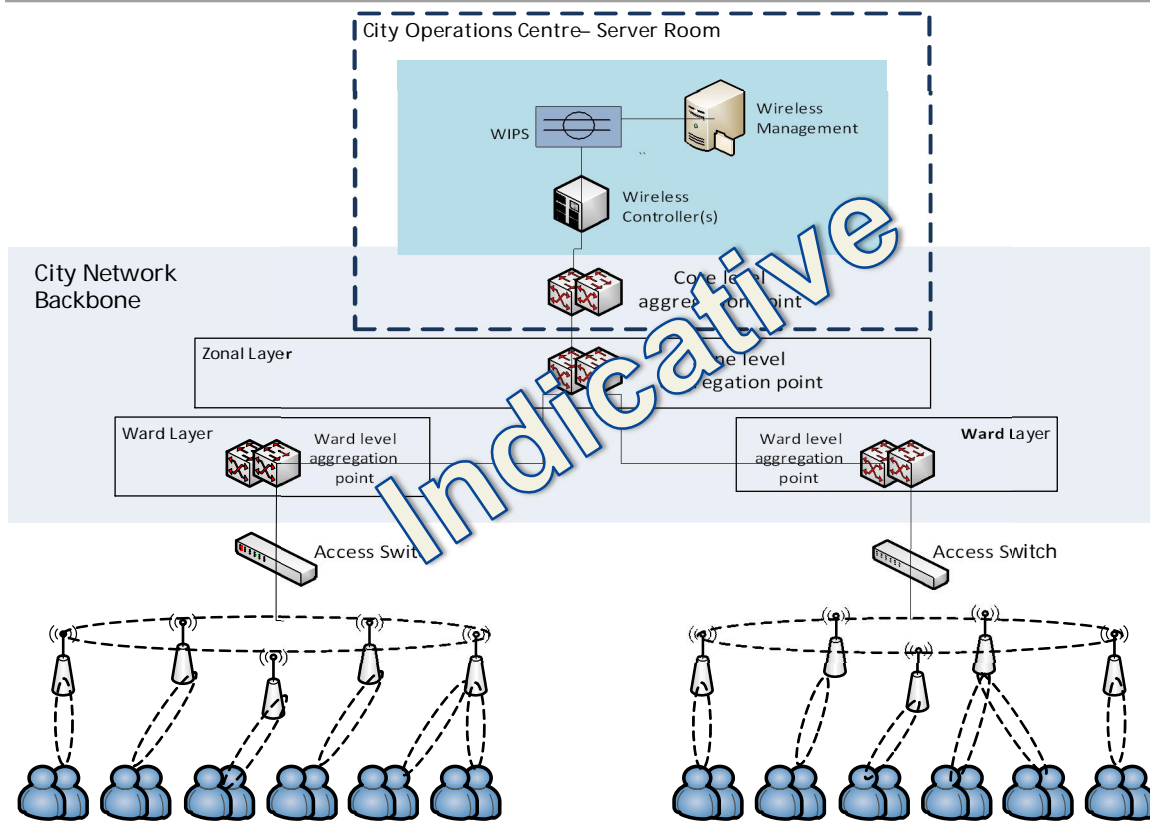
To start with, access points shall be provisioned at identified locations. Based on demand new WiFi locations may be added. The access points shall be implemented in controller based model where access points shall be managed by using wireless controller that shall be positioned at COC server room (NMC-HO). The proposed solution shall include access points and related infrastructure as per specifications mentioned in the RFP. SI is expected to procure bandwidth as a service till the time city network backbone is created.

SI shall conduct the survey and design the Wi-Fi setup at each location to accommodate the users' bandwidth need and requirements. Profiling of users and appropriate policies shall be pushed from COC server room. Wireless controllers shall also be integrated with AAA (Authentication server) to properly manage the policies that may be required for different user types. Access points shall negotiate using SSID with controller. The controllers register the access points and accordingly allow the access point post checking with AAA server.

SI shall supply, install, commission and maintain the access points and related infrastructure as specified in the Bill of Materials within this RFP for the entire duration of contract period. Based on need, SI shall be required to supply additional access points as per the rate quoted in the financial bid.

### **1.2.2. Solution requirements**

The indicative architecture diagram for the City WiFi solution is depicted in the schematic below.



Key expectations from the system include:

- a. The network shall support user devices with 2.4 GHz as well as 5 GHz frequency band at the same time
- b. The City Wi-Fi network should be manageable from a central location at City operations centre through the wireless management system. The management system shall support unified wired and wireless network management.
- c. It shall be possible to configure and manage access points (APs) remotely through a wireless controller.
- d. System shall support multiple VLANs to support users with different privileges.
- e. The system should be designed for scalability and allow future expansions in terms of subsequent project phases, increased user density and geographical coverage.
- f. Data communication between devices shall take place in encrypted form to ensure end-to-end security of user information/ data with requisite security standards.
- g. The system should be designed for multiple authentication mechanisms
- h. The system shall support user authentication and one time OTP based registration, thereafter user shall login through respective username and password.
- i. Every user shall get access to only those services for which they are authorized.
- j. The system should be capable of Rule based Access Rights.
- k. The system should have centralized billing and authentication system wherein profile for each individual user shall be created.
- l. Users shall be able to manage their account by subscribing / renewing the packages on the self-service portal.

The access points may be deployed outdoor or indoor depending on the requirement of the purchaser or its assigned agency. The implementation of these access-points shall be carried



out on the basis of feasibility of access-points at each location and in consultation with purchaser.

### **1.2.3. Scope of Work**

The SI shall be required to carry out following activities:

1. Survey of the defined locations to ascertain number of Access Points and their positioning to ensure maximum coverage and excellent signal strength. This shall be done in consultation with officials assigned by purchaser or its authorized entity
2. Supply, installation, integration, testing, commissioning and maintenance of all products required for enabling 24x7 City WiFi services at identified locations. These include but are not limited to IT, telecom, networking, peripheral hardware and software products and applications.
3. Leverage City Network Backbone infrastructure that is being created for Nagpur city. However, till the time city network backbone is commissioned by the SI, the SI needs to procure bandwidth as a service in order to meet requirements as defined within service level agreement. Purchaser estimates provisioning of City WiFi services at 136 locations across the city with 10 Mbps bandwidth at each AP level. However, in times to come, City WiFi locations may scale up, hence SI needs to provision for the network bandwidth accordingly.
4. Development and implementation of billing and accounting software for e-recharge and accounting for the service revenue.
5. SI shall also be responsible for:
  - a. Providing Technical manpower, for the contract period from the date of acceptance, to look after the day to day management of services related to Wi-Fi facility management. These services shall include:
    - i. Providing connectivity to user devices as per Wi-Fi access policy,
    - ii. Satisfactorily handling all the issues related to connectivity, performance and security.
  - b. Edge or street level network including access network architecture leveraging city network backbone
    - i. Planning and design of the Edge network architecture (access controllers, backhaul connectivity, routers, switches, fiber, junction box, UPS, etc.) to meet the technical, capacity and service requirements.
    - ii. Planning for high availability, reliability and redundancy of the access network elements as per requirements stated in the SLA.
    - iii. Till the time city network backbone is in place, provisioning for bandwidth shall be done on bandwidth as a service model.
  - c. City Wi-Fi Locations
    - i. Purchaser shall be responsible for providing of Access Point locations
    - ii. Commissioning & deployment of WiFi solution
      - a) SI shall be responsible for design and RF planning based on the locations identified by Purchaser.
      - b) SI shall be responsible for installation of Access Points and related equipment at WiFi locations
      - c) SI shall be responsible for providing and executing cabling, testing etc.

- d. SI shall be responsible for design and engineering of all the network components to meet capacity requirements
  - i. Network shall be designed keeping in view the peak load conditions.
- e. Equipment and network upgrades, support and maintenance for the contract period
  - i. SI shall provide local support at each zone for repair and maintenance of all equipment, cabling and connectivity provided at the City WiFi locations
  - ii. SI shall be responsible for periodic updates of all equipment, cabling and connectivity provided at the City WiFi locations
- f. Set up Wi-Fi network across locations proposed in phased manner
- g. Procurement, planning, design, installation, commissioning and support of all end point equipment (IT and non IT) required to set up WiFi locations.
- h. Providing adequate security mechanisms in City WiFi service equipment to prevent unauthorized access or interfaces to services, calls, protocols and data.
- i. Providing complete network diagram including detailed technical documentation, survey, drawing and detailed Project Plan for all the locations mentioned.
- j. City WiFi management: City WiFi setup shall be monitored and managed at core layer. The City WiFi access points shall be provisioned in client server mode where controller of the City WiFi system shall be placed at core layer and all access-points based on the feasibility shall be implemented at ward layer. All the key services available for citizens shall be catered using City WiFi access.
- k. Ensuring compliance with all Regulatory and Legal guidelines issued by Department of Telecommunications, TRAI and Government of India from time to time. At no point purchaser or its authorized entities shall be responsible for any non-compliance on account of non-adherence by the SI.

### 1.3. SOLUTION 3 – Nagpur City Surveillance

#### 1.3.1. Overview

Protecting citizens and ensuring public safety is one of the topmost priorities for any Government agency. It requires advanced security solutions to effectively fight threats from activities of terrorism, organized crime, vandalism, burglary, random acts of violence, and all other forms of crime. CCTV based video surveillance is a security enabler to ensure public safety. Government of Maharashtra, under the smart city initiative, intends to implement a holistic City Surveillance System in City Police Jurisdiction limits in the Nagpur City

##### 1.3.1.1. Nagpur Police

Nagpur City police, headed by the Commissioner of Police, covers entire Nagpur City which is divided into 4 zones and each zone has 6 police stations. Nagpur Rural Police headed by Superintendent of Police covers about 13 tehsils comprising the rural areas of Nagpur. It is subdivided under 6 sub divisional police office (SDPO) divisions with a total of 22 police stations. Following table shows the City & Rural Police areas.

<b>Nagpur Police</b>			
<b>Nagpur City</b>		<b>Nagpur Rural</b>	
<b>Commissioner of Police</b>		<b>Superintendent of Police</b>	
<b>1</b>	<b>Zone 1</b>	<b>1</b>	<b>SDPO NAGPUR DIVISION</b>
<b>I</b>	Sitabuldi	<b>i</b>	Bori
<b>ii</b>	Ambazari	<b>ii</b>	Hingna
<b>iii</b>	MIDC	<b>iii</b>	Bela
<b>iv</b>	Wadi	<b>2</b>	<b>SDPO KAMPTEE DIVISION</b>
<b>V</b>	Sonegaon	<b>i</b>	Kamptee
<b>vi</b>	RP Nagar	<b>ii</b>	Kanhan
<b>2</b>	<b>Zone 2</b>	<b>iii</b>	Mouda
<b>I</b>	Sadar	<b>iv</b>	Khaperkheda
<b>ii</b>	Gittikhadan	<b>3</b>	<b>SDPO KATOL DIVISION</b>
<b>iii</b>	Panchpaoli	<b>i</b>	Katol
<b>iv</b>	Jaripatka	<b>ii</b>	Narkhed
<b>V</b>	Koradi	<b>iii</b>	Kondhali
<b>vi</b>	Mankapur	<b>iv</b>	Jalalkheda
<b>3</b>	<b>Zone 3</b>	<b>4</b>	<b>SDPO UMRED DIVISION</b>
<b>I</b>	Lakadganj	<b>i</b>	Umred
<b>ii</b>	Tahsil	<b>ii</b>	Bhiwapur
<b>iii</b>	Kotwali	<b>iii</b>	Kuhi
<b>iv</b>	Ganeshpeth	<b>iv</b>	Veltur
<b>V</b>	Kalamana	<b>5</b>	<b>SDPO RAMTEK DIVISION</b>
<b>vi</b>	Yashodhara	<b>i</b>	Ramtek
<b>4</b>	<b>Zone 4</b>	<b>ii</b>	Parshivni
<b>I</b>	Ajani	<b>iii</b>	Deolapar
<b>ii</b>	Dhantoli	<b>6</b>	<b>SDPO SAONER DIVISION</b>
<b>iii</b>	Imamwada	<b>i</b>	Saoner
<b>iv</b>	Sakkaradara	<b>ii</b>	Kalmeshwar
<b>V</b>	Nandanwan	<b>iii</b>	Khapa

<b>Nagpur Police</b>			
<b>Nagpur City</b>		<b>Nagpur Rural</b>	
<b>Commissioner of Police</b>		<b>Superintendent of Police</b>	
vi	Hudkeshwar	iv	Killod

In the current context of City Surveillance, the area pertaining to Nagpur City under Police is covered.

### 1.3.1.2. Geographical Spread

Nagpur City Police covers an area of about 446 Sq. km. The following map represents the Geographical spread of the area and zone wise distribution of police jurisdictions. This includes Nagpur Municipal Corporation limits.



### 1.3.2. Solution requirements

The SI shall be responsible for Supply, Installation, Implementation and Operation & Maintenance of Nagpur City Surveillance System for a period of Five Years from the date of Go Live of the respective phase independently. The indicative requirement for SI is broadly categorized into following:

Category	Scope of Work
<b>Surveillance System Infrastructure at field locations</b>	Supply, install, implement and maintain: <ol style="list-style-type: none"> <li>1. PTZ Camera</li> <li>2. Fixed Box Camera</li> <li>3. Dome Cameras</li> <li>4. Thermal Camera</li> </ol> Additional features within above cameras

Category	Scope of Work
	<ol style="list-style-type: none"> <li>1. Camera to support ANPR</li> <li>2. Camera to support RLVD</li> <li>3. Cameras with online FRS</li> </ol> <p>Other components:</p> <ol style="list-style-type: none"> <li>1. Public Announcement System</li> <li>2. Variable Messaging System</li> <li>3. Drone</li> <li>4. Mobile Surveillance Vehicle</li> </ol> <p><b>Data retention period: 30 days</b> Kindly refer Bill of Material for detailed location wise camera distribution</p>
<b>Network Infrastructure</b>	<ol style="list-style-type: none"> <li>1. Between camera &amp; aggregation point – Field location</li> <li>2. Between aggregation points &amp; server room</li> <li>3. Between server room &amp; command control center</li> <li>4. Between server room &amp; viewing/monitoring center</li> <li>5. Between drone ground station / mobile surveillance vehicle &amp; server room</li> </ol> <p>It is envisaged that the system shall leverage City Network Backbone infrastructure that is being created for Nagpur city. However, till the time city network backbone is commissioned, the SI is expected to procure bandwidth as a service in order to meet requirements as defined within service level agreement. The SI is also expected to migrate to the City Network Backbone within a month of operationalization of city backbone.</p>
<b>Server Room</b>	<ol style="list-style-type: none"> <li>1. Supply &amp; installation of IT Infrastructure including server, storage, network components and peripherals to handle 100% load along with provisioning for redundancy</li> <li>2. Supply &amp; installation of Non IT infrastructure like furniture, AC, and interior work etc. excluding civil work at the space provided by the purchaser</li> </ol>
<b>Command Control Center</b>	<ol style="list-style-type: none"> <li>1. Supply &amp; installation of IT &amp; Non IT infrastructure like video wall, workstation, furniture, AC, and interior work etc. excluding civil work at the space provided by purchaser</li> <li>2. Supply &amp; establishment of Mobile Command Control Center</li> </ol>
<b>City Operation Center</b>	<p>City Operation Center establishment at the identified location for viewing and controlling the selected field locations in a fully automated environment including:</p> <ol style="list-style-type: none"> <li>1. Supply &amp; installation of IT &amp; Non IT infrastructure like server, router, video wall, workstation, furniture, AC, and interior work etc. excluding civil work</li> </ol>
<b>Surveillance System Applications</b>	<ol style="list-style-type: none"> <li>1. Video Management System (VMS)</li> <li>2. Video Analytics (VA)</li> <li>3. Red Light Violation Detection (RLVD) System</li> <li>4. Automatic Number Plate Recognition (ANPR) System</li> <li>5. Facial Recognition System (FRS)</li> <li>6. Integrated Operation Platform (IOP)</li> </ol>

<b>Category</b>	<b>Scope of Work</b>
<b>Video feeds at few selected locations</b>	SI is expected to provision for viewing of feeds at selected locations including DCP office and key police stations
<b>Training/Capacity Building</b>	Technical & functional training to the designated officials on a continuous basis

### **1.3.3. Scope of Work:**

#### **1.3.3.1. 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 Nagpur Police Department.

A detailed survey shall be conducted, by the SI along with a team of Purchaser and Nagpur police, at each of the strategic locations. This survey shall finalize the position of all field equipments 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:

1. Cameras (Fixed Box Cameras, PTZ Cameras, ANPR cameras etc.)
2. IR Illuminators
3. Local processing unit for ANPR / RLVD cameras
4. Switches
5. Outdoor Cabinets
6. Pole for cameras / Mast
7. Junction box
8. UPS
9. Networking and power cables and other related infrastructure

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

#### **1.3.3.1.1. Supply & Installation of CCTV Surveillance Infrastructure:**

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

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

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.

#### **1.3.3.1.2. Installation of Poles/Cantilevers/Gantry**

1. The SI 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. SI shall provide appropriate poles & cantilevers and any supporting equipment.
3. SI shall be required to supply, install, configure and integrate surveillance cameras at the identified locations and thereafter undertake necessary work towards their commissioning.
4. SI shall ensure that the poles erected to mount cameras are good, both qualitatively and aesthetically
5. SI shall use the industry leading practices while positioning and mounting the cameras and ensure that the pole / mast implementation is vibration resistant. Arrangements for bird scare spikes on top of camera shall be made to prevent birds from sitting on top of camera box.
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 SI.
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 SI so that there is clear line of sight.
9. SI shall be responsible to undertake required structural analysis regarding the regulated load conditions and considering the respective wind load while installing the poles / cantilevers for Variable Messaging Sign boards
10. SI 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. SI 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. SI shall ensure that physical look of the installation area returns to neat & tidy conditions after installation of poles, cantilevers etc. The placement shall be designed

keeping in mind the normal flow of vehicular traffic and pedestrian movement is not disturbed.

#### **2.3.3.1.3 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. SI 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. SI shall install UPS at the identified intersections in secure, tamper-proof housing in corrosion resistant cabinets.
4. SI shall ensure that the UPS is suitably protected against storms, power surges and lightning.
5. SI shall provide UPS for efficient heat dissipation without air conditioning. It shall be able to withstand temperatures prevalent in Nagpur throughout the year.

#### **2.3.3.1.4 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. SIs 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 Nagpur'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. SI shall ensure that all the hardware is placed inside the junction boxes that could withstand temperatures prevalent in Nagpur City throughout the year.

#### **2.3.3.1.5 Civil and Electrical Works**

8. SI shall be responsible for carrying out all the civil work required for setting up all the field components of the system including:



- a) Preparation of concrete foundation for MS-Poles & cantilevers
  - b) Laying of GI Pipes (B Class) complete with GI fitting
  - c) Hard soil deep digging and backfilling after cabling
  - d) Soft soil deep digging and backfilling after cabling
  - e) Chambers with metal cover at every junction box, pole and at road crossings
  - f) Concrete foundation from the Ground for outdoor racks
9. SI shall provide electricity to the cameras through the aggregation point. Since this component has dependency on approval from local authorities, it is recommended that SI plans this requirement well in advance & submits the application to the concerned electricity distribution agency with requisite fees, if applicable.
  10. SI shall carry out all the electrical work required for powering all the components of the system
  11. Electrical installation and wiring shall conform to the electrical codes of India.
  12. SI 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,
  13. For the wired Box cameras, SI 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.
  14. Registration of electrical connections at all field sites shall be done in the name of SI/Purchaser as agreed and finalized in the contract agreement.
  15. SI shall house the electricity meters inside the power cabinet as mentioned in the controller Cabinet section as above.

#### **2.3.3.1.6 Earthing and Lightning Proof Measures**

1. SI 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. SI 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

#### **2.3.3.1.7 Miscellaneous:**

1. Purchaser shall assist in obtaining all necessary go ahead, legal permissions, NOC (No Objection Certificate) from various departments to execute the project. SI shall have to identify and obtain necessary legal / statutory clearances for erecting the poles and installing cameras, for provisioning of the required power, etc. SI shall provide & manage all necessary paper work to pursue permission from respective authorities. No

- commercial/legal fees shall be applicable to Purchaser for obtaining the necessary permissions. These shall be provisioned for by the SI in their financial bid.
2. The SI 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. SI shall also get comprehensive insurance from reputed insurance company for the project duration for all the equipments / components installed under this project.
  5. SI shall ensure all the equipment's installed in the outdoor locations are vandal proof and in case the equipments 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 also when calls are placed by Purchaser or its designated agency.
  7. SI 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, the SI 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.

### **1.3.3.2 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 SI 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.

### **1.3.3.3 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 SI 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 100m and various angles on the road.

For installing VaMS Signboards, the SI 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. SI shall consider additional space for lateral clearance as well as a vertical clearance height as per NHAI (National Highway Authority of India) guidelines.

### **1.3.3.4 Drone based Surveillance**

Drones are airborne systems providing advanced surveillance solutions that can be used by law enforcement agencies to monitor situations like large scale crowd gathering, processions, dharnas, Rasta-roko and similar surveillance purposes wherein the incidents like stampede, chaos etc., may happen causing irrevocable aftermath.

Remote-controlled drone could be flown to incident locations and scenes of accident. A high resolution camera is mounted on the drone that can rotate to have a complete 360<sup>o</sup> view of the ground and the data is transmitted to the command control room providing a real time awareness of the situation thus facilitating the authorities to assess and control the situation and prevent any untoward incidents. Preventive measures could be properly assessed and planned in advance in case of any further events.

High resolution photos received from the feeds can be stored as records and can provide valuable evidence for subsequent analysis.

### **1.3.3.5 Mobile Surveillance Vehicle**

The Mobile Surveillance Vehicle (MSV) is a surveillance vehicle that dramatically increases the surveillance, protection & localized command capabilities as a mobile operational unit. This system could be installed on any suitable vehicle (preferred Innova diesel GX2.5 or similar type), and has a vital “look-up and see” capability to cover a wide area of security

operation. The flexible modular architecture of the MSV system enables progressive system growth with connectivity to Command Control Centre. The MSV shall have feature for real-time data link communication, transmitting video and receiving data simultaneously.

1. The MSV shall be a fully customizable vehicle unit with rapid deployment capability within the city environment and other rugged terrain in all weather conditions. The entire solution is to be made ruggedized to handle vibration and shocks during transportation. The fully mobile van can easily be deployed at any location for surveillance.
2. The specialized vehicle shall have capabilities for data processing, real-time communication and situational analysis. It shall work as a mobile surveillance command center.
3. The vehicle shall have a PTZ camera mounted on top and two fixed box cameras all equipped with Infrared capability to see during low light conditions. The PTZ camera shall be mounted on a retractable hydraulic shaft arrangement.
4. The registration of MSV under the Project shall be in the name of Purchaser/Nagpur Police.
5. The vehicle can be divided into three main sections:
  - a. Driver Side
  - b. Monitoring Side
  - c. Power Compartment

The driver side section of the MSV shall house space for one driver and one passenger. The monitoring side of the MSV shall have seating for at least two personnel who shall monitor the cameras (PTZ camera) on on-board screens. The monitoring section shall also have LED screens, laptop etc. All the cameras in the MSV shall have the Video Management Software and Video Analytics software.



**Figure 1: Illustrative picture of mobile surveillance vehicle**

A portable generator shall be installed in the vehicle to power surveillance equipment. The portable generator shall be of necessary capacity to support equipment's installed in MSV. A UPS shall also be installed in the MSV of adequate capacity.

MSV operator shall be empowered to monitor, coordinate and relay commands to & fro with the field units and Central Command Centre.

The MSV operators should be empowered to monitor, coordinate and relay commands to & fro with the field units and Central & Command Centre. The vehicle should also include, a PA system to broadcast for the outside people.

Other supporting components shall include but are not limited to:

1. Observation hatch on the roof
2. Siren with integrated PA system
3. Flame Proof - water proof cabins
4. Search lights
5. Mobile office Seating arrangement
6. LCD screen
7. Power Generator/ UPS for uninterrupted power supply
8. Air-conditioning
9. First-aid Box
10. Umbrellas, Torches etc.

### **Mobile Command Control Centre**

SI shall be required to provide mobile Command Control Centre setup in a vehicle with features as described in subsequent sections of this RFP. Mobile CCC shall be equipped with video display screen, camera, workstations, GPS etc. Mobile CCC shall be able to capture and analyse video of the events at the location itself. SI shall devise a mechanism for the video feed to be uploaded to the main system once the mobile CCC is in the network zone of fixed CCC. A provision for live streaming (of appropriate resolution) of video feed from the Mobile CCC to the Command Control Centre shall also be there where possible.

#### **1.3.3.6 Server Room**

The SI shall establish a state of the art Server Room facility at Command Control Center at the identified location that shall house the IT and non-IT infrastructure for the complete operation of the Integrated Security and Surveillance system for Nagpur city. The Server Room 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 Server Room LAN connections shall be provided through switches placed in this area. The approximate size of the Server Infrastructure zone shall be approx. 1100sq.ft. 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 the authorized personnel. Indoor CCTV Cameras shall be installed to monitor the 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.

### **2.3.3.8.1 IT Infrastructure for Server Room**

Following sections highlight the indicative scope of work of the SI and not limited for Design, Supply and Deployment of IT Infrastructure for Server Room

#### **1. Hardware and Network Provisioning**

SI shall be responsible for the following but not limited to:

- a. Appropriate sizing and provisioning of IT & non 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
- b. Warranty for all the IT hardware assets procured to comply with the requirements as defined in this RFP.
- c. Size the bandwidth requirements across all locations considering the application performance, replication, data transfer, internet connectivity for server room and other requirements.
- d. Furnish a schedule of delivery of all IT Infrastructure items
- e. Ensure all the hardware requirements of the application suite (including third party applications), databases, OS and other software are met.
- f. Purchaser may at its sole discretion evaluate the hardware sizing. The SI needs to provide necessary explanation for sizing to Purchaser
- g. Ensure that the proposed servers are able to accommodate newer versions of processors, memory, etc. that support enhanced capability (e.g. lower power footprint, higher working temperature, smaller process architecture, higher frequency) 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. SI shall substantiate with proof; preferably with an undertaking to replace the processors as and when such processors of highest level of frequency are supported.
- h. The proposed server models wherever applicable shall be Blade Mount servers with key board, monitor, etc. shared to minimize the requirement of rack space in server room considering any space constraints. The model however shall not pose constraints in performance.

#### **2. Provisioning switches**

- a. The SI shall size and propose requisite switch at server room with the required components/modules considering redundancy and load balancing.
- b. The SI shall size and propose other switches required for interconnecting various segments, operations center, work area, etc.

#### **3. IP address schema**

- a. The SI shall design suitable IP Schema for the entire Wide Area Network including server room and interfaces to external systems/network. The SI shall ensure efficient traffic routing irrespective of link medium.

- b. The SI shall maintain the IP Schema with required modifications from time to time during the project period.

#### **4. Sub-Networks & Management of Network operation**

- a. The proposed architecture of server room shall be divided into different sub-networks. These networks shall be separated from other networks through switches and firewalls. The logical separations of these sub-networks shall be done using VLANS.
- b. A separate VLAN shall be created to manage the entire network. This network shall have systems to monitor, manage routers, switches, Firewalls, etc. The SI shall provide necessary hardware / server for loading the monitoring software if required.

#### **5. Provisioning Storage**

- a. Storage requirements for the application suite shall have to be assessed by the SI and the storage solution shall be sized and procured accordingly. SI shall propose appropriate storage mechanism in order to accommodate proposed application suite requirement of the purchaser
- b. The proposed storage shall be configured with appropriate redundancy to maintain business continuity

#### **6. Network Equipment level redundancy**

- a. The SI shall provide real-time redundancy at the network equipment level in server room, and there shall not be any single point of failure.
- b. 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).
- c. The Network Equipment redundancy stipulations wherever prescribed are the minimum requirements that the SI needs to consider. However, SI needs to estimate and plan actual requirements considering service level requirements specified in this RFP.

#### **7. Provisioning IT Security Equipment**

- a. The SI shall size and propose firewalls with the required components/modules for server room.
- b. Necessary IDS/ IPS shall be provided for monitoring the traffic of all the VLANs at server room.
- c. Necessary devices for log capture from servers, network equipment and other devices shall to be provisioned.
- d. The SI 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 server room shall be provisioned by the SI.
- e. SI shall implement management systems and procedures that adhere to Purchaser's security policies.
- f. SI shall secure network resources against unauthorized access from internal or external sources.
- g. SI 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

- h. SI 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.
- i. SI shall ensure that all firewall management is initiated from a segregated management rail on the network.
- j. SI shall provide intrusion management services to protect Purchaser's resources from internal and external threats.
- k. SI shall provide Purchaser with the necessary hardware/software required for efficient intrusion management.

### **1.3.3.7 Command and Control Center (CCC) – City Surveillance**

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 the cameras and display them on the Video wall and provide necessary interface for integrating with other applications like Dial 100 and response mechanism as required by the Purchaser, it shall present a Common Operating Picture (COP) of the real time events in the area of purview. Functions of the Command Control Centre shall include but not limited to the following:

1. Video Surveillance
2. Video Investigations
3. Emergency Response activities
4. Video data storage & retrieval

The Central Command Control Center shall be working in a fully automated environment for optimized monitoring, regulation and enforcement of traffic with various law enforcement services. Various applications/ modules like ANPR, RLVD, specified in this RFP shall be integrated into one functional system and shall be accessible by the operators and concerned agencies with necessary login credentials. The operators/ end users shall be able to access master data like Vahan and Sarathi databases (that are available with the agencies and that can be integrated as and when available).

Location for Command Control Center shall be provided by the Purchaser. Responsibilities of the SI shall include site preparation activities as mentioned in this RFP.

The SI shall ensure that the Command Control Center shall control and integrate systems in a seamless manner.

- i. The Command Control Center 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 for the purpose of preserving operational continuity. The minimum technical specification for the equipment required at the Command Control Center is listed in this RFP.
- ii. The SI shall be required to undertake detailed assessment of the requirements at the command control center and prepare a plan to implement the Command Control



Center and commission required IT and non-IT infrastructure and also carry out the civil/ electrical work as required.

- iii. The data and surveillance network share the same physical infrastructure with guaranteed bandwidth for each individual segment. The software components provide comfortable monitoring experience, easy extraction of clips, and management of storage.
- iv. The video feed from the surveillance cameras shall be received at the Command Control Center where a video wall shall be installed for viewing.
- v. The surveillance team shall receive live feeds from the surveillance camera and shall also control the PTZ camera using joysticks. They shall be alerted if an incident is detected through video content analytics, ANPR system, events generated from various sensors sending feed to the central Command Control Center and shall be able to view the relevant feed from the surveillance cameras. The operator on each of the workstation shall be able to work on multiple monitors at the same time, for which there is requirement of multi screens with one computer (specifically three) to be installed on work desks (appropriate furniture) with appropriate multi monitor mounts.

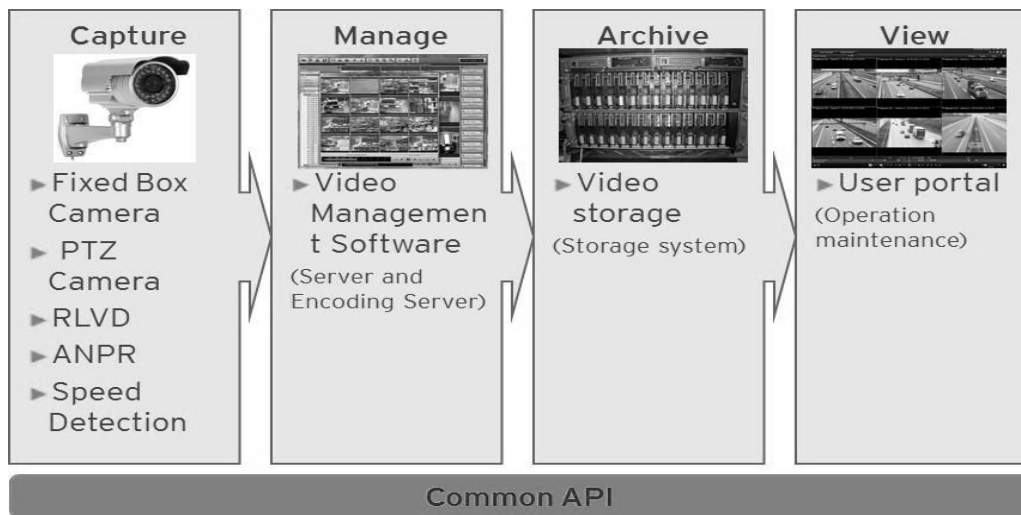
### **1.3.3.8 Application Environment:**

#### **1.3.3.8.1 Video Management System**

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 accept the feed from IP Camera installed at field locations. Server shall stream incoming video to a connected storage. VMS shall support video IP fixed colour / B&W cameras, PTZ / Dome cameras, infrared cameras, low light/IR cameras and any other camera that provides a composite PAL video signal.



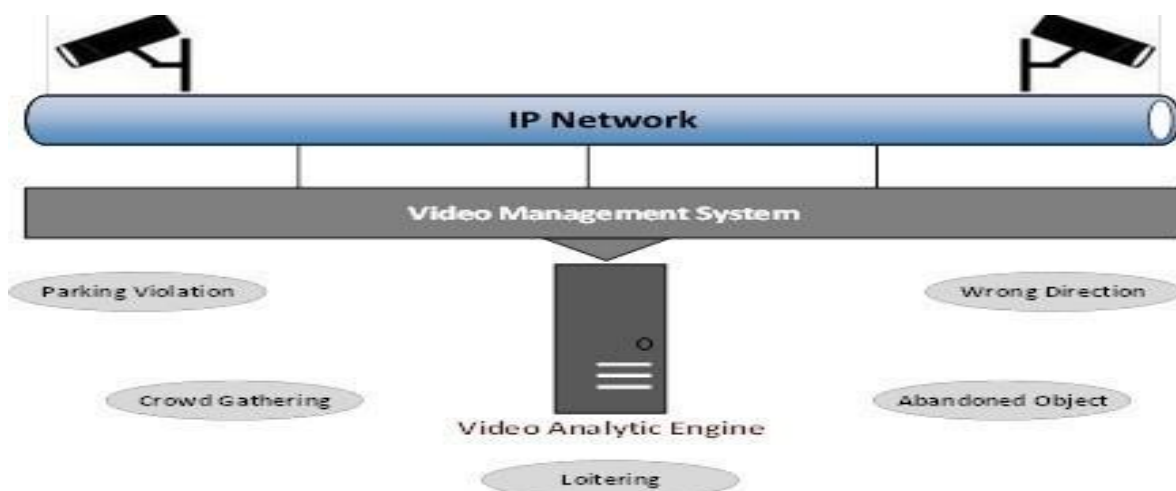
### 1.3.3.8.2 Video Analytics

Surveillance system shall have the capability to deploy intelligent video analytics software on any of the selected cameras. This software shall have the capability to provide various alarms & triggers. The software shall essentially evolve to automate the Suspect activity capture and escalation; eliminate the 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.

Various video analytics that shall be offered on identified cameras are (Number of FB cameras):

1. Parking Violation
2. People loitering within restricted area
3. Wrong/One way detection
4. Camera tampering
5. Unattended object
6. Object Classification
7. Tripwire/Intrusion



The solution shall enable simultaneous digital video recording from network, intelligent video analysis and remote access to live and recorded images from any networked computer. It shall be able to automatically track and classify objects such as cars and people and push content to the respective security personnel as required for real time analysis. The system shall also have display of time line, customizable site map, live video, video playback, integrated site map, remote live view, multi-site capability, encryption, watermarking and event based recording.

All cameras should support motion detection, camera tampering and audio analytics .All cameras must be capable to run two analytics in addition to motion detection and camera tampering as required at any given time.

Solution shall be so designed to have Automated PTZ camera control for zooming in on interesting events like motion detection etc. as picked up by camera without the need of human intervention. It shall be completely scalable, with a many-to-many client-server model allowing multiple physical systems to be used in an array of servers. The server specified in the RFP indicates only the minimum requirements. However, SI shall offer the server system to suit the video analytics requirements specified herein.

#### **1.3.3.8.3 Automatic Number Plate Recognition**

SI shall provide Automatic Number Plate Recognition (ANPR) solution at the identified locations. SI 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 center, 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 enhance 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. ANPR software shall be integrated with video management system.

The 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 the image captured shall be done in real time. The 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.

#### **1.3.3.8.4 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.

TSI 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 with Purchaser.

#### **1.3.3.8.5 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 system shall be able to:

- i. Capture face images from CCTV feed and generate alerts if a blacklist match is found.
- ii. Search photographs from the database matching suspect features.
- iii. 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.
- iv. Add photographs obtained from newspapers, raids, sent by people, sketches etc. to the criminal's repository tagged for sex, age, scars, tattoos, etc. for future searches.
- v. Investigate to check the identity of individuals upon receiving such requests from Police Stations.
- vi. 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. These cameras identified shall be installed at critical locations as mentioned in Annexure II of the RFP document.

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

The detailed functional requirement specification of the facial recognition system is provided in subsequent sections of this RFP.

#### **1.3.3.8.6 System Integration**

The SI shall ensure seamless integration of City Surveillance system with an external Geographical Information System (GIS). The GIS console shall allow operators to get an overview of the entire system and access to all system components. GIS shall enable dynamic view of the location and status of resources and objects/sensors. System shall enable authorized user to open a new incident and associate the incident with its geographic location automatically, via the GIS display.

The proposed City Surveillance System shall also provision for seamless integration with other government datasets like Vaahan, Sarathi, Dial 100, e-challan etc. as and when they are available from respective agencies. The system shall be capable of providing evidence support for ANPR, RLVD events and be integrable with e-challan system if required.

#### **1.3.3.9 City Operations Center**

The City Operation Center shall facilitate the purchaser with a viewing and controlling mechanism for selected field locations in a fully automated environment for optimized monitoring, regulation and enforcement of services. City Operation Center shall be accessible by operators and concerned agencies with necessary authentication credentials. City Operation Center shall be used and manned by the NMC officers to keep surveillance on civil issues.

City Operation Center shall be located at a designated place decided by the Purchaser.

- i. City Operation Center shall provide a comprehensive system for planning, optimizing resources and response pertaining to the standard functions of Nagpur Municipal Corporation, minimum technical specification for the equipment required at the City Operations Center is listed in this RFP.
- ii. SI shall be required to undertake detailed assessment of the requirements at the city operation center and commission required IT and non-IT infrastructure and also carry out the civil/electrical work as required.
- iii. Data and surveillance network share the same physical infrastructure with guaranteed bandwidth for each individual segment. Software components shall provide comfortable monitoring experience, easy extraction of clips, and management of storage.
- iv. Video feed from the surveillance cameras shall be received at the City Operation Center where a video wall shall be installed for viewing relevant feed from the surveillance cameras. The operator/s in the Command Control Centre shall be able to work on multiple monitors at the same time on each workstation This requires multi screens with one computer (specifically three) to be installed on work desks (and appropriate furniture) along with appropriate multi monitor mounts.

Purchaser shall carry out a detail assessment of the proposed design solution and review design of the Command Control Center, Server Room and City Operation Center on the parameters of overall Design, Safety & Security. Purchaser reserves the right to accept, reject or suggest any modifications to the proposed solution.

### **1.3.3.10 Near DR Site**

Purchaser intends to provision for City Operation Center as a Near DR Site for City Surveillance Solution. Control Command Center shall provision to cater 100% load of the City Surveillance system i.e. video recording of all the field cameras feeds, all applications like VMS, Video Analytics, RLVD, FRS, and complete compute and storage capacity. However, SI shall be responsible to provision City Surveillance Near DR Site with 30% capacity (as compared to CCC) i.e. catering to 30% of field cameras with all the application functionalities and appropriate compute and storage capacity as well.

Both Command Control Center and Near 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.

Both CCC and Near DR Site shall work in an Active-Active mode with CCC recording all 100% of cameras and Near DR Site recording 30% of critical cameras feeds.

The SI shall establish dedicated connectivity between the Command Control Center and Near DR Site for replication & failover.

The SI shall design the CCC & Near DR Site solution with the necessary load balancing, replication and recovery solution that provide zero RPO (Recovery Point Objective) and RTO (Recovery Time Objective) of 10 minutes.

The SI shall submit the detailed solution document for the Near DR Site solution with justification for the proposed design meeting the requirements.

### **1.3.3.11 Network Infrastructure**

Network Connectivity is the backbone for all the other components of the project and needs attention in assessment, planning and implementation. It is important for the SI not only to ensure that the required connectivity is provisioned within the required timelines but also ensure that it is reliable, secure and supports the required SLA parameters. The most important parameter to be taken care of shall be the quality of video being streamed to the Command Control Centre from the surveillance locations that shall exceed expectations as the quality of video is of essence.

SI is required to cover following aspects while designing the network architecture, roll-out plan and implementation of network backbone across all the locations.

#### **1.3.3.11.1 Network Design and Rollout plan**

The SI shall be required to prepare detailed network architecture of the overall system, incorporating findings of site survey exercise. Network so designed shall be able to provide real time video stream to the Command Control Centre. The design shall also cover LAN connectivity requirements at locations such as Command and Control center, Server room that shall include setting up of structured cabling, commissioning of active and passive components for operationalization of the Integrated Security and Surveillance system.

SI is expected to provision for necessary bandwidth and connectivity during the contract period. Till the time city network backbone is in place, provisioning for bandwidth shall be done

on bandwidth as a service model. City Network backbone shall provision for all the Safe & Smart initiatives for Nagpur Smart City including City Surveillance.

### 1.3.3.11.2 Implementation of Network connectivity

SI shall ensure that redundant, high quality, seamless connectivity is provided to all cameras across the city. Connectivity to server room and Command and Control Center shall be provided with scalable capacities to allow for expansion in the future. SI is required to undertake estimation of bandwidth & storage requirements considering the benchmark parameters shared below.

Description	PTZ Camera	Fixed Camera	Box	ANPR Camera
Resolution (Pixels)	1920 x 1080	1920 x 1080		1920 x 1080
Frames Per Second (FPS)	25 FPS	25 FPS		25 FPS

SI shall provide adequate bandwidth for each camera to maintain high quality video transmission to the Command Control Centre. The actual bandwidth requirement to cater to above mentioned bandwidth & storage parameters and to meet SLAs shall be estimated by the SI and proposed in the technical bid with detailed calculations. It is expected that SI shall design the networking solution in such a manner that there are no single point of failures at every pole and solution meets all the uptime & and quality related SLAs.

SI needs to undertake the following activities (including but not limited to) provisioning of the network backbone for Purchaser:

#### 1. Provisioning Network Links

- a. All field locations shall be connected to server room & control command center through optical fiber backbone network.
- b. SI is expected to procure bandwidth as a service till the time city network backbone is created.
- c. SI shall ensure that the bandwidth estimated and proposed meets the locations' requirement and expected performance level.
- d. All the required network and security equipment like routers, switches, firewall, etc. shall be provided by the SI.

#### 2. Network Management Services

- a. SI shall ensure that the network is available 24x7x365 as per the prescribed SLAs.
- b. SI shall provide services for management of network environment to maintain performance at optimum levels.
- c. SI shall be responsible for attending to and resolving network failures and snags
- d. SI shall support and maintain the overall network infrastructure including but not limited to LAN passive components, routers, switches, Firewalls', etc.
- e. SI shall provide information on performance of Ethernet segments, including capacity utilization and error statistics for the segment and the top-contributing hosts and routers

- f. SI shall create required facilities for providing network administration services including administrative support for user registration, creating and maintaining user profiles, granting user access and authorization, providing ongoing user password support, announcing and providing networking services for users and providing administrative support for print, file, directory and e-mail servers for the Purchaser.
- g. SI shall provide a single-point-of-contact for requesting LAN and Server administration services and answering administrative questions. Network Administrator shall respond to the initial request from the users within the agreed service level objectives and service coverage hours.
- h. SI shall provide support as required to assist with hardware and software problem isolation and resolution in the LAN environment.
- i. SI shall undertake LAN and Server problem determination.
- j. SI shall communicate server changes affecting the LAN environment.
- k. SI shall maintain LAN and server configuration data.
- l. SI shall be responsible for polling / collecting of server, devices and desktops security logs from all the systems. All these logs shall be made available to the Enterprise Management System (EMS) solution.

### **3. Network Security**

SI shall be responsible for management of Integrated Security and Surveillance system's network security. As part of network security, the SI shall ensure the following:

- a. Network shall be used for valid purposes only. Protection of information available on the networks is the responsibility of SI. The activity and content of user information on the computer networks is within the scope of review by management.
- b. SI shall develop and implement network security systems and procedures, and provide network security resources (Firewall etc.) to protect all Purchaser's data, related application systems and operating systems software from unauthorized or illegal access at a level that is appropriate for the information /computing resources.
- c. SI shall be responsible for the following activities:

#### **1. Network Access**

- i. SI shall ensure that Access to network and network resources shall be on need to know basis and authorizations shall be obtained from appropriate authorities before providing access.
- ii. Network and network services required for every job function and role shall be identified and verified by the SI
- iii. Policies detailed in Access Controls Policy – User Account Management shall be followed by the SI for providing access to network and network services
- iv. SI shall ensure that the networks are logically or physically divided based on the criticality of the information stored in the networks.

#### **2. Internet Service Management**



- i. SI shall be responsible for granting, monitoring, and revoking access to the internet.
- ii. SI shall ensure that users utilize the internet only for operational use.
- iii. All the internet activity shall be logged and monitored, and appropriate network devices shall be deployed so that access controls and related security mechanisms could be applied.

### **3. Network Management**

- i. All network equipment and communication lines shall be identified, documented, and shall be regularly updated by the SI.
- ii. Network diagrams at all levels shall be maintained and updated regularly by the SI.
- iii. Minimum Baseline Security Standards (MBSS) shall be developed and maintained by the SI.
- iv. All network equipment shall be configured as per MBSS.
- v. All network services that are not required on the servers shall be disabled.
- vi. Any problems with the network equipment leading to delay or stopping of any business processes shall be escalated as an Incident.

### **4. Data Transmission**

- i. Care shall be taken by the SI while transmitting confidential information over public networks to other government agencies.
- ii. Confidential information not being actively used, when stored or transported in computer-readable storage media (such as magnetic tapes or CDs), shall be stored securely under lock and key
- iii. SI shall ensure and prevent unauthorized disclosure of data when computers are sent out for repair or used by others within or outside CCC and the data could be deleted. All data stored on hard disks shall be backed up and erased via user-transparent processes.

### **5. Network Assessment**

- i. Network vulnerability assessments shall be performed on an ongoing basis by the SI.
- ii. Assessment report shall be submitted to the purchaser on a quarterly basis.
- iii. The SI shall coordinate for Third-party independent network assessment that shall be carried annually in order to provide assurance to the purchaser.

#### **1.3.3.12 Installation & Commissioning of a Sample Site**

The SI shall complete the installation work at the identified sample sites from all the aspects and then request the Purchaser to conduct a detailed assessment of all the quality parameters that it expects at the sample site. Following aspects shall be assessed thoroughly:

- a. Quality of concrete foundation made for erecting Poles and Junction Box.
- b. Quality of Poles and Junction Box erected at site.

- c. Quality of resurfacing of the cut roads and pavements.
- d. Placement of relevant equipment like network switch, local processing unit, UPS, Telecom Service Providers MUX inside the rack.
- e. Electrical earthing of the Junction Box and Poles.
- f. Structured cabling standards inside the Junction box.
- g. Cabling from the junction box to the poles to be completely covered
- h. Labelling of the entire infrastructure inside the rack and also all the poles and cameras at the junction site for ease of maintenance.

A Site visit report shall be prepared and presented to the purchaser covering all the observations. The same shall be dually vetted by Purchaser and changes if any suggested shall be highlighted.

The SI shall ensure the observations/ changes suggested by Purchaser shall be incorporated for the first site and also incorporated for all locations. Due verification of the same shall be done at the time of User Acceptance of the project.

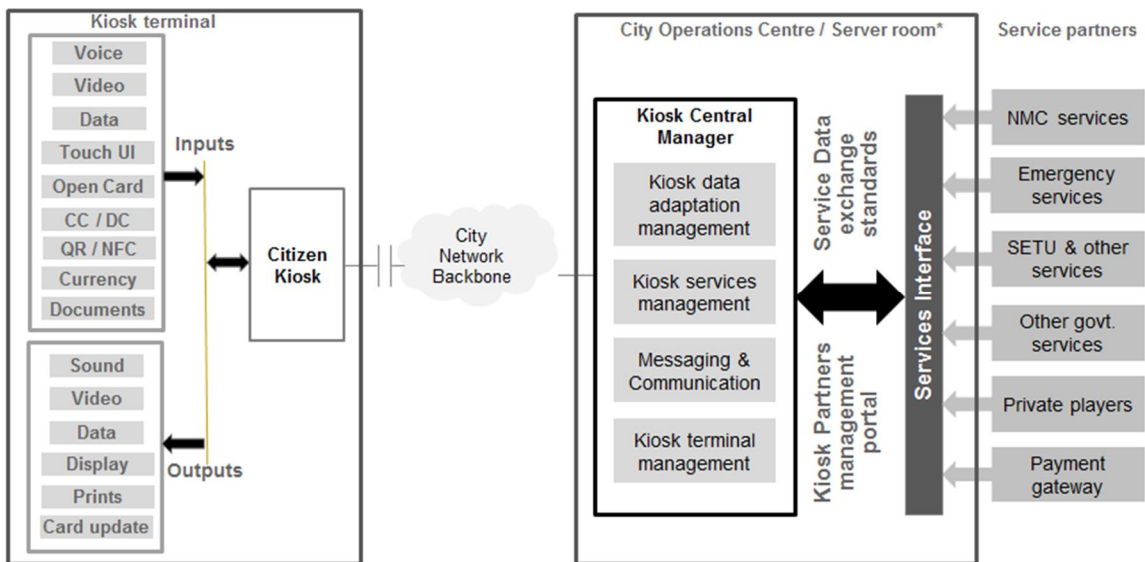
## 1.4 SOLUTION 4: Nagpur City Kiosk

### 1.4.1 Overview

As a move towards an “approachable city administration”, purchaser wishes to deploy a number of touch points in form of City Kiosks across the city of Nagpur. These City Kiosks are expected to act as an extended arm of city administration departments and help in connecting with citizens while promoting “anytime services” complementing the mobile platform based service delivery. While delivery of G2C services shall be the primary focus of City Kiosk systems, in order to ensure broader adoption and ensure business viability, B2C services may be provided through City Kiosk.

### 1.4.2 Solution requirements

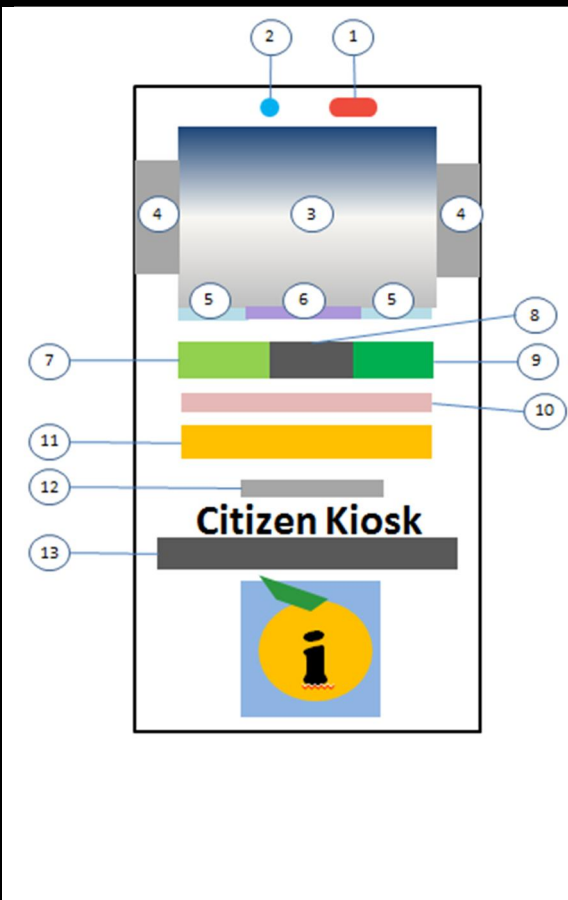
The below schematic provides a view of various components of City Kiosk solution. These have been described subsequently.



\* It is envisaged that central system of City Kiosk may be migrated to a cloud-based data center in future. Hence, SI is expected to factor cost of one time shifting of system from City operations Centre to cloud-based data center

SI shall only be responsible for providing City Kiosk machines along with maintenance support to purchaser or authorized entity which in turn shall use these City Kiosk machines to provide various informative and transactional services to the end citizens.

## City Kiosk Terminal

Illustrative representation of Kiosk	Item
 <p>The diagram shows a vertical kiosk terminal labeled 'Citizen Kiosk'. At the top, there is a red button (1) and a blue button (2). Below them is a camera (3). The main display area (4) is a touchscreen. Below the display are two microphones (5) and a keyboard (6). Further down are a credit/debit card reader (8), a QR code interface (9), a currency acceptor (11), a receipt/ticket printer (12), and a document inlet (13). The kiosk has a yellow and green logo at the bottom.</p>	1. Panic Button which shall trigger response to emergency services within city administration
	2. Camera to enable teleconferencing and photos through kiosk
	3. Touchscreen, display and processor Support for multilingual interface including Marathi, Hindi & English
	4. Speakers
	5. Microphone
	6. Keyboard for accepting user input
	7. Open city card interface which may be used to enable transactions through open city card*
	8. Credit card / Debit card reader – accepting payments through credit / debit card
	9. QR code interface – enable inputs through QR code*
	10. Interface for accepting NFC based payments*
	11. Currency acceptor – with features such as fake currency detection
	12. Receipt & ticket printer
	13. Inlet for cheques / documents

\* Marked components may not be embedded within body of kiosk. However, these interfaces are expected to be provided by SI.

As mentioned in the diagram the various formats in which input shall take place to kiosk include voice, video, data, touch UI, open card, credit card/ debit card, QR code, NFC, currency and documents whereas outputs include sound, video, data, display, prints, card updates. Above mentioned components shall enable these interfaces.

Functionalities such as open city card reader / writer may be disabled, depending on readiness these functionalities may be enabled in the kiosk machine progressively.

In future it is envisaged that most transactions shall be enabled via open city card for Nagpur city. The City Kiosks shall be the key anchors in ensuring smooth functioning of the said functionality.

### 1.4.2.1 City operations centre and server room:

Staff for managing daily operations of City Kiosk which include kiosk upkeep, services and partner support shall be carried out through team deployed at city operations center. To begin with the server side infrastructure requirement, for carrying out City Kiosk operations, shall be hosted at city operations center at NMC head office.

The central system for City Kiosk management is envisaged to consist of following key modules:

1. Kiosk terminal management

This module shall facilitate controlling of end terminals deployed across various locations. Functionalities which are expected to be part of this module include:

- a. Kiosk deployment details such as unique id, IP address, form factor, components included, and others
- b. Kiosk terminal health monitoring – health of kiosk components, whether equipment is functional or requires replacement
- c. Maintenance & support module – controlling maintenance of various components within kiosk, ensuring periodic maintenance as per schedules defined at the time of planning
- d. Upgrade of firmware, OS and other related platforms
- e. Management, upgradation, deployment and maintenance of various applications /API's through central locatoin which shall then be populated across all the field located kiosks.
- f. Replenishment of consumables including receipt printers, open city cards
- g. Maintaining details of money collected by kiosk, items put in drop box and others
- h. Data encryption and data security within kiosk terminal

2. Kiosk services management

This module shall facilitate management of services provided through City Kiosk. It is envisaged that based on the location of the City Kiosk, services shall be configured on the end terminal. Functionalities which are expected to be part of this module include:

- a. Service portfolio management across all City Kiosks, services which are operational, being tested (in pilot) or in pipeline
- b. Enabling and disabling of services based on information received from partner management portal
- c. Monitoring finances, accounts, billing and payments related to services to partners
- d. Managing of advertisements and other promotional messages being displayed through City Kiosk
- e. Managing survey and feedback on various City Kiosk services
- f. Ensuring delivery of services detailed in subsequent sections
- g. Any other functions related to services delivery through City Kiosk

3. Kiosk partner management portal

This shall be the interface for all partners (read: entities using kiosk for service delivery). This includes government agencies such as NMC, police, etc. and private businesses. Each partner shall be registered on the portal and shall have an account through which various services can be enabled / disabled / configured on basis of portal. The portal shall be single window interface for all interaction for partners with City Kiosk. Payments, bills, refunds, account statements, grievances for partners shall be managed through this portal.

4. Services interface

This module shall enable interfacing with partners for providing of services. Functionalities which are expected to be part of this module include:

- a. Information exchange from City Kiosk terminal with partner system
- b. Payment gateway system with banks and intermediaries
- c. Interfaces with partners to display status of public transport reservations and booking

5. Service data exchange standards

This shall be metadata repository of various standards which may be established with multiple partners. Interface with various service providers, develop standards for information exchange as required for delivery of services through City Kiosk machines. Open standards for data exchange shall be preferred.

6. City Kiosk data adaptation management

Considering the series of different inputs and related information being exchanged through City Kiosk, this component is expected to manage conversion of data as per exchange standards required. This component shall closely work with service interface and message and communication modules.

7. Message and communication

This module is expected to manage message and communication between various modules within the overall system.

The aforementioned modules are key modules which are proposed for smooth delivery of City Kiosk functions. SI shall add more modules depending on the solutions as long as the functionalities mentioned are taken care of.

#### **1.4.2.2 Services and service partners**

City Kiosk is expected to partner with government and private agencies to provide G2C and B2C services. These partners shall include Nagpur city administration, police, other government agencies, banks and private business (local and otherwise)

Below is an indicative listing of services which are expected to be made available from city kiosk. These have been categorized as below

- a. Information services: These may include but not limited to
  - i. Places near me services – government offices in city, tourist attractions, businesses, hotels, etc.
  - ii. Navigation services, displaying routes to key locations in Nagpur
  - iii. Information related to public transport in Nagpur such as bus, train, metro route information, real time information about public transport, available taxi services, etc.
  - iv. Important locations including government hospitals, police stations, and contact information etc.
  - v. Tracking status of various applications made to city administration including birth certificate, death certificate, marriage certificate, etc.
  - vi. Account / activity statement for open city card
- b. Application support services

- i. These services shall be provided through a manned kiosk where in personnel shall be deployed with laptop, scanner and printer. Documentary evidence related to applications being made shall be digitized, scanned and accepted. Acknowledgement for each application shall be printed and provided to the citizen.
- c. Grievances and Feedback
  - i. City Kiosk shall provide for forums to citizen to raise complaints regarding various services provided by city administration. This includes pot holes, cleanliness, garbage collection, delay in services, etc.
  - ii. Feedback may be collected in form of a online submission, video file may also be used to involve participation from all citizens
  - iii. Facility to gather feedback from citizen on various services being provided in city, or any other questionnaire / polling questions.
- d. Bill payment services
  - i. Payments of property tax, and other payments to city administration
  - ii. Payments of utility bills, mobile bills, etc.
- e. Dropbox services
  - i. Dropbox of cheques/DDs are alternate form of payment
  - ii. Dropbox for duplicate copies related to applications as deemed necessary
- f. Emergency services
  - i. Panic buttons which enable connectivity (audio / video) to emergency locations such as police, hospitals, fire department, etc.
  - ii. Reporting of incidents such as accidents
- g. Kiosk purchase services
  - i. Kiosk may facilitate purchase of tickets for trains, bus, metro
  - ii. Recharge / issuance of proposed Nagpur open city card through kiosk
  - iii. Purchase of movie tickets, etc.
  - iv. Recharge of mobile phone, etc.

*Note: The above list is indicative and shall undergo elaboration based on participating entities/agencies.*

### **1.4.3 Scope of work:**

#### **1.4.3.1 Sub-component: City Kiosk Terminal**

##### **1. Supply and installation of City Kiosk terminals at identified locations**

- a. SI shall be required to supply City Kiosk terminal meeting requirements as mentioned in the RFP. There shall be two types of kiosks which are expected to be deployed at:
  - i. Self-service Kiosk – no personnel deployed providing services as described in the RFP

- ii. Manned kiosk - Same as self-service kiosk with a support person deployed for accepting applications for government services with following items:
  - Laptop
  - Multifunction Device
  - Webcam
  - Table, chair, etc. for one resource
- b. Required civil work, electricity work, etc. for installation of City Kiosk
- c. Providing last mile connectivity and other networking infrastructure leveraging on network backbone specified in the RFP

## **2. City Kiosk terminal upgrade, repair and maintenance**

SI shall provide end-to-end support, upgrade, update, repair and maintenance of City Kiosk terminal:

- a. Patch update/upgrade of firmware, OS, etc.
- b. Repair and maintenance of kiosk terminal and various interfaces

### **1.4.3.2 Sub-component: Central system**

- a. Setup of required infrastructure within city operation center at NMC Head Office, It is envisaged that central system of City Kiosk may be migrated to a cloud-based data center in future. Hence, SI is expected to factor cost for one time shifting of system from City operations Centre to cloud-based data center
- b. Creation of required computing, storage, network and software platform for delivery of services through City Kiosk. The software created shall support the functionality as mentioned in the RFP and any other requirements envisaged by SI for successful operations of the software. This includes but not limited to
  - i. Developing interfaces for interaction with City Kiosk
  - ii. Developing interfaces for service provides including NMC system, Police system, other business systems
  - iii. Payment gateway interface to enable payments through kiosk
  - iv. Inventory management for City Kiosk machines

### **Locations for City Kiosk deployment**

Various locations where City Kiosk is expected to be deployed are:

1. Phase I - Initial phase: NMC offices – head office(10) and 10 zonal offices (20)
2. Phase II – 70 City Kiosks in mutually agreed locations within NMC approved franchisee locations



## **1.5 “Smart Strip”**

### **1.5.1 Overview**

It has been observed that, Information and Communication Technology (ICT) has changed the evolution of cities; the notion of “growing” cities is being replaced with the idea of making a city “Smart”. ICT has forced the think tank and compelling planners of the cities to not only consider the physical planning of a city but to also consider ICT enablement to make the economy, environment, mobility and governance more efficient and effective.

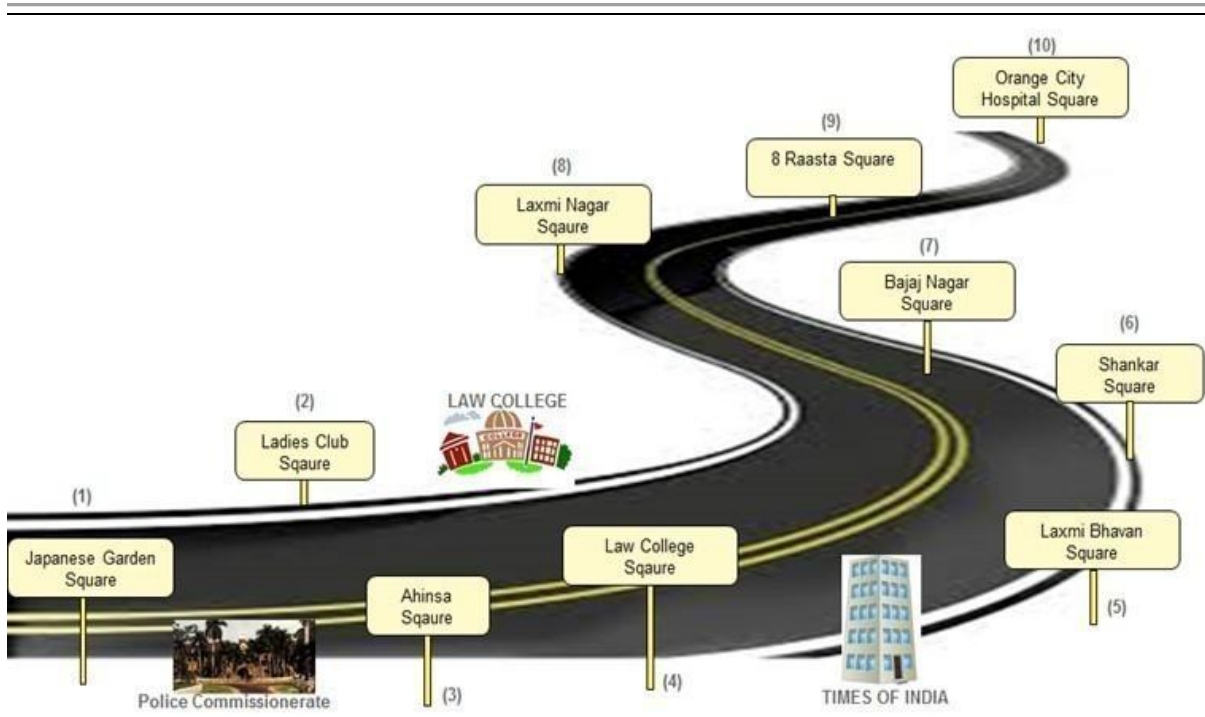
To build on these advances, innovative governments continue to seek new ways of maximizing business value; purchaser keens to take up an initiative for transforming Nagpur into a Smart City by embedding Smart devices, sensors, and actuators within physical space and infrastructures of the city. This offers real-time data management, alerts, and information processing for the city administration and thus allows city planners to develop other innovative ecosystems in line with its people through technology.

Purchaser has identified a strip of approx. 6 KM to be developed as “Smart Strip” with state-of-the-art systems powered with Smart ICT interventions; a prototype model which can be further leveraged in adopting the city wide coverage.

Considered as one of the busiest route of the city, known as West high Court Road, majorly consisting of commercials establishments and government offices. The street has popular Times of India Office along with Law College, Police Commissionerate, shops/showrooms etc.

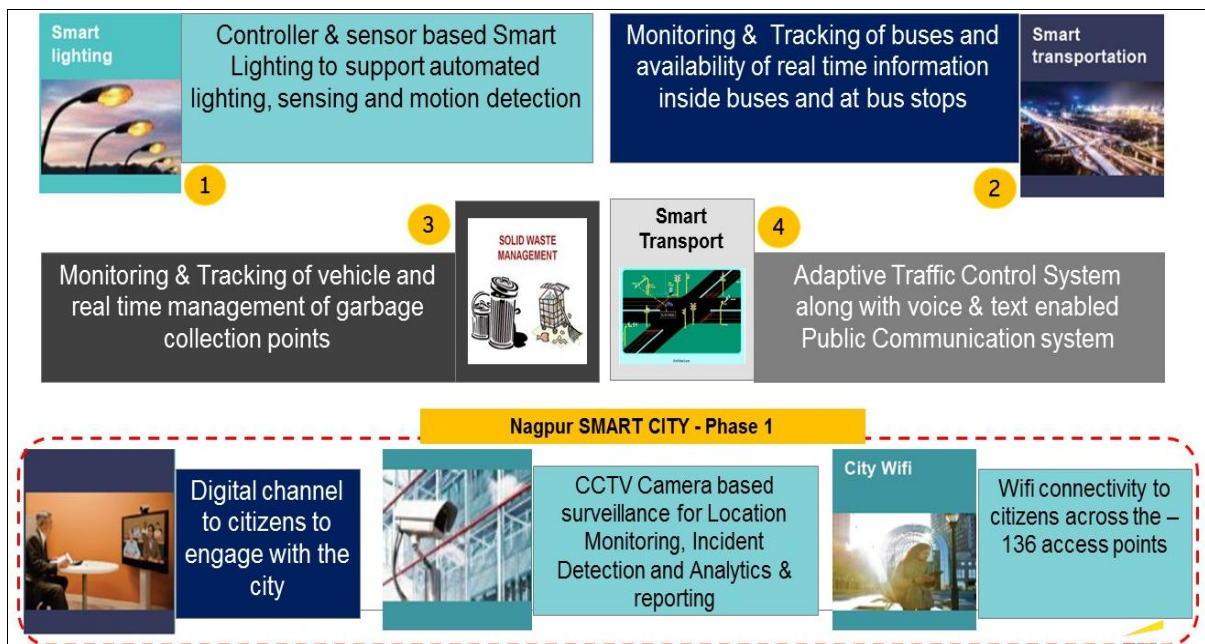
#### **Key Facts about SMART Strip:**

1. Linear stretch of approx. 5.8 km - Starting from Japanese Garden Square to Orange City Hospital Square
2. Residential cum commercial area with majorly offices/shops/government establishments etc. (Commercial : Residential occupancy – 70:30)
3. No. of Households (nearby) – Approx. 200
4. No. of Commercial properties – Approx. 500
5. Total 10 major traffic junctions



Nagpur Municipal Corporation intends to develop a “SMART Strip” encompassing various ICT enabled functionalities which offers more reliable, convenient and hassle free services to its citizen in an effective and coordinated manner. NMC has identified following SMART solutions to be included as part of Nagpur “SMART Strip” initiative:

1. Smart Transport
2. ICT enabled Solid Waste Management
3. Smart Traffic
4. Smart Lighting
5. Smart Parking
6. Environmental Sensors



The “Smart Strip” solutions shall work in conjunction with aforementioned City WiFi, City Kiosk, City Surveillance solutions through City Operation System, thus, allows for cross domain collaboration. For example, it is helpful for public safety departments to know lighting conditions in the city. Similarly, the traffic department would do well to understand environmental data trends, such as of quality of air or temperature, over time in order to make better planning decisions. In the event of a public safety situation, different department representatives sitting together in a common center can coordinate their response much better as well.

The “Smart Strip” solution shall be hosted on NMC City Operation Center and SI shall be required to provision for the appropriate infrastructure (server/storage) as per Indicative Bill of Material mentioned in the subsequent sections.

It is envisaged that the “Smart Strip” system shall leverage City Network Backbone infrastructure that is being created for Nagpur city. However, till the time city network backbone is commissioned, the SI is expected to procure bandwidth as a service in order to meet requirements as defined within service level agreement. SI shall also adequately provision to provide communication sub system (GPRS/GSM/3G) including procurement & installation of SIM cards for the field devices, wherever required. Payment of monthly charges for the required GPRS/GSM communication, for the entire contract period of five years shall also be the responsibility of SI along with network bandwidth payments.

The SI shall also be responsible for providing adequate training to representative of Purchaser/Authorised agency enabling them with functionalities of the various proposed solutions and shall also operate & manage the entire “Smart Strip” solution for a period of five years from the date of Go Live of the system. The proposed hardware infrastructure shall have five years OEM warranty.

Mentioned below the scope of work for “Smart Strip” initiative, Functional & Technical Requirement Specifications and Bill of Material is mentioned subsequently. However, SI has to quote all required materials which may be not mentioned in BoM and are required to make entire system live based on their experience.

### **1.5.2 Smart Transport**

NMC is responsible for the maintenance and operations of bus services within Nagpur City. The city has approx. 240 buses, combination of JNNURM- I and standard mini buses and another 160 buses are being procured (JNNURM – II). Currently, electronic ticketing machine has been the primary mode of issuance of bus tickets which also supports Smart card based payment.

NMC intends to implement ICT enabled Smart Transport System in order to provide economic, adequate, punctual and efficient service to its passengers. NMC envisaged following benefits from the proposed Smart Transport System:

1. Simplifying public transport use by providing accurate real time information about services
2. Better efficiency in operational processes
3. Reduced costs, better turnaround times and reduced wastages

4. Better accountability of people, process and technology
5. Helping drivers find the best route to their destination, and changing that route if major incidents occur on it;
6. Improving the security of public transport passengers and staff by providing extra communications
7. Helping to achieve 'Best Value' within network management as a result of greater information gathering and improved decision making;
8. Reducing the number of accidents by providing drivers with more information about conditions on the roads they are using;

### Scope of Work

#### “Smart Strip” Smart Transport Management Landscape:

1. Smart Strip No. of Buses (JNNURM –I) – 77
2. Smart Strip No. of Bus Stops – 80

#### Scope of RFP (PAN City Coverage) –

1. Total No. of Buses – 400
2. Total No. of Bus Stops – 160

#### Details of Work –

##### 1. Business Solutions

The SI shall be responsible for Supply, Design, Development, Testing, Implementation (as per the functional requirement specifications mentioned in the RFP document), Operation and Maintenance (5 years) of “Smart Strip” Smart Transport Management System which includes:

ICT Interventions	Key Features
Automated Vehicle Locator System	Real time tracking of bus to ensure dedicated route travelled
	ETA at next bus stops in real-time based on speed and distance measurement
Passenger Information System	Manage content of display board/screen in bus
	Centrally control message system
	Public address system - Bus / Route information , other key informative messages like social campaign, Chief minister communication etc.
	Manage content of display board/screen at bus stop
Fleet Management System	Management of complete fleet staff and duty allocation
Mobile Application	Mobile app based tracking of bus information
	Navigation system for reaching to the nearest bus stand basis shortest path
	Information on selection of best route basis travelling start & end point

ICT Interventions	Key Features
Alert Management	Alerts on all pre-configured parameters such as non-stoppage at designated points, unauthorized stoppages, bus breakdown, vehicles stopping for long duration, not meeting the ETA schedule etc.
Two way communication - panic button	Provision of sending SOS messages to City Operation center in case of emergency
Third Party Integration	Integration with ETM system
Monitoring , Controlling and Analysis of transport resources	Passenger to bus utilization analysis, bus route optimization etc.

### I. Automated Vehicle Locator System (AVLS)

The AVLS system shall be a web based application which utilizes GIS map to show real time positions of the buses. The system shall have enterprise capabilities which enables multiple user type to be enabled to carry out various functions like, Alarm Management, Vehicle Schedule Tracking, Speed Management, Stoppage Management, Route replays, bus tracking dashboard etc. as a standard functionality. The system shall have screen based tracking capability, so as to enable tracking staff to quickly analyse activities and have a better insight into operational data of all activities within the system. The system shall be seamlessly integrated with bus GPS system, fleet management system, passenger information system, public address system and mobile application.

### II. Passenger Information System (PIS)

The PIS shall manage the content on all the LED's (inside the bus and at bus stops) and shall manage the next stop announcements in in-bus passenger facing display along with audio from speakers based on GPS location received from AVLS system. The system shall have provision to change the message on outfacing displays whenever required directly from City Operation center. PIS shall be seamlessly integrated with Mobile Application, bus GPS system, AVLS system, Public address system to show bus route, schedule, real time bus location and ETA details. It shall also display bus number, route, schedule and ETA on LED screens at bus stops along with the provision to show advertisement on LED displays on bus stops.

### III. Fleet Management System

The Fleet management system shall be responsible for keeping all the records pertaining to all the buses, fuel consumption, routes, drivers & conductors available for duty allocation and also allow assigning duty for driver, conductor and buses. The system shall provision to send SMS to respective driver and conductor about their duty.

### IV. Public Address System

The PA system shall seamlessly work with PIS system to make audio announcement (pre-recorded) regarding bus routes & stoppages, city communication etc.

### V. Smart Transport Mobile Application (Android platform)

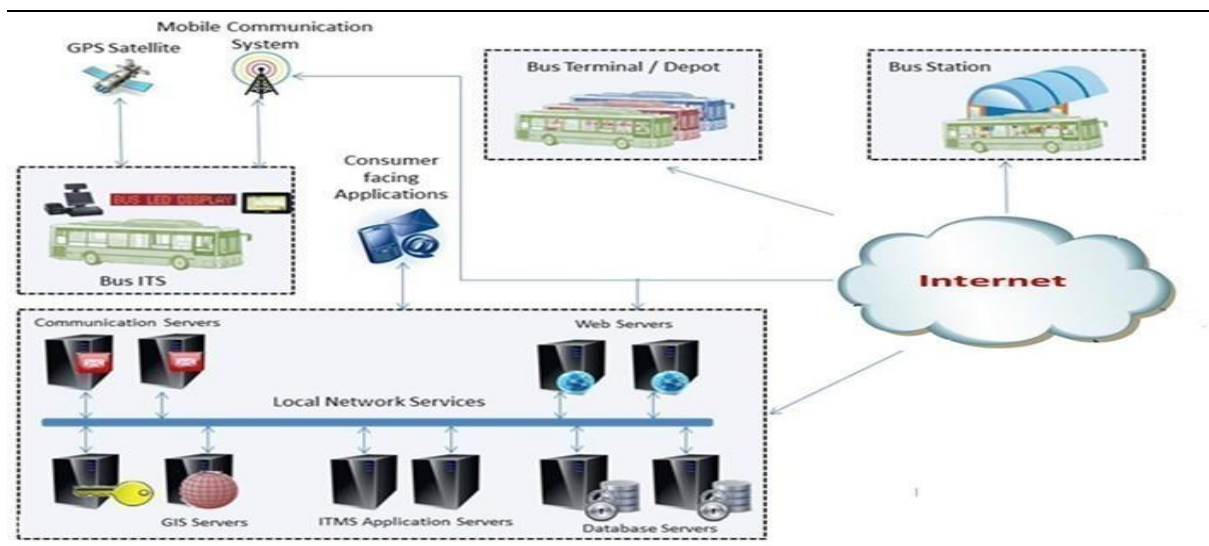
The android based SMART Transport Mobile Application shall give its users access to real time bus schedules along with expected time of arrival at each stop along with bus route no. and route name. The mobile application shall be a navigation based support system that offers users to locate the nearest bus stops from his/her current location with respect to the intended destination.

## 2. Infrastructure Solutions

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

- a. GPS Tracking System with all fittings & fixtures in all the buses
- b. LED monitor/display for Buses & Bus stops along with necessary H/w
- c. Public Address System
- d. Network connectivity for buses, bus stops and city operation center

### Smart Transport Schematic Solution Overview



### 1.5.3 ICT Enabled Solid Waste Management

NMC is responsible for collection, segregation, transportation, dumping and processing of the city waste from door to door. NMC has deployed 3 wheelers and 4 wheelers for collection of door to door waste and dumping into the bins/collection points at strategic 140 locations. From these bins/collection point separate 4 wheelers (loaders) carries the waste to the single location called waste processing plant. Also, NMC has approx. 7800 field staff which is responsible for street sweeping and collection of street waste and dumping to the nearest bins/collection points.

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

1. Lack of information about the collecting time and area.

2. Lack of proper system for monitoring, tracking the vehicles and trash bin that have been collected in real time.
3. There is no estimation to the amount of solid waste inside the bin and the surrounding area due to the scattering of waste
4. There is no quick response to urgent cases like truck accident, breakdown, long time idling etc.

NMC intends to implement a GIS/GPS enabled Solid Waste Management System practices within the existing landscape (pertaining to “Smart Strip”) to

1. Manage routes and vehicles dynamically through an automated system.
2. Real time management of missed garbage collection points
3. Efficient monitoring and management of waste collection bins
4. Route optimization can be done which shall help in reduction of trip time, fuel saving and serving more locations
5. To reduce the human intervention in monitoring process
6. To keep history of vehicle routes, attended sites and other details
7. To integrate the dumping ground and transfer station facilities with the centralized locations
8. Reporting of vehicles, garbage collected and other SWM details to higher authorities from any location at any time
9. Monitor and track the activities of field staff force on daily basis

## Scope of Work

### “Smart Strip” Solid Waste Management Landscape –

1. Total No. of waste collection vehicles – 4
2. Total No. of Bins – 6 (3 per location)
3. Total No. of Loaders – 1
4. Total NMC Field Staff (PAN City) - 7823

### Details of Work –

#### 1. Business Solutions

The SI shall be responsible for Supply, Design, Development, Testing, Implementation (as per the functional requirement specifications mentioned in the RFP document), Operation and Maintenance (5 years) of “Smart Strip” ICT based Solid Waste Management System which includes:

ICT Interventions	Key Features
Solid Waste Management System	GPS tracking of the waste pick up vehicle for real time tracking
	Route Optimization which shall help in reduction of trip time, fuel saving and serving more locations
	Manage routes and vehicles dynamically through an automated system
	Efficient monitoring and management of waste collection bins
	Attendance Management System - Field Staff

ICT Interventions	Key Features
	Ensure complete coverage of door to door and community collections served by vehicles
	Monitor and track other municipal corporation vehicles under Solid Waste Management Dept.
	Record history of vehicle routes, attended sites and other details
	RFID devices with vehicle and RFID tagging of Bin to ensure serving by requisite vehicle
	Weight & Volume Sensor based bin to indicate maximum utilization status and trigger vehicle pick up
	Alert / Alarm management - Real time management of missed garbage collection points
	Monitoring & Reporting Application - reports of vehicles, garbage collection status, bin status etc.

#### **I. Automated Vehicle Locator Management System –**

Web Based Vehicle Tracking and Monitoring Application customized to meet the functional requirements of the solution. NMC intends to extend the Automated Vehicle Locator Management System of the above Smart Transport System with the top on requirement of customized dashboard specific for monitoring and tracking of solid waste management activities and integration with the RFID system & weight and volume sensor system for bin collection management. The application shall be hosted in the City Operation Center. The application shall leverage on the advanced GPS and GIS technologies for route scheduling, route monitoring, reporting and providing a quick dashboard.

#### **II. RFID based Bin Management System –**

The waste collection vehicles shall be fitted with RFID readers. The RFID readers identify the RFID tags installed in the each of the collection Bins and read the Bin details. This data shall be transferred through the GPS device unit GSM/GPRS connectivity to the integrated application. The RFID readers shall be integrated to the vehicle GPS device unit to achieve this functionality.

#### **III. Weight & Volume Sensor Management System –**

The weight sensors shall be placed at the fixed location over which Bin shall be placed every time it being served by the waste collection vehicle. The weight sensor shall sense the level of occupancy of the bin placed above and trigger alert signal to the city operation center application through GPRS/GSM network.

Volume sensor shall be placed at the fixed location over Bin. When the volume of occupancy (waste) reaches to a particular threshold value, an alert/SMS shall be sent to the concerned person through GSM modem.

#### **IV. Mobile GPS based Staff Attendance Management System –**

GPS based mobile device shall enable NMC's field staff to register their attendance/presence throughout the day. The system shall periodically track the location (with time stamping) of the



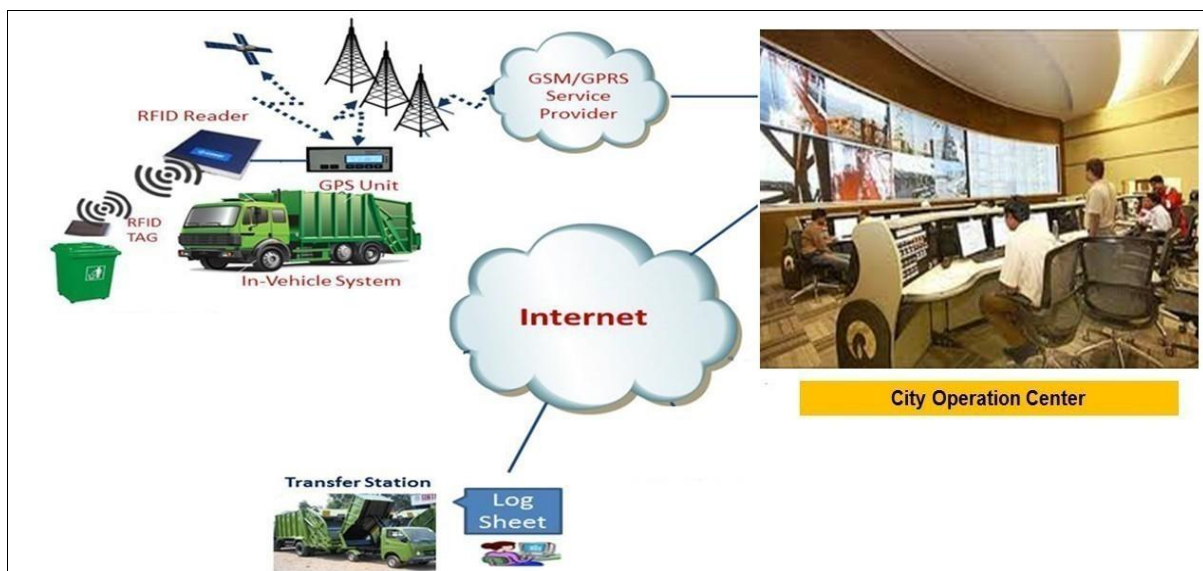
staff through their GPS based mobile device and shall map it in the system with the pre-defined area coordinates. The device shall send the data through GPRS/GSM network to the city operation centre central application for reporting generation and alerts.

## 2. Infrastructure Solutions

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

- a. GPS Tracking System with all fittings & fixtures in all the vehicles
- b. RFID device installation in all the vehicles & loaders and RFID tagging of all the Bins
- c. Mobile biometric device for workers
- d. Weight sensors installation at collection point/ bin
- e. Network connectivity for vehicles, bins and city operation center

### ICT Based Solid Waste Management System Schematic Solution Overview



#### 1.5.4 Smart Lighting

Nagpur city has about 1,05,000 streetlights installations on poles (which belongs to Maharashtra State Electricity Distribution Company Ltd. (MSEDCL)) as well as NMC's owned poles masts / high masts. Out of these street lights majority of street lights are on MSEDCL's poles and remaining are installed on poles, masts and high masts belongs to NMC. Out of these total street lights, 320 streetlights is under the scope of work for "Smart Strip" Smart Light System.

These 320 streetlights are switched 'ON' and switched 'OFF' automatically / manually by feeder panels. Types of majority of these 320 streetlights are 250 Watt H.P.S.V. /Metal halide and 150 Watt H.P.S.V./ Metal halide streetlights. There is underground cabling network for the said street lights with feeder panels as mentioned above.

These aforementioned existing streetlights / floodlights i.e. 250 Watt H.P.S.V. /Metal halide and 150 Watt H.P.S.V./ Metal halide streetlights are to be replaced with Smart LED streetlights/ floodlights.

Also, NMC has installed approx. 80 LED Street Lights on the “Smart Strip” which to be integrated with intended “Smart Strip” Smart Light System.

Currently, existing traditional street light system is facing issues like

1. Lack of information about the real time status of the street lights and area.
2. Lack of proper system for monitoring and operating lights ON/OFF schedule
3. Lack of system to optimize the efficiency of street light system as per requirement
4. Managing the independent unit of street light in terms of turning ON/OFF, fault detection & replacement etc.

NMC intends to implement an energy efficient LED based Street Light System bundled with motion & ambient light sensors along with Smart controllers within the existing landscape (pertaining to “Smart Strip”) to

1. Minimize energy usage
2. Operate the street lights in three state (Dual DIM/Bright/Off) automatically as per the real time field requirement
3. Automated controls that make adjustments based on conditions such as occupancy or daylight availability
4. Policy driven central controlling mechanism to regulate the street lighting intensity and energy consumption
5. Real time tracking and management of street lights

### Scope of Work

#### “Smart Strip” Smart Light System Landscape –

1. Total No. of Traditional Street Lights (Sodium) – 320
2. Total No. of High Masts with LED – 7 (~49 lights)
3. Total No. of LED Street Lights – 80

#### Details of Work –

##### 1. Business Solution

The SI shall be responsible for Supply, Design, Development, Testing, Implementation (as per the functional requirement specifications mentioned in the RFP document), Operation and Maintenance (5 years) of “Smart Strip” Smart Light Management System which includes:

ICT Intervention		Key Features
Smart Lighting		LED base Smart lighting to support automated lighting and sensing
		Ability to control individual Outdoor LED lights on the street for turning on, off and dimming
		Ability to create policies for Outdoor City lighting based on time of the day, ambient lighting conditions and other scenarios and events on the street

ICT Interventions	Key Features
	Monitor voltage, current, voltage fluctuation, power consumption for each individual light as well as a group of lights and city areas
	Detect failures of LED bulbs and other circuitry and generate alarms for maintenance automatically.

### I. Smart Lighting Operation Management System –

The system shall provision for:

- a. Individual switch on/off, increase/decrease luminosity as per ground situation
- b. Policy based Operation example: set up policies like light up alternate lights during low traffic density, increase the luminosity of the lights as per the dullness of the day lights
- c. Real time status of the Smart Lighting System on a city map view of Lighting Operations Management software

### 2. Infrastructure Solution

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

- a. LED based Smart lighting fixtures with all fittings & fixtures (Motion & Ambient light sensors)
- b. Smart Controllers mechanism
- c. Network connectivity for street light poles, high masts, controllers and city operation center

#### 1.5.5 Smart Traffic

NMC is the nodal agency for regulating and managing the entire road network and traffic signals in the city. Currently, there are total 151 traffic junctions enabled with traffic signals either with LED or with GLS lights. Majorly, city is having a large proportion of 4Arm traffic junction just like every other Indian city.

Currently, city is lacking on advanced ICT enabled Traffic Management and Communication tools/systems and existing system is facing few problems like:

1. Traffic congestion and huge waiting time
2. No right of way to 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
5. Absence of street level public information & communication channel
6. Absence of central control mechanism to monitor & regulate the city traffic flow

NMC intends to implement a Smart Traffic Management System within the existing landscape (pertaining to “Smart Strip”) to

1. Automate the process of traffic management by optimally configuring the traffic junction lights on real time basis
2. Minimize the traffic congestions and waiting time
3. Centrally controlled traffic management system to ensure smooth movement of emergency services like ambulance, police etc.
4. Managed & coordinated VIP movements
5. Availability of traffic data to further analyse and optimize the traffic flow
6. Real Time Incident Message and Advisory Messages to citizens
7. Improved Traffic Regulation

## Scope of Work

### “Smart Strip” Smart Traffic System Landscape –

1. Total SMART Strip Length – approx. 5.8 km
2. Total No. of Traffic Junctions (with traffic lights) – 10
  - I. No. of 5Arm Junction – 1
  - II. No. of 4Arm Junction – 9

### Details of Work –

#### 1. Business Solution

The SI shall be responsible for Supply, Design, Development, Testing, Implementation (as per the functional requirement specifications mentioned in the RFP document), Operation and Maintenance (5 years) of “Smart Strip” Smart Traffic Management System which includes:

ICT Interventions	Key Features
Smart Traffic	Adaptive Traffic Management System
	Public Announcement System
	Variable Message System

#### I. Adaptive Traffic Control System –

ATCS shall offers traffic signal optimizing functionalities, use data from vehicle detectors and optimize traffic signal settings resulting much improved vehicle delays and stops. The system shall also allow interconnecting individual area controllers and thus enabling traffic monitoring and regulating functionality from the central location.

The primary objective of the system is to 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.

All junctions under Adaptive Traffic Control System shall be provided vehicle detection system & communication equipment. This shall allow each intersection controller to be monitored from central control for proper functionality. Any corrective action can be initiated either

automatically based on status information or by an operator. The real time detection data shall be communicated to the central control station by each controller.

ATCS shall be driven central control system, on real time basis, with the capacity to calculate the optimal cycle times, effective green time ratios, and change intervals for all system traffic signal controllers connected to it which in turn can also work in configurable manner. These calculations shall be based upon assessments carried out by the ATCS central application software running on a City Operation Center based on the data and information gathered by vehicle detectors at strategic locations at the intersections controlled by the system

## **II. Public Address System –**

PA system shall be placed at critical locations as identified by purchaser with the “SMART Strip” to make important announcements for the public. It shall be able to broadcast messages across all PA systems or specific announcement shall 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 which shall drive the speakers. The system shall also contain the control software which shall be used to control/ monitor all the components of the system which include Controller, Calling Station & keypad, Amplifier (Mixing & Booster).

The SI 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.

## **III. Variable Message System (VaMS) –**

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 SI 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 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.

The VaMS shall be managed and operated from the Command Control Centre / City Operations Center, 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 100m and various angles on the road.

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

## **2. Infrastructure Solution**

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

- a. Adaptive Traffic Control System traffic junction Unit -
  - i. Traffic signal controllers
  - ii. Vehicle detectors
  - iii. Communication network
  - iv. ATCS edge application software
- b. Public Address System
- c. Variable Message System
- d. Network connectivity for traffic junctions, controllers, PA system, VaMS, and city operation center

### **1.5.6 Smart Parking**

Residents of Nagpur are facing trouble in finding parking space and frequently find themselves without change. With Smart Parking solution that alerts residents where the open parking space is available and allows them to pay with mobile wallets or bank wallets or mobile wallets like payTM etc through their mobile phones.

#### **Challenges with Conventional Parking :**

1. High Parking Search Time
2. Traffic Congestion on Road
3. Poor Usage of Parking Space
4. Poor Occupancy in Parking Lot
5. Less Revenue / collection
6. Less effective parking operations
7. High Parking violations
8. Accidental Hazards
9. Stress to user & dissatisfaction
10. Pollution – High Emission of gas
11. No flexibility in Parking Charges
12. Suspicious parking / Lack of security arrangements in Parking
13. No real time tracking, data/report for analysis for future need/expansion

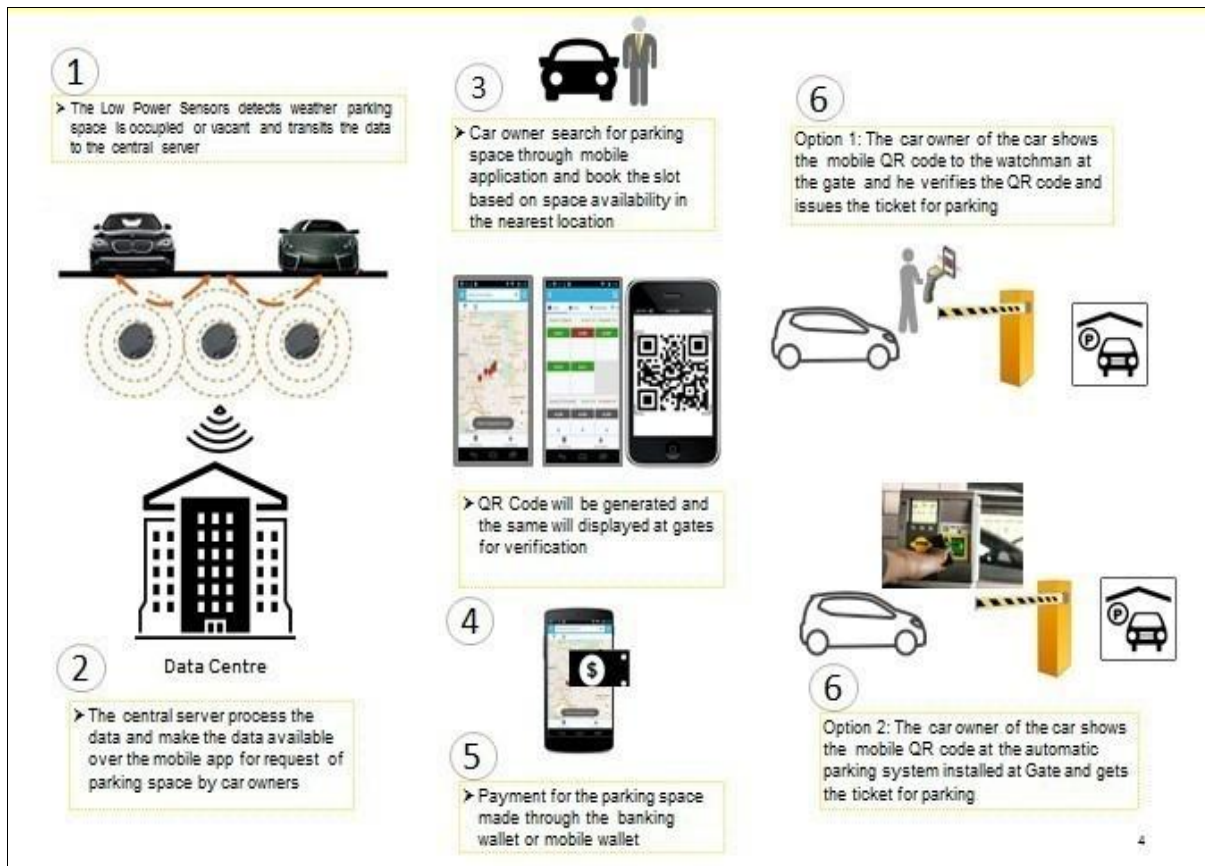
**Value Proposition SMART Parking offers to its Stakeholders :**

<b>Nagpur Municipal Corporation</b>	<b>Nagpur Citizens</b>
<ol style="list-style-type: none"><li>1. Increase quality of life</li><li>2. Improvement in citizen's parking experience &amp; satisfaction</li><li>3. More efficient use of parking</li><li>4. Reduces illegal parking</li><li>5. Reduces revenue leakages</li><li>6. Reduces Man power cost</li></ol>	<ol style="list-style-type: none"><li>1. Simplifies Payment</li><li>2. Easily finds the parking space</li><li>3. Time saving</li><li>4. Avoid traffic congestion</li></ol>

**SMART Parking – Solution & its Benefits:**

1. Mobile App can help in finding parking space quickly & easily
2. Finding parking space with clear & simple directions reducing traffic Congestion. Parking violation detection real time system also help.
3. Assisting user in directing to correct parking slot help in correct parking at correct slot, making optimal usage of parking space
4. Real time update of entry & exit of vehicle improve occupancy
5. Improved Parking Occupancy increase collection
6. Ease of payment improve collection & save time
7. Real time info, Smart meters, ease of payment improve parking operations
8. Clear, simple directions & ease in parking reduces road accidents
9. Improved user satisfaction by saving time, effort & cost
10. Less parking search time reduces emission of gases & control pollution
11. Provision for demand responsive parking charges – Higher charges during peak hours etc
12. Correct detections of violations & suspicious parking/over duration parking
13. Availability of data & Analysis for growing need for expansion or more parking slots; subsequently required measures to handle problem

**Smart Parking Solution Overview –**



1. Installation of sensors in each bay, which register whether the bay is occupied or vacant.
2. This information is relayed live to local and Central system where parking management application is hosted, which collates and analyses the data.
3. Then this information is relayed instantaneously to signage & digital-display screens which let customers know how many spaces are available and give directions for locating them, throughout the car park, until the driver arrives at a vacant space.

**Smart Parking Key Components –**

**1. Parking Sensors**

1. Installation of parking sensors in the allotted space which communicate information wirelessly

**2. Wireless Sensor Networks Module**

1. Collect sensor data
2. Check parking slot state in real-time
3. Send parking slot information to embedded webserver

**3. Embedded Web-Server**

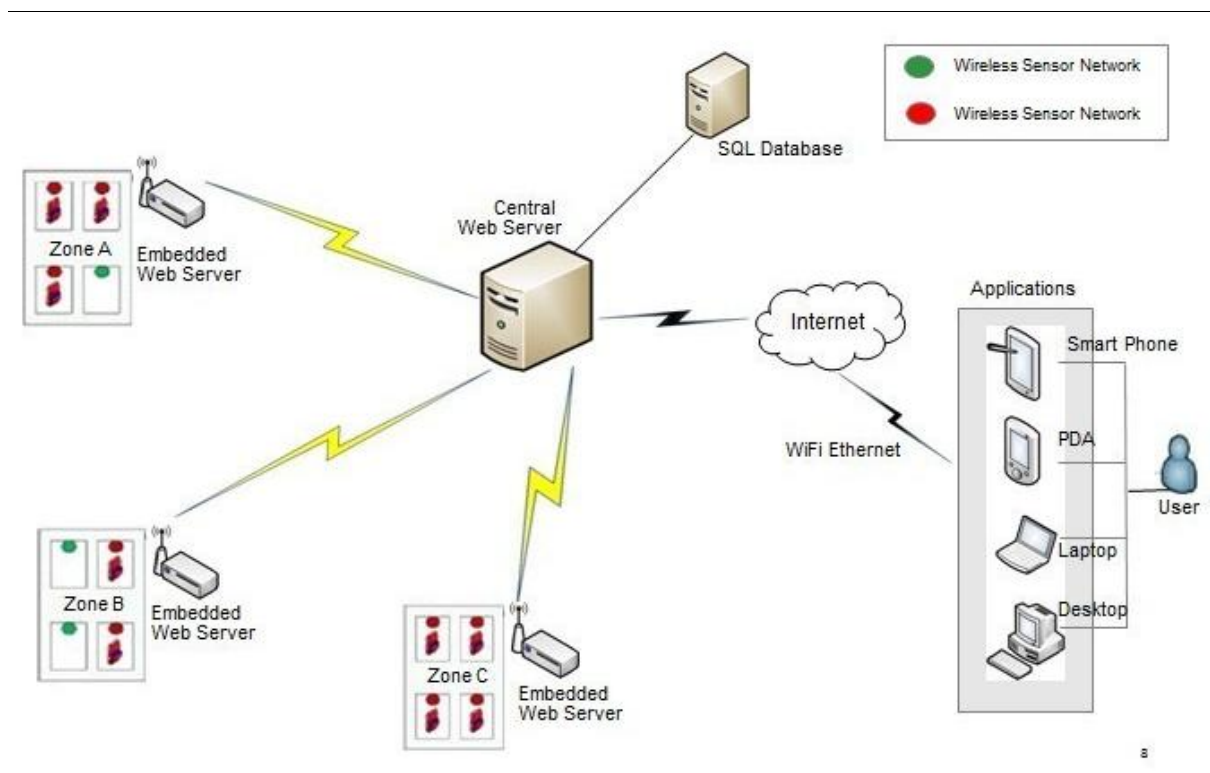
1. Receive parking information from wireless sensor networks
2. Send them with the position of parking zone to central web-server
3. Generate ticket of the mobile users via QR code reading
4. Allocate parking space to local users and generate ticket
5. Integrated with local display unit and boom barrier

**4. Mobile Device of Driver**



1. Connect to central web-server
  2. Receive parking slot information from central web-server
  3. Display the real-time monitoring of parking slots state in the nearest parking zone
- 5. Central Web-Server**
1. Receive parking slot information from embedded web-server
  2. Display the parking slots state of parking zone in real-time
  3. Send information to mobile phone application
  4. Save information in SQL database
  5. Reporting & analytics
- 6. Boom Barrier & Digital Display Unit**
1. Shall receive information from the Parking Information System and operate accordingly

**Smart Parking Technical Architecture –**



**1.5.7 Environmental Sensors**

Environmental pollution, particularly of the air, is nowadays a major problem that unknowingly affects lives in the cities. As clear focus of building Nagpur as one of the finest example of SMART city, NMC believes it is important that citizens know of the air that they breathe. Nagpur Citizens & visitors to Nagpur City can enjoy unique experiences that keep them feeling good by knowing city’s environment condition at different locations.

With reference to installation of Variable Message System, NMC also intends to:

1. Install environment sensors (as per the technical specifications) to display environment related information at various strategic locations
2. The environment sensors shall be integrated with the central control system to capture and display/ provide feed on Temperature, Humidity, Pollutants like SoX, NoX, CoX, etc Noise Pollution, Electromagnetic Radiation etc. The data it collects is location-marked.
3. Various environment sensors shall sense the prevailing environment conditions and send the data to the integrated control system where real time data resides and the same shall be made available to various other departments and applications for decision making.
4. Then this information is relayed instantaneously to signage – large, clear, digital-display screens which let customers know regarding the prevalent environmental conditions.
5. Further environmental sensors recorded data shall be used by Smart Environment Mobile application to enable user for alarm management and notification of environmental details on real time basis.

#### **Components of Environmental Sensors:**

- 1. Wireless Environment Sensor**
  - Collect sensor data
  - Send recorded information to central system
- 2. Central System**
  - Receive information from environment sensors
  - Display the information on real-time basis
  - Send information to mobile phone application
  - Save information in SQL database
- 3. Mobile Device of Driver**
  - Connect to central web-server
  - Receive environment information from central system
  - Alarm management and safe environment mode features
- 4. Digital Display Unit**
  - Shall receive information from the central application System and operate accordingly

#### **1.6 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., it should 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.

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 Nagpur Smart City Initiative it is intended to cover various disparate systems including:

- City WiFi
- City Surveillance
- City Kiosk
- "Smart Strip" Solutions
- GIS Application

However, the platform shall support adding more layers of solutions seamlessly with minimal effort which purchaser intends to develop in time to come like:

- Water Management
- Open City Card
- Smart Health
- Disaster Management

On the Integrated Operation Platform (IOP), the system shall provide Standard Operating Procedures (SOPs), step-by-step instructions based on the purchasers 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

## **1.7 GIS Map for Nagpur City**

SI shall be responsible for providing GIS map of Nagpur city which shall be a common platform across all the solutions including City WiFi, City Kiosk, City Surveillance, "Smart Strip" etc. SI shall also be responsible for appropriate geo referencing & geo tagging on the map covering

all relevant assets like WiFi Hotspots, bus stops, bus routes, bin locations, transfer stations, street poles, high masts, traffic signals, PA & VaMS systems etc.

- a) GIS maps shall be comprehensive and detailed up to roads, houses and building level
- b) Solution shall ensure that the GIS Map provides complete details of the city in various digital vector layers and allows for zoom in/out, searching, and retrieving information capabilities.
- c) GIS details procured shall include the following data with attributes:
  - i. Road Network.
    - o City Arterial Roads.
    - o Streets
  - ii. Administrative boundaries
    - o District and Sub District Boundary.
    - o Town Boundaries.
  - iii. Building footprints and names
  - iv. Points of Interest data to include:
    - o Health services (Hospitals, Blood Banks, and Diagnostics center, Ambulance Services, Other Medical Services, etc.)
    - o Community services (fire stations, police stations, banks, ATMs, post offices, educational facilities, Govt. Buildings etc.)
    - o Business Centres (Shopping malls, markets, commercial complexes etc.
    - o Residential areas (Apartments, housing societies etc.)
    - o Transportation (bus stops/Terminus, parking areas, petrol bunk, metro stations, seaports, airports etc.)
    - o Recreation facilities (Restaurants, theatres, auditoriums etc.)
    - o Other utilities such as travel and tourism facilities, religious places, burial grounds, solid waste locations etc.
    - o Local landmarks with locally called names.
  - v. Land-Cover
    - o Green areas
    - o Open Areas
    - o Water bodies
  - vi. Address layers (Pin code, Locality, Sub-locality, House numbers/names)
  - vii. Geo referencing of all the assets pertaining to the aforementioned solutions as required shall be provided by the SI
  - viii. All data procured shall be imported into a central database.
  - ix. System Functionalities:
    - o The system shall have capability to perform attribute or spatial queries on data from selected sources.
    - o The system shall support Mobile platform, Android and Windows
    - o The system shall support clipping and/or downloading of raster and vector data by authorised users.
    - o The system shall support server side Geo-processing
    - o The application shall have standard and modern map navigation tools of pan and zoom.

- The application shall support client requests to print the spatial data.
  - The system shall be able to support industry-standard data types, industry-standard data formats, unlimited file size or database size, unlimited number of files or tables, and unlimited number of users.
  - The system shall support geocoding and reverse geocoding
  - The system shall allow the users to perform advanced spatial analysis like geocoding, routing, buffering and attribute based analysis.
  - The application shall have standard and modern map navigation tools of pan and zoom.
  - The system shall have the facility wherein the user can opt to view in 2D or 3D environment.
  - The system shall be compatible with Google Maps, Bing™ Maps, Micro Station, AutoCAD, MGE, FRAMME, G/Technology, ODBC source.
  - The System shall support hierarchical legends, and watermarks
  - The application shall allow users to views the data with different symbology styles like differentiating feature records based on attributes or types, dynamic label generation with conflict detection, and translucency of all raster data and area colour fill.
  - The system shall allow the user to find Address
  - The system shall be able to consume real-time enterprise published spatial data. It shall be able to consume the third-party published OGC web-services.
- x. Application shall be OGC compliant for database and shall provision conversion to other database formats.
  - xi. GIS base maps shall be installed on work stations at Control Command Centre and City Operation centre. GIS maps and data replication shall happen from central system remotely.
- d) Provide GIS engine that shall allow operators to get an overview of the entire system and access to all the system components dynamically. GIS engine shall enable dynamic view of the location and status of resources and objects/sensors. System shall enable authorized user to open a new incident and to associate the incident with its geographic location automatically, via GIS display.

## 1.8 OPERATION CENTRES

### 1.8.1 Overview

With a view of enabling respective stakeholders to operate all the above-specified Smart City Components, following Operations Centers have been proposed:

1. City Operations Center
2. Command and Control Center for City Surveillance
3. Network Operations Center

Snapshot of location and stakeholders operating each of the proposed Operations Centers is as follows:

Operations Center	Location	Stakeholder operating the Center
-------------------	----------	----------------------------------

City Operations Center with Server Room	As specified by Nagpur Municipal Corporation specified	Nagpur Municipal Corporation
Command and Control Center with Server Room	As specified by Nagpur Police specified	Nagpur Police
Network Operations Center (NOC)	As specified by Nagpur Municipal Corporation * <i>NOC and Helpdesk is proposed to be co-located with City Operations Center</i>	System Integrator

## 1.8.2 City Operations Center

### Overview

The City Operation Center shall facilitate with a viewing and controlling mechanism for the selected field locations in a fully automated environment for optimized monitoring, regulation and enforcement of services. The City Operation Center shall be accessible by the operators and concerned authorized entities with necessary authentication credentials. The City Operation Center shall be used and manned by the NMC officers to keep surveillance on civil issues.

Location for City Operation Center shall be at the designated location as decided by the Purchaser.

- i. The City Operation Center shall provide a comprehensive system for planning, optimizing resources and response pertaining to the standard functions of Nagpur Municipal Corporation. The minimum technical specification for the equipment required at the Command Control Center is listed in this RFP.
- ii. The SI shall be required to undertake detailed assessment of the requirements at the city operation center and commission required IT and non-IT infrastructure and also carry out the civil/ electrical work as required.
- iii. The data and surveillance network share the same physical infrastructure with guaranteed bandwidth for each individual segment. The software components provide comfortable monitoring experience, easy extraction of clips, and management of storage.
- iv. The video feed from the surveillance cameras shall be received at the City Operation Center where a video wall shall be installed for viewing relevant feed from the surveillance cameras. The operator on each of the workstation shall be able to work on multiple monitors at the same time, for which there is requirement of multi screens with one computer (specifically three) to be installed on work desks (appropriate furniture) with appropriate multi monitor mounts.
- v. Similarly, inputs/feeds from the different components of "Smart Strip" shall be received at City Operation Center video wall for monitoring, tracking and decision support purpose on real time basis supported with GIS technology. Further, operators shall be

working on their respective monitors for assessing the inputs and triggering actions at ground level.

Purchaser shall carry out a detail assessment of the proposed design solution and review design for the Command Control Center, Server Room and City Operation Center on the parameters of overall Design, Safety & Security and reserves it right to accept, reject or suggest for modifications on the proposed solution.

### **1.8.3 Network Operations Center**

As part of this RFP, it is proposed that a Network Operations Center (hereinafter referred to as “NOC”) shall be established for monitoring the network infrastructure laid as part of City Network Backbone across all locations as proposed in this RFP.

The minimum requirements/ specifications for the NOC area are detailed in the following sub-sections. While it is mandatory for the SI to meet these minimum requirements, if the SI estimates that a particular requirement would need a higher category of equipment, the SI shall provision for the same in the bid response. The SI shall however provide basis for arriving at the solution being proposed as part of the bid response.

The NOC shall analyse network problems, perform troubleshooting, communicate with various NMC 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 SI 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 SI includes the following:

- a. City Operation Centre area consists of the Network Operation Area (NOC), Server Room, Reception area (including Visitor’s gallery), material handling room, Conference room.
- b. Design, supply, installation and setting up of the necessary basic Infrastructure for City Operation Centre area in terms of civil, interior, electrical and Air-Conditioning System, Fire Prevention, Detection and Suppression System, Lighting system, Power, multi-layer Physical Security infrastructure like bio-metric based access-control system, CCTV/ surveillance systems etc.
- c. SI shall take consultation and approval of Purchaser/authorized entity, for the interior layout and material to be procured for the operations area.
- d. Primary responsibilities of NOC personnel shall include but not limited to:
  - o Network Supervision and Monitoring
    - Monitor the complete network 24/7, to keep network and systems functioning in a stable operation mode
  - o Configuration Management
    - Ensure the proper configuration of network, systems and applications for the provision of reliable and high quality end-user services
  - o 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

- Performance Management
  - Provide efficient performance management procedures ensuring a reliable, high-quality network performance and service
- 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
- 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
- IT and DB Management
  - Day-to-day management of all OSS systems, IT systems and databases (administration, backups)
- Security Management
  - Define and implement security policies, guidelines, and best practices, and check for compliance with security regulations
- Quality Management
  - Define quality management policies, and ensure implementation and usage for competitive quality of service
- Workforce Management
  - Manage field personnel to ensure timely interventions and respect of the preventive maintenance plan
- Network Inventory Management
  - Ensure consistent management of network equipment, and accurate, up-to-date documentation of it
- Spare Parts Management
  - Manage spare part handling and logistics to minimize repair/swap turn-around times for defective items, and keep low CAPEX for spare parts and consumables
- Asset Inventory Management
  - Ensure consistent inventory management for all assets including infrastructure, buildings, tools, spares, and equipment
- Repair and Return
  - Receive and repair defective boards, return repaired or replacement boards.

#### **1.8.3.1 Features of NOC**

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

#### **1.8.3.2 Services to be provided through NOC**



The Services Catalogue for the NOC has to be prepared by the SI and get a sign off from Purchaser. Indicative list of services that have to be provided through the NOC are mentioned below.

### **1. Enterprise Management System**

- a. In addition to hardware and software requirements as prescribed in this RFP, SI is required to also design size, supply, implement and maintain an Enterprise Management System (EMS). The EMS shall be able to support the proposed hardware and software components deployed over the tenure of the Contract. The EMS shall be capable of providing early warning signals to the Helpdesk Agents on the performance issues, and future infrastructure capacity augmentation. The EMS shall also support single pane / dashboard with visibility across multiple areas of applications for monitoring.
- b. SI is required to design, supply, install, customize, test, implement, rollout and maintain the EMS application and hardware as per the requirements of this RFP.
- c. SI is expected to provide EMS encompassing but not limited to the following functions:
  - Configuration Management
  - Fault Management
  - Incident, Problem and Change Management
  - Asset Management
  - Remote Control
  - SLA Management & Monitoring
  - Performance Management
  - Monitoring Backup and Management
  - Event Management
  - Server, Storage and other Infrastructure Management
  - Monitor network components of the LAN & WAN
  - Network Link Monitoring
  - Other modules as required by SI to meet the requirements of the RFP

### **2. Monitoring, Management & Reporting with Enterprise Management System (EMS)**

The EMS system shall provide for the regular monitoring, management and reporting of the ICT infrastructure of the project assets installed in the respective operations centre as well as field locations. It shall be noted that the activities performed by the SI shall be under the supervision of Purchaser. The EMS system shall have the following features including but not limited to and as well act as authoritative source for the same:

Following functionalities are desired by use of such EMS tools:

- Availability Monitoring, Management and Reporting
- Performance Monitoring, Management and Reporting
- Helpdesk Monitoring, Management and Reporting
- Traffic Analysis
- Asset Management
- Incident Management and RCA reporting.
- Change and Configuration management.

#### **I. Availability - Monitoring, Management and Reporting**

This part of the specification shall ensure the monitoring, management, and reporting parameters of availability like discovery, configuration, faults, service levels etc. including but not limited to the following:

### **Discovery, Configuration and Faults**

#### **i. Monitoring and Management**

- a. The proposed system shall support multiple types of discovery like IP range discovery – including built-in support for IPv6 , Seed router based discovery and discovery whenever new devices are added with capability to exclude specific devices
- b. The proposed system shall support exclusion of specific IP addresses or IP address ranges.
- c. The system shall provide discovery & inventory of physical network devices like Layer-2 & Layer-3 switches, Routers and other IP devices and shall provide mapping of LAN & WAN connectivity.
- d. The discovery shall be able to identify and model of the ICT asset.
- e. The proposed system shall provide a detailed asset report, organized by vendor name and device, listing all ports for all devices. The proposed system shall provide sufficient reports that identify unused ports in the managed network infrastructure that can be reclaimed and reallocated. The proposed system shall also intelligently determine which ports are operationally dormant.
- f. The proposed system shall determine device availability and shall exclude outages from the availability calculation with an option to indicate the reason.
- g. The proposed system shall provide out of the box root cause analysis.
- h. The proposed system shall include the ability to monitor and visualize a virtualized system infrastructure by discovering and monitoring virtual machines and providing ability to depict the logical relationships between virtual servers and virtual machines.
- i. The proposed solution shall detect virtual server and virtual machine configuration changes and automatically update topology and shall raise alarm when VM migrations happen between hosts.
- j. The proposed solution shall have the ability to collect data from the virtual systems without solely relying on SNMP.
- k. The proposed solution shall support an architecture that can be extended to support multiple virtualization platforms and technologies.
- l. The proposed system shall support SNMPv3-based network discovery and management out-of-box without the need for any external third-party modules.
- m. The proposed system shall be able to administer configuration changes to network elements by providing toolkits to automate the following administrative tasks of effecting configuration changes to network elements like Capture running & startup configuration, Upload configuration etc.

#### **ii. Reporting**

- a. The proposed system shall provide sufficient reports pertaining to asset and change management, alarms and availability of critical network resources as well as network response times for critical links.
- b. The proposed system shall able to perform real-time or scheduled capture of

device configurations. It shall also provide features to capture, view & upload network device configuration.

- c. The proposed system shall able to store historical device configurations captured in the database and thereby enable comparison of current device configuration against a previously captured configuration as well as compare the current configuration against any user-defined standard baseline configuration policy.
- d. The proposed system shall be able to monitor compliance & enforce change control policies within the diverse infrastructure by providing data & tools to run compliance reports, track & remediate violations, and view history of changes.
- e. The proposed tool shall display configuration changes differences in GUI within central Console. Also this shall be able to identify which user has made changes or modifications to device configurations using the Interface.

## **II. Service Level Management**

### **i. Monitoring and Management**

- a. The proposed service management system shall provide a detailed service dashboard view indicating the health of each of the departments / offices in the organization and the health of the services they rely on as well as the SLAs.
- b. The system shall provide an outage summary that gives a high level health indication for each service as well as the details and root cause of any outage.
- c. The system shall be capable of managing IT resources in terms of the business services they support, specify and monitor service obligations, and associate users/Departments/ Organizations with the services they rely on and related Service/Operational Level Agreements. Presently, services shall include E-mail, Internet Access, Intranet and other services hosted.
- d. The Service Level Agreements (SLAs) definition facility shall support defining a set of one or more service that specify the Service obligations stipulated in an SLA contract for a particular time period (weekly, monthly, and so on).
- e. SLA violation alarms shall be generated to notify whenever an agreement is violated or is in danger of being violated.
- f. The system shall provide the capability to designate planned maintenance periods for services and take into consideration maintenance periods defined at the IT resources level. In addition the capability to exempt any service outage from impacting an SLA shall be available.

### **ii. Reporting**

- a. The reports supported shall include one that monitors service availability (including Mean Time to Repair (MTTR), Mean Time between Failure (MTBF), and Maximum Outage Time thresholds) and the other that monitors service transaction response time.
- b. The system shall provide a historical reporting facility that shall allow for the generation of on-demand and scheduled reports of Service related metrics with capabilities for customization of the report presentation.
- c. The system shall provide for defining service policies like Service Condition High\Low Sensitivity, Port Status High\Low Sensitivity shall be provided out of the box.
- d. The system shall display option on Services, Customer, SLA's, SLA templates.

The customer definition option shall allow associating a service or an SLA with a customer.

### **III. Performance - Monitoring, Management and Reporting**

The proposed performance management system shall integrate network, server and database performance information and alarms in a single console and provide a unified reporting interface for network components.

#### **A. Network Performance Monitoring, Management and Reporting**

##### **i. Monitoring and Management**

- a. The System shall have all the capabilities of a Network Management System which shall provide Real time network monitoring and Measurement offend-to-end Network performance & availability to define service levels and further improve upon them.
- b. The tool shall provide a live exceptions list displaying the various health and threshold exceptions that are occurring in the managed infrastructure.
- c. The tool shall have the capability to configure different polling speeds for different devices in the managed infrastructure with capability to poll critical devices
- d. The proposed system shall use intelligent alarm algorithms to learn the behaviour of the network infrastructure components over a period of time

##### **ii. Reporting**

- a. The Network Performance Management console shall provide a consistent report generation interface from a single central console.
- b. This central console shall also provide all required network performance reports (including latency, threshold violations, packet errors, availability, bandwidth utilization etc.) for the network infrastructure. The proposed system shall identify over-and under-utilized links and assist in maximizing the utilization of current resources
- c. The proposed system shall enable complete customization flexibility of performance reports for network devices and monitored servers.
- d. The proposed system shall provide an integrated performance view for all the managed systems and networks along with the various threshold violations alarms in them.
- e. The proposed system shall provide the following reports as part of the base performance monitoring product out-of-the-box to help network operators quickly identify device problems quickly. The following charts like mentioned below shall be available for routers: Backplane Utilization, Buffer Create Failures, Buffer Hits, Buffer Misses, Buffer Utilization, Bus Drops, CPU Utilization, Fan Status, Free Memory, Memory Utilization, Packets by Protocol, and Packets out.
- f. The proposed system shall be able to auto-calculate resource utilization baselines for the entire managed systems and networks and allow user to set corresponding upper and lower threshold limits.

### **IV. Application Performance Monitoring, Management and Reporting**

##### **i. Monitoring and Management**

- a. The proposed solution shall proactively monitor all user transactions for any web-application hosted; detect failed transactions; gather evidence necessary for triage and diagnosis of problems that affect user experiences and prevent completion of critical business processes
- b. The proposed solution shall determine if the cause of performance issues is inside the application, in connected back-end systems or at the network layer.
- c. The proposed solution shall correlate performance data from HTTP Servers (external requests) with internal application performance data
- d. The proposed solution shall see response times based on different call parameters. For example the proposed solution shall be able to provide CPU utilization metrics
- e. The proposed Solution shall be able to correlate Application changes (code and configuration files) with change in Application performance.
- f. The proposed solution shall allow data to be seen only by those with a need to know and limit access by user roles
- g. The proposed solution shall measure the end users' experiences based on transactions
- h. The proposed solution shall give visibility into user experience without the need to install agents on user desktops.
- i. The solution shall be deployable as an appliance-based system acting as a passive listener on the network thus inducing zero overhead on the network and application layer.
- j. The proposed solution shall be able to provide the ability to detect and alert which exact end users experience HTTP error codes such as 404 errors or errors coming from the web application.

**ii. Reporting**

- a. The proposed system shall be able to detect user impacting defects and anomalies and reports them in real-time for Slow Response Time, Fast Response time, Low Throughput, Partial Response, Missing component within transaction
- b. The proposed system shall be able to instantly identify whether performance problems like slow response times are within or outside the server room without having to rely on network monitoring tools.
- c. The proposed system shall be able to provide trend analysis reports and compare the user experience over time by identifying transactions whose performance or count has deteriorated over time.

**V. Systems and Database Performance Monitoring, Management and Reporting**

**i. Monitoring and Management**

- a. The proposed system shall addresses management challenges by providing centralized management across physical and virtual systems
- b. The proposed system shall be able to monitor various operating system parameters such as processors, memory, files, processes, file systems, etc. where applicable, using agents on the servers to be monitored.
- c. It shall be possible to configure the operating system monitoring agents to monitor based on user-defined thresholds for warning/critical states and escalate events to event console of enterprise management system.
- d. It shall also be able to monitor various operating system parameters depending

on the operating system being monitored yet offer a similar interface for viewing the agents and setting thresholds.

- e. The proposed solution shall support monitoring Processors, File Systems, Log Files, System Processes, and Memory etc.
- f. The proposed tool shall provide Process and NT Service Monitoring wherein if critical application processes or services fail, administrators are immediately alerted and processes and services are automatically re-started
- g. The proposed tool shall be able to provide Log File Monitoring which enables administrator to watch system logs and text log files by specifying messages to watch for. When matching messages gets logged, the proposed tool shall notify administrators and enable to take action like sending an email.
- h. The proposed database performance management system shall integrate network, server & database performance management systems and provide the unified view of the performance state in a single console.
- i. It shall be able to automate monitoring, data collection and analysis of performance from single point.
- j. It shall also provide the ability to set thresholds and send notifications when an event occurs, enabling database administrators (DBAs) to quickly trace and resolve performance-related bottlenecks.

**ii. Reporting**

- a. The proposed system shall provide Performance Management and Reporting — Provides real-time and historical performance of physical and virtual environments enabling customers gain valuable insights of a given virtual container of the relative performance of a given Virtual Machine compared to other Virtual Machines, and of the relative performance of groups of Virtual Machines .
- b. Role based Access — Enables role-based management by defining access privileges according to the role of the user.
- c. The proposed Virtual Performance Management system shall integrate latest virtualization technologies

**VI. Helpdesk - Monitoring, Management and Reporting**

- a. The proposed helpdesk system shall provide flexibility of logging, viewing, updating and closing incident manually via web interface.
- b. The proposed helpdesk system shall support ITIL processes like request management, problem management, configuration management and change order management with out-of-the-box templates for various ITIL service support processes.
- c. Each incident shall be able to associate multiple activity logs entries via manual update or automatic update from other enterprise management tools.
- d. The proposed helpdesk system shall be able to provide flexibility of incident assignment based on the workload, category, location etc.
- e. Each escalation policy shall allow easy definition on multiple escalation levels and notification to different personnel via window GUI/console with no or minimum programming.
- f. The proposed helpdesk system shall provide grouping access on different security knowledge articles for different group of users.

- g. The proposed helpdesk system shall have an updateable knowledge base for technical analysis and further help end-users to search solutions for previously solved issues.
- h. The proposed helpdesk system shall support tracking of SLA (service level agreements) for call requests within the help desk through service types.
- i. The proposed helpdesk system shall be capable of assigning call requests to technical staff manually as well as automatically based on predefined rules, and shall support notification and escalation over email, web etc.
- j. The proposed helpdesk system shall integrate tightly with the Knowledge tools and CMDB and shall be accessible from the same login window.
- k. It shall support remote management for end-user & allow analysts to do the desktop sharing for any system located anywhere, just connected to internet.
- l. Remote desktop sharing in the system shall be agent less & all activity shall be automatically logged into the service desk ticket.
- m. It shall allow IT team to create solution & make them available on the end – user login window for the most common requests

## **VII. Traffic analysis**

- a. The proposed system shall enable the server room to centrally manage user access privileges and allow deploying baseline security policies so that the right people have access to the right information. It shall proactively secure access to data and applications located on Linux, UNIX and Windows system servers
- b. The traffic analysis system shall be from same OEM providing Network Fault & Performance Management System.
- c. The tool shall support Flow monitoring and traffic analysis for NetFlow, J-Flow, sFlow, Netstream, IPFIX technologies.
- d. The solution shall provide a central web based integration point for NetFlow based reporting and able to report from a single console across 100,000 interfaces.
- e. The solution shall be of the type passive monitoring without a need to install any probe or collector for data collection.
- f. The solution shall provide the following NetFlow based metrics:
  - o Rate, Utilization, Byte Count, IP hosts with automatic DNS resolution, IP conversation pairs with automatic DNS resolution, Router/interface with automatic SNMP name resolution, IPv6 addresses
  - o The proposed solution shall keep historical rate and protocol data for a minimum of 12 months (most recent) in its current long term operating database. All data in that database shall have a maximum 15 minute window granularity without roll up. A user shall be able to select any 15 minute window over the last 12 months and display unique utilization and protocol data for every monitored interface.
  - o The proposed solution shall keep historical rate and protocol data for a minimum of 30 days (most recent) in its short term operating database. All data in that database shall have a maximum 1 minute window granularity. A user shall be able to select any 1 minute window over the last 30 days and display unique utilization and protocol data for every monitored interface.
  - o All custom reports from the long term database shall support the ability to be run manually or scheduled to run automatically at user selectable intervals.
  - o All reports shall be generated and displayed directly by the system from a

- common interface.
- The system shall allow via API for Excel to download data to generate reports.
- The system shall be able to restrict views and access for defined users to specific routers, interfaces, and reports.
- The user shall be able to generate reports from the long term database based on specific thresholds defined by the user where the threshold can be compared to rate, utilization or volume of every monitored interface as a filter for inclusion in the report.
- The proposed system shall be capable of automatically detecting anomalous behaviour such as virus attacks or unauthorized application behaviour.
- The system shall analyze all NetFlow traffic and alert via SNMP trap and syslog of any suspicious activity on the network.
- The system shall provide the ability to group interfaces into functional groups based on any user criteria. The grouping function shall allow users to create group names and add interfaces into that grouping for reporting purposes. Once created, these groups shall be available for selection within custom reports as a mechanism to include multiple interfaces without individual selection for inclusion.
- The monthly view shall provide a graphical representation of the level of utilization for each fifteen minute interval of each day of the month.
- The user shall be able to easily change the data type of the main interface view to a tabular format showing the increase or decrease of traffic generated by that protocol as a percentage using discrete least-squares approximation to find a best fit line of growth

#### **VIII. Asset Management through EMS**

- a. Ability to provide inventory of hardware and software applications on end-user desktops, including information on processor, memory, OS, mouse, keyboard, etc. through agents installed on them
- b. Ability to have reporting capabilities; provide predefined reports and ability to create customized reports on data in the inventory database. Report results could be displayed as lists or graphs
- c. Ability to provide the facility to collect custom information from desktops
- d. Ability to provide facility to recognize custom applications on desktops
- e. Facility for the administrator to register a new application to the detectable application list using certain identification criteria. Shall enable the new application to be detected automatically next time the inventory is scanned
- f. Facility for User self-registration.
- g. Ability to support configuration management functionality using which standardization of configuration can be achieved of all the desktops
- h. Software metering shall be supported to audit and control software usage. Shall support offline and online metering.
- i. Ability to support dynamic grouping of enabling assets to be grouped dynamically based on some pre-defined criteria e.g. a group shall be able to display how many and which computers has a specific application installed. As and when a new computer gets the new application installed it shall dynamically add to the group
- j. Ability to use the query tool to identify specific instances of concern like policy



violation (presence of prohibited programs / games and old versions, etc.), inventory changes (memory change, etc.) and accordingly it could perform several actions as reply. These actions could be (a) sending a mail, (b) writing to files, sound an alarm (c) message to scroll on monitor screen if the administrator, etc.

- k. Facility to track changes by maintaining history of an asset
- l. Ability to have web based console

The proposed EMS solution shall provide comprehensive and end -to-end management of all the components for each service including all the hardware devices, Network, Systems and Application infrastructure.

**Note:** It is mandatory that all the modules for the proposed EMS Solution shall provide out-of-the-box and seamless integration capabilities. SI shall provide the specifications and numbers for all necessary Hardware, OS & DB (if any) which is required for an EMS to operate effectively.

### **IX. Incident Management and Root Cause Analysis Reporting**

Incident management shall be governed by the change management and configuration management policy of DIT Govt. of Maharashtra. The policy shall be shared with the SI.

- a. An information security incident is an event (or chain of events) that compromises the confidentiality, integrity or availability of information. All information security incidents that affect the information or systems of the enterprise (including malicious attacks, abuse / misuse of systems by staff, loss of power / communications services and errors by users or computer staff) shall be dealt with in accordance with a documented information security incident management process.
- b. Incidents shall be categorized and prioritized. While prioritizing incidents the impact and urgency of the incident shall be taken into consideration.
- c. It shall be ensured that the incident database is integrated with Known Error Database (KeDB), Configuration Management Database (CMDB). These details shall be accessible to relevant personnel as and when needed.
- d. Testing shall be performed to ensure that recovery action is complete and that the service has been fully restored.
- e. The SI shall keep the end users informed of the progress of their reported incident.
- f. When the incident has been resolved, it shall be ensured that the service desk records of the resolution steps are updated, and confirm that the action taken has been agreed to by the end user. Also, unresolved incidents (known errors and workarounds) shall be recorded and reported to provide information for effective problem management.
- g. Information security incidents and weaknesses associated with information systems shall be communicated in a manner allowing timely corrective action to be taken.
- h. The SI shall conduct regular reviews on performance of incident management activities against documented Key Performance Indicators (KPI's).
- i. The incident management activities shall be carried out by the SI in such a way that an incident is resolved within the agreed time schedule.

- j. Root Cause Analysis (RCA) shall be conducted by the SI.
- k. Controls related to incident management need to be implemented and each implemented control shall have a documentary evidence to substantiate and demonstrate effective implementation.

## **X. Change and Configuration Management**

Change and configuration management shall be governed by the change management and configuration management policy of DIT Govt. of Maharashtra.

- a. Change management provides information on changes, and enables better control of changes to reduce errors and disruption in services.
- b. All changes shall be initiated using change management process; and a Request For Change (RFC) shall be created. All requests for change shall be evaluated to determine the impact on business processes and IT services, and to assess whether change shall adversely affect the operational environment and introduce unacceptable risk.
- c. The SI shall ensure that all changes are logged, prioritized, categorized, assessed, authorized, planned and scheduled to track and report all changes.
- d. Ensure review of changes for effectiveness and take actions agreed with interested parties. Requests for change shall be analyzed at planned intervals to detect trends. The results and conclusions drawn from the analysis shall be recorded and reviewed to identify opportunities for improvement.
- e. Controls related to change management need to be implemented and each implemented control shall have a documentary evidence to substantiate and demonstrate effective implementation.
- f. The roles and responsibilities of the management shall include review and approval of the implementation of change management policies, processes and procedures.
- g. A configuration management database shall be established which stores unique information about each type Configuration Item CI or group of CI.
- h. The Configuration Management Database (CMDB) shall be managed such that it ensures its reliability and accuracy including control of update access.
- i. The degree of control shall maintain the integrity of services and service components taking into consideration the service requirements and the risks associated with the CI.
- j. Corrective actions shall be taken for any deficiencies identified in the audit and shall be reported to the management and process owners.
- k. Information from the CMDB shall be provided to the change management process and the changes to the CI shall be traceable and auditable.
- l. A configuration baseline of the attached CI shall be taken before deployment of a release into the live environment. It shall be stored in the safe environment with appropriate access control.
- m. Master copies of CI shall be recorded in the CMDB and shall be stored in secure physical or electronic libraries which shall be referenced in the configuration records. This shall be applicable to documentations, license information, software and hardware configuration images.

## **XI. EMS Ability to integrate with other services**

The proposed EMS solution shall comply with key integration points out of the box as listed below but not limited to:

- a. The proposed network management system shall integrate with the helpdesk system by updating the Asset with CI information to support viewing history or open issues in helpdesk on the particular managed asset and associate an SLA to the ticket in the helpdesk.
- b. The proposed network management system shall attach an asset identifier when submitting a helpdesk ticket. In case the asset is not found in the helpdesk database, it shall be automatically created prior to submitting the ticket. NMS console shall show associated helpdesk ticket number for the alarms that generated those tickets.
- c. SLA's violation on monitored end user response time shall open a helpdesk incident out of the box.
- d. Proposed Application Performance Solution shall integrate with Network Fault Monitoring Solution to forward Application Performance Threshold violation alarms in proposed Network Fault Manager Console.
- e. The proposed Fault Management Solution shall support integration with proposed help desk or trouble ticketing system such that integration shall Associates alarms with Service Desk tickets in the following ways:
  - o Manually creates tickets when requested by Fault Management GUI operators
  - o Automatically creates tickets based on alarm type
  - o Provides a link to directly launch a Service Desk view of a particular ticket created by alarm from within the Network Operation console.
  - o Maintains the consistency of the following information that is shared between alarm and its associated Service Desk ticket including status of alarms and associated tickets and current assignee assigned to tickets.
  - o Helpdesk ticket number created for associated alarm shall be visible inside Network Operation Console. It shall be integrated in a way that Helpdesk incident can be launched once clicked on ticket number for associated alarm from within Network Operation Console.
  - o The proposed virtual performance management system shall integrate with proposed Network Management and Performance Management system out of the box.
  - o The proposed NMS shall provide unified workflow between the fault and performance management systems including bi-directional and context-sensitive navigation, such as
  - o Navigate from the Topology View to At-a-Glance or Trend Reports for any asset
  - o Navigate from the Alarm View to At-a-Glance, Trend or Alarm Detail Reports
  - o Proposed Performance Management system shall feed in discovery from Devices already discovered in Network Management Module without starting discovery process again all together in Performance Management Engine this shall reduce effort of having to perform discovery on both Fault and Performance Management Engines .Discovery can be synchronized.

**Note:**

SI shall use Industry standard EMS tools recognized by analysts (like Gartner, Forrester etc.) to report desired SLA's for availability & performance of Various IT Components including Networks, Systems and OS. Keeping in view the intricacies involved in the installation, configuration and day to day use of various components of Enterprise Management System covered under this document, the proposed EMS solution shall involve tools to ensure smooth/seamless integration and out of the box workability of the offered solution.

## **XII. ICT Assets Hardening**

All the ICT assets shall be hardened as per the Hardening guidelines and industry leading practices. Remove all unauthorised software, utilities, and services. All required logs shall be configured and monitored

### **1.8.3.3 NOC Operations Centre**

As part of this RFP, it is proposed that a Network Operations Center (hereinafter referred to as "NOC") shall be established for monitoring the network infrastructure laid as part of City Network Backbone across all locations as proposed in this RFP.

The minimum requirements/ specifications for the NOC area are detailed in the following sub-sections. While it is mandatory for the SI to meet these minimum requirements, if the SI estimates that a particular requirement would need a higher category of equipment, the SI shall provision for the same in the bid response. The SI shall however provide basis for arriving at the solution being proposed as part of his bid.

The NOC shall analyse network problems, perform troubleshooting, communicate with various NMC 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 SI 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 SI includes the following:

- a. Design, supply, installation and setting up of the necessary basic Infrastructure for City Operation Centre area in terms of interior, electrical and Air-Conditioning System, Fire Prevention, Detection and Suppression System, Lighting system, Power, multi-layer Physical Security infrastructure like bio-metric based access-control system, CCTV/ surveillance systems etc.
- b. SI shall take consultation and approval of Purchaser/authorized entity, for the interior layout and material to be procured for the operations area.
- c. Primary responsibilities of NOC personnel shall include but not limited to:
  - o Network Supervision and Monitoring
    - Monitor the complete network 24/7, to keep network and systems functioning in a stable operation mode
  - o Configuration Management
    - Ensure the proper configuration of network, systems and applications for the provision of reliable and high quality end-user services
  - o 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

- Performance Management
  - Provide efficient performance management procedures ensuring a reliable, high-quality network performance and service
- Service and Network Provisioning
  - Define all necessary actions to be performed when a request for a new customer service is issued, and control the actions performed at NOC level or field level until completion
- 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
- IT and DB Management
  - Day-to-day management of all OSS systems, IT systems and databases (administration, backups)
- Security Management
  - Define and implement security policies, guidelines, and best practices, and check for compliance with security regulations
- Quality Management
  - Define quality management policies, and ensure implementation and usage for competitive quality of service
- Workforce Management
  - Manage field personnel to ensure timely interventions and respect of the preventive maintenance plan
- Network Inventory Management
  - Ensure consistent management of network equipment, and accurate, up-to-date documentation of it
- Spare Parts Management
  - Manage spare part handling and logistics to minimize repair/swap turn-around times for defective items, and keep low CAPEX for spare parts and consumables
- Asset Inventory Management
  - Ensure consistent inventory management for all assets including infrastructure, buildings, tools, spares, and equipment
- Repair and Return
  - Receive and repair defective boards, return repaired or replacement boards.

#### **1.8.3.3.1 Features of NOC**

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

#### **1.8.3.3.2 Services to be provided through NOC**

The Services Catalogue for the NOC has to be prepared by the SI and get a sign off from Purchaser. Indicative list of services that have to be provided through the NOC are mentioned below.

### **1. Enterprise Management System**

- a. In addition to hardware and software requirements as prescribed in this RFP, SI is required to also design size, supply, implement and maintain an Enterprise Management System (EMS). EMS shall support the proposed hardware and software components deployed over the tenure of the Contract. EMS shall be capable of providing early warning signals to the Helpdesk Agents on the performance issues, and future infrastructure capacity augmentation. EMS shall also support single pane / dashboard with visibility across multiple areas of applications for monitoring.
- b. SI is expected to provide EMS encompassing but not limited to the following functions:
  - Configuration Management
  - Fault Management
  - Incident, Problem and Change Management
  - Asset Management
  - Remote Control
  - SLA Management & Monitoring
  - Performance Management
  - Monitoring Backup and Management
  - Event Management
  - Server, Storage and other Infrastructure Management
  - Monitor network components of the LAN & WAN
  - Network Link Monitoring
  - Other modules as required by SI to meet the requirements of the RFP

### **2. Monitoring, Management & Reporting with Enterprise Management System (EMS)**

The EMS system shall provide for the regular monitoring, management and reporting of the ICT infrastructure of the project assets installed in the operations centre as well as field locations. EMS system shall have following features including but not limited to and as well act as authoritative source for the same:

Following functionalities are desired by use of such EMS tools:

- Availability Monitoring, Management and Reporting
- Performance Monitoring, Management and Reporting
- Helpdesk Monitoring, Management and Reporting
- Traffic Analysis
- Asset Management
- Incident Management and RCA reporting.
- Change and Configuration management.

### **XIII. Availability - Monitoring, Management and Reporting**

This part of the specification shall ensure the monitoring, management, and reporting parameters of availability like discovery, configuration, faults, service levels etc. including but not limited to the following:

**i. Monitoring and Management**

- a. The proposed system shall support multiple types of discovery like IP range discovery – including built-in support for IPv6 , Seed router based discovery and discovery whenever new devices are added with capability to exclude specific devices
- b. The proposed system shall support exclusion of specific IP addresses or IP address ranges.
- c. The system shall provide discovery & inventory of physical network devices like Layer-2 & Layer-3 switches, Routers and other IP devices and shall provide mapping of LAN & WAN connectivity.
- d. The discovery shall be able to identify model of the ICT asset.
- e. The proposed system shall provide a detailed asset report, organized by vendor name and device, listing all ports for all devices. The proposed system shall provide sufficient reports that identify unused ports in the managed network infrastructure that can be reclaimed and reallocated. The proposed system shall also intelligently determine which ports are operationally dormant.
- f. The proposed system shall determine device availability and shall exclude outages from the availability calculation with an option to indicate the reason.
- g. The proposed system shall provide out of the box root cause analysis.
- h. The proposed system shall include the ability to monitor and visualize a virtualized system infrastructure by discovering and monitoring virtual machines and providing ability to depict the logical relationships between virtual servers and virtual machines.
- i. The proposed solution shall detect virtual server and virtual machine configuration changes and automatically update topology and shall raise alarm when VM migrations happen between hosts.
- j. The proposed solution shall have the ability to collect data from the virtual systems without solely relying on SNMP.
- k. The proposed solution shall support an architecture that can be extended to support multiple virtualization platforms and technologies.
- l. The proposed system shall support SNMPv3-based network discovery and management out-of-box without the need for any external third-party modules.
- m. The proposed system shall be able to administer configuration changes to network elements by providing toolkits to automate the following administrative tasks of effecting configuration changes to network elements like Capture running & startup configuration, Upload configuration etc.

**ii. Reporting**

- a. The proposed system shall provide sufficient reports pertaining to asset and change management, alarms and availability of critical network resources as well as network response times for critical links.
- b. The proposed system shall able to perform real-time or scheduled capture of device configurations. It shall also provide features to capture, view & upload network device configuration.
- c. The proposed system shall able to store historical device configurations captured in the database and thereby enable comparison of current device configuration against a previously captured configuration as well as compare the current configuration against any user-defined standard baseline configuration policy.

- d. The proposed system shall be able to monitor compliance & enforce change control policies within the diverse infrastructure by providing data & tools to run compliance reports, track & remediate violations, and view history of changes.
- e. The proposed tool shall display configuration changes differences in GUI within central Console. Also this shall be able to identify which user has made changes or modifications to device configurations using the Interface.

#### **XIV. Service Level Management**

##### **i. Monitoring and Management**

- a. The proposed service management system shall provide a detailed service dashboard view indicating the health of each of the departments / offices in the organization and the health of the services they rely on as well as the SLAs.
- b. The system shall provide an outage summary that gives a high level health indication for each service as well as the details and root cause of any outage.
- c. The system shall be capable of managing IT resources in terms of the business services they support, specify and monitor service obligations, and associate users/Departments/ Organizations with the services they rely on and related Service/Operational Level Agreements. Presently, services shall include E-mail, Internet Access, Intranet and other services hosted.
- d. The Service Level Agreements (SLAs) definition facility shall support defining a set of one or more service that specify the Service obligations stipulated in an SLA contract for a particular time period (weekly, monthly, and so on).
- e. SLA violation alarms shall be generated to notify whenever an agreement is violated or is in danger of being violated.
- f. The system shall provide the capability to designate planned maintenance periods for services and take into consideration maintenance periods defined at the IT resources level. In addition the capability to exempt any service outage from impacting an SLA shall be available.

##### **ii. Reporting**

- a. The reports supported shall include one that monitors service availability (including Mean Time to Repair (MTTR), Mean Time between Failure (MTBF), and Maximum Outage Time thresholds) and the other that monitors service transaction response time.
- b. The system shall provide a historical reporting facility that shall allow for the generation of on-demand and scheduled reports of Service related metrics with capabilities for customization of the report presentation.
- c. The system shall provide for defining service policies like Service Condition High\Low Sensitivity, Port Status High\Low Sensitivity shall be provided out of the box.
- d. The system shall display option on Services, Customer, SLA's, SLA templates. The customer definition option shall allow associating a service or an SLA with a customer.

#### **XV. Performance - Monitoring, Management and Reporting**

The proposed performance management system shall integrate network, server and database performance information and alarms in a single console and provide a



unified reporting interface for network components.

## **B. Network Performance Monitoring, Management and Reporting**

### **i. Monitoring and Management**

- a. The System shall have all the capabilities of a Network Management System which shall provide Real time network monitoring and Measurement offend-to-end Network performance & availability to define service levels and further improve upon them.
- b. The tool shall provide a live exceptions list displaying the various health and threshold exceptions that are occurring in the managed infrastructure.
- c. The tool shall have the capability to configure different polling speeds for different devices in the managed infrastructure with capability to poll critical devices
- d. The proposed system shall use intelligent alarm algorithms to learn the behaviour of the network infrastructure components over a period of time

### **ii. Reporting**

- a. The Network Performance Management console shall provide a consistent report generation interface from a single central console.
- b. This central console shall also provide all required network performance reports (including latency, threshold violations, packet errors, availability, bandwidth utilization etc.) for the network infrastructure. The proposed system shall identify over-and under-utilized links and assist in maximizing the utilization of current resources
- c. The proposed system shall enable complete customization flexibility of performance reports for network devices and monitored servers.
- d. The proposed system shall provide an integrated performance view for all the managed systems and networks along with the various threshold violations alarms in them.
- e. The proposed system shall provide the following reports as part of the base performance monitoring product out-of-the-box to help network operators quickly identify device problems quickly. The following charts like mentioned below shall be available for routers: Backplane Utilization, Buffer Create Failures, Buffer Hits, Buffer Misses, Buffer Utilization, Bus Drops, CPU Utilization, Fan Status, Free Memory, Memory Utilization, Packets by Protocol, and Packets out.
- f. The proposed system shall be able to auto-calculate resource utilization baselines for the entire managed systems and networks and allow user to set corresponding upper and lower threshold limits.

## **XVI. Application Performance Monitoring, Management and Reporting**

### **i. Monitoring and Management**

- a. The proposed solution shall proactively monitor all user transactions for any web-application hosted; detect failed transactions; gather evidence necessary for triage and diagnosis of problems that affect user experiences and prevent completion of critical business processes
- b. The proposed solution shall determine if the cause of performance issues is inside the application, in connected back-end systems or at the network layer.

- c. The proposed solution shall correlate performance data from HTTP Servers (external requests) with internal application performance data
- d. The proposed solution shall see response times based on different call parameters. For example the proposed solution shall be able to provide CPU utilization metrics
- e. The proposed Solution shall be able to correlate Application changes (code and configuration files) with change in Application performance.
- f. The proposed solution shall allow data to be seen only by those with a need to know and limit access by user roles
- g. The proposed solution shall measure the end users' experiences based on transactions
- h. The proposed solution shall give visibility into user experience without the need to install agents on user desktops.
- i. The solution shall be deployable as an appliance-based system acting as a passive listener on the network thus inducing zero overhead on the network and application layer.
- j. The proposed solution shall be able to provide the ability to detect and alert which exact end users experience HTTP error codes such as 404 errors or errors coming from the web application.

**ii. Reporting**

- a. The proposed system shall be able to detect user impacting defects and anomalies and reports them in real-time for Slow Response Time, Fast Response time, Low Throughput, Partial Response, Missing component within transaction
- b. The proposed system shall be able to instantly identify whether performance problems like slow response times are within or outside the server room without having to rely on network monitoring tools.
- c. The proposed system shall be able to provide trend analysis reports and compare the user experience over time by identifying transactions whose performance or count has deteriorated over time.

**XVII. Systems and Database Performance Monitoring, Management and Reporting**

**i. Monitoring and Management**

- a. The proposed system shall addresses management challenges by providing centralized management across physical and virtual systems
- b. The proposed system shall be able to monitor various operating system parameters such as processors, memory, files, processes, file systems, etc. where applicable, using agents on the servers to be monitored.
- c. It shall be possible to configure the operating system monitoring agents to monitor based on user-defined thresholds for warning/critical states and escalate events to event console of enterprise management system.
- d. It shall also be able to monitor various operating system parameters depending on the operating system being monitored yet offer a similar interface for viewing the agents and setting thresholds.
- e. The proposed solution shall support monitoring Processors, File Systems, Log Files, System Processes, and Memory etc.
- f. The proposed tool shall provide Process and NT Service Monitoring wherein if critical application processes or services fail, administrators are immediately

- alerted and processes and services are automatically re-started
- g. The proposed tool shall be able to provide Log File Monitoring which enables administrator to watch system logs and text log files by specifying messages to watch for. When matching messages gets logged, the proposed tool shall notify administrators and enable to take action like sending an email.
  - h. The proposed database performance management system shall integrate network, server & database performance management systems and provide the unified view of the performance state in a single console.
  - i. It shall be able to automate monitoring, data collection and analysis of performance from single point.
  - j. It shall also provide the ability to set thresholds and send notifications when an event occurs, enabling database administrators (DBAs) to quickly trace and resolve performance-related bottlenecks.

**ii. Reporting**

- a. The proposed system shall provide Performance Management and Reporting — Provides real-time and historical performance of physical and virtual environments enabling customers gain valuable insights of a given virtual container of the relative performance of a given Virtual Machine compared to other Virtual Machines, and of the relative performance of groups of Virtual Machines .
- b. Role based Access — Enables role-based management by defining access privileges according to the role of the user.
- c. The proposed Virtual Performance Management system shall integrate latest virtualization technologies

**XVIII. Helpdesk - Monitoring, Management and Reporting**

- a. The proposed helpdesk system shall provide flexibility of logging, viewing, updating and closing incident manually via web interface.
- b. The proposed helpdesk system shall support ITIL processes like request management, problem management, configuration management and change order management with out-of-the-box templates for various ITIL service support processes.
- c. Each incident shall be able to associate multiple activity logs entries via manual update or automatic update from other enterprise management tools.
- d. The proposed helpdesk system shall be able to provide flexibility of incident assignment based on the workload, category, location etc.
- e. Each escalation policy shall allow easy definition on multiple escalation levels and notification to different personnel via window GUI/console with no or minimum programming.
- f. The proposed helpdesk system shall provide grouping access on different security knowledge articles for different group of users.
- g. The proposed helpdesk system shall have an updateable knowledge base for tech al analysis and further help end-users to search solutions for previously solved issues.
- h. The proposed helpdesk system shall support tracking of SLA (service level agreements) for call requests within the help desk through service types.
- i. The proposed helpdesk system shall be capable of assigning call requests to tech

al staff manually as well as automatically based on predefined rules, and shall support notification and escalation over email, web etc.

- j. The proposed helpdesk system shall integrate tightly with the Knowledge tools and CMDB and shall be accessible from the same login window.
- k. It shall support remote management for end-user & allow analysts to do the desktop sharing for any system located anywhere, just connected to internet.
- l. Remote desktop sharing in the system shall be agent less & all activity shall be automatically logged into the service desk ticket.
- m. It shall allow IT team to create solution & make them available on the end – user login window for the most common requests

## **XIX. Traffic analysis**

- a. The proposed system shall enable the server room to centrally manage user access privileges and allow deploying baseline security policies so that the right people have access to the right information. It shall proactively secure access to data and applications located on Linux, UNIX and Windows system servers
- b. The traffic analysis system shall be from same OEM providing Network Fault & Performance Management System.
- c. The tool shall support Flow monitoring and traffic analysis for NetFlow, J-Flow, sFlow, Netstream, IPFIX technologies.
- d. The solution shall provide a central web based integration point for NetFlow based reporting and able to report from a single console across 100,000 interfaces.
- e. The solution shall be of the type passive monitoring without a need to install any probe or collector for data collection.
- f. The solution shall provide the following NetFlow based metrics:
  - o Rate, Utilization, Byte Count, IP hosts with automatic DNS resolution, IP conversation pairs with automatic DNS resolution, Router/interface with automatic SNMP name resolution, IPv6 addresses
  - o The proposed solution shall keep historical rate and protocol data for a minimum of 12 months (most recent) in its current long term operating database. All data in that database shall have a maximum 15 minute window granularity without roll up. A user shall be able to select any 15 minute window over the last 12 months and display unique utilization and protocol data for every monitored interface.
  - o The proposed solution shall keep historical rate and protocol data for a minimum of 30 days (most recent) in its short term operating database. All data in that database shall have a maximum 1 minute window granularity. A user shall be able to select any 1 minute window over the last 30 days and display unique utilization and protocol data for every monitored interface.
  - o All custom reports from the long term database shall support the ability to be run manually or scheduled to run automatically at user selectable intervals.
  - o All reports shall be generated and displayed directly by the system from a common interface.
  - o The system shall allow via API for Excel to download data to generate reports.
  - o The system shall be able to restrict views and access for defined users to specific routers, interfaces, and reports.
  - o The user shall be able to generate reports from the long term database based on specific thresholds defined by the user where the threshold can be

compared to rate, utilization or volume of every monitored interface as a filter for inclusion in the report.

- The proposed system shall be capable of automatically detecting anomalous behaviour such as virus attacks or unauthorized application behaviour.
- The system shall analyze all NetFlow traffic and alert via SNMP trap and syslog of any suspicious activity on the network.
- The system shall provide the ability to group interfaces into functional groups based on any user criteria. The grouping function shall allow users to create group names and add interfaces into that grouping for reporting purposes. Once created, these groups shall be available for selection within custom reports as a mechanism to include multiple interfaces without individual selection for inclusion.
- The monthly view shall provide a graphical representation of the level of utilization for each fifteen minute interval of each day of the month.
- The user shall be able to easily change the data type of the main interface view to a tabular format showing the increase or decrease of traffic generated by that protocol as a percentage using discrete least-squares approximation to find a best fit line of growth

## **XX. Asset Management through EMS**

- a. Ability to provide inventory of hardware and software applications on end-user desktops, including information on processor, memory, OS, mouse, keyboard, etc. through agents installed on them
- b. Ability to have reporting capabilities; provide predefined reports and ability to create customized reports on data in the inventory database. Report results could be displayed as lists or graphs
- c. Ability to provide the facility to collect custom information from desktops
- d. Ability to provide facility to recognize custom applications on desktops
- e. Facility for the administrator to register a new application to the detectable application list using certain identification criteria. Shall enable the new application to be detected automatically next time the inventory is scanned
- f. Facility for User self-registration.
- g. Ability to support configuration management functionality using which standardization of configuration can be achieved of all the desktops
- h. Software metering shall be supported to audit and control software usage. Shall support offline and online metering.
- i. Ability to support dynamic grouping of enabling assets to be grouped dynamically based on some pre-defined criteria e.g. a group shall be able to display how many and which computers has a specific application installed. As and when a new computer gets the new application installed it shall dynamically add to the group
- j. Ability to use the query tool to identify specific instances of concern like policy violation (presence of prohibited programs / games and old versions, etc.), inventory changes (memory change, etc.) and accordingly it could perform several actions as reply. These actions could be (a) sending a mail, (b) writing to files, sound an alarm (c) message to scroll on monitor screen if the administrator, etc.
- k. Facility to track changes by maintaining history of an asset
- l. Ability to have web based console

The proposed EMS solution shall provide comprehensive and end -to-end management of all the components for each service including all the hardware devices, Network, Systems and Application infrastructure.

**Note:** It is mandatory that all the modules for the proposed EMS Solution shall provide out-of-the-box and seamless integration capabilities. SI shall provide the specifications and numbers for all necessary Hardware, OS & DB (if any) which is required for an EMS to operate effectively.

## **XXI. Incident Management and Root Cause Analysis Reporting**

Incident management shall be governed by the change management and configuration management policy of DIT Govt. of Maharashtra. The policy shall be shared with the SI.

- a. An information security incident is an event (or chain of events) that compromises the confidentiality, integrity or availability of information. All information security incidents that affect the information or systems of the enterprise (including malicious attacks, abuse / misuse of systems by staff, loss of power / communications services and errors by users or computer staff) shall be dealt with in accordance with a documented information security incident management process.
- b. Incidents shall be categorized and prioritized. While prioritizing incidents the impact and urgency of the incident shall be taken into consideration.
- c. It shall be ensured that the incident database is integrated with Known Error Database (KeDB), Configuration Management Database (CMDB). These details shall be accessible to relevant personnel as and when needed.
- d. Testing shall be performed to ensure that recovery action is complete and that the service has been fully restored.
- e. The SI shall keep the end users informed of the progress of their reported incident.
- f. When the incident has been resolved, it shall be ensured that the service desk records of the resolution steps are updated, and confirm that the action taken has been agreed to by the end user. Also, unresolved incidents (known errors and workarounds) shall be recorded and reported to provide information for effective problem management.
- g. Information security incidents and weaknesses associated with information systems shall be communicated in a manner allowing timely corrective action to be taken.
- h. The SI shall conduct regular reviews on performance of incident management activities against documented Key Performance Indicators (KPI's).
- i. The incident management activities shall be carried out by the SI in such a way that an incident is resolved within the agreed time schedule.
- j. Root Cause Analysis (RCA) shall be conducted by the SI.
- k. Controls related to incident management need to be implemented and each implemented control shall have a documentary evidence to substantiate and demonstrate effective implementation.

## **XXII. Change and Configuration Management**

Change and configuration management shall be governed by the change management and configuration management policy of DIT Govt. of Maharashtra.

- a. Change management provides information on changes, and enables better control of changes to reduce errors and disruption in services.
- b. All changes shall be initiated using change management process; and a Request For Change (RFC) shall be created. All requests for change shall be evaluated to determine the impact on business processes and IT services, and to assess whether change shall adversely affect the operational environment and introduce unacceptable risk.
- c. The SI shall ensure that all changes are logged, prioritized, categorized, assessed, authorized, planned and scheduled to track and report all changes.
- d. Ensure review of changes for effectiveness and take actions agreed with interested parties. Requests for change shall be analyzed at planned intervals to detect trends. The results and conclusions drawn from the analysis shall be recorded and reviewed to identify opportunities for improvement.
- e. Controls related to change management need to be implemented and each implemented control shall have a documentary evidence to substantiate and demonstrate effective implementation.
- f. The roles and responsibilities of the management shall include review and approval of the implementation of change management policies, processes and procedures.
- g. A configuration management database shall be established which stores unique information about each type Configuration Item CI or group of CI.
- h. The Configuration Management Database (CMDB) shall be managed such that it ensures its reliability and accuracy including control of update access.
- i. The degree of control shall maintain the integrity of services and service components taking into consideration the service requirements and the risks associated with the CI.
- j. Corrective actions shall be taken for any deficiencies identified in the audit and shall be reported to the management and process owners.
- k. Information from the CMDB shall be provided to the change management process and the changes to the CI shall be traceable and auditable.
- l. A configuration baseline of the attached CI shall be taken before deployment of a release into the live environment. It shall be stored in the safe environment with appropriate access control.
- m. Master copies of CI shall be recorded in the CMDB and shall be stored in secure physical or electronic libraries which shall be referenced in the configuration records. This shall be applicable to documentations, license information, software and hardware configuration images.

### **XXIII. EMS Ability to integrate with other services**

The proposed EMS solution shall comply with key integration points out of the box as listed below but not limited to:

- a. The proposed network management system shall integrate with the helpdesk system by updating the Asset with CI information to support viewing history or open issues in helpdesk on the particular managed asset and associate an SLA to the ticket in the helpdesk.

- b. The proposed network management system shall attach an asset identifier when submitting a helpdesk ticket. In case the asset is not found in the helpdesk database, it shall be automatically created prior to submitting the ticket. NMS console shall show associated helpdesk ticket number for the alarms that generated those tickets.
- c. SLA's violation on monitored end user response time shall open a helpdesk incident out of the box.
- d. Proposed Application Performance Solution shall integrate with Network Fault Monitoring Solution to forward Application Performance Threshold violation alarms in proposed Network Fault Manager Console.
- e. The proposed Fault Management Solution shall support integration with proposed help desk or trouble ticketing system such that integration shall Associates alarms with Service Desk tickets in the following ways:
  - o Manually creates tickets when requested by Fault Management GUI operators
  - o Automatically creates tickets based on alarm type
  - o Provides a link to directly launch a Service Desk view of a particular ticket created by alarm from within the Network Operation console.
  - o Maintains the consistency of the following information that is shared between alarm and its associated Service Desk ticket including status of alarms and associated tickets and current assignee assigned to tickets.
  - o Helpdesk ticket number created for associated alarm shall be visible inside Network Operation Console. It shall be integrated in a way that Helpdesk incident can be launched once clicked on ticket number for associated alarm from within Network Operation Console.
  - o The proposed virtual performance management system shall integrate with proposed Network Management and Performance Management system out of the box.
  - o The proposed NMS shall provide unified workflow between the fault and performance management systems including bi-directional and context-sensitive navigation, such as
  - o Navigate from the Topology View to At-a-Glance or Trend Reports for any asset
  - o Navigate from the Alarm View to At-a-Glance, Trend or Alarm Detail Reports
  - o Proposed Performance Management system shall feed in discovery from Devices already discovered in Network Management Module without starting discovery process again all together in Performance Management Engine this shall reduce effort of having to perform discovery on both Fault and Performance Management Engines .Discovery can be synchronized.

**Note:**

SI shall use Industry standard EMS tools recognized by analysts (like Gartner, Forrester etc.) to report desired SLA's for availability & performance of Various IT Components including Networks, Systems and OS. Keeping in view the intricacies involved in the installation, configuration and day to day use of various components of Enterprise Management System covered under this document, the proposed EMS solution shall involve tools to ensure smooth/seamless integration and out of the box workability of the offered solution.



#### **XXIV. ICT Assets Hardening**

All the ICT assets shall be hardened as per the Hardening guidelines and industry leading practices. Remove all unauthorised software, utilities, and services. All required logs shall be configured and monitored

##### **1.8.3.3.3 NOC Operations Centre**

Location for the NOC shall be specified by Nagpur Municipal Corporation. It is expected by the SI to provide details of space and other resources including power required at the location as part of their bid response.

The detailed specification for NOC is listed below:

- a. SI shall provision for 10 seats in the NOC room of approximately 1200 sq. ft. of carpet area. The SI shall provide the necessary infrastructure such as furniture, fixtures, PSTN phones, other services with the following per Workstation:
  - o Data- 4 ports
  - o Voice- 2 ports
  - o Raw Power- 2 Nos., 5/ 15 Amps
  - o UPS Power- 3 Nos., 5/ 15 Amps
- b. The NOC operations area requires round the clock monitoring and therefore the officials shall be provisioned for comfortable and ergonomically designed modular office furniture, one white board, 1 set of trolley type storage space (3/ 4 drawer unit) with 3 sets of keys, etc.
- c. NOC operation room shall have finished floor with blinds, Fire rated glass window, Furniture etc. NOC operation room shall be planned as elevated floor with steps arrangement for each seating rows.
- d. Thin clients to be used by individuals operating and administering the NOC as per technical specification
- e. NOC operation area shall have split comfort air-conditioning system with redundancy level of N+1.
- f. NOC operation area shall have proximity readers for entry and Push switches for exit.
- g. NOC operation area shall have CCTV system (fixed dome variable cameras) at entry and exit points.
- h. SI needs to provide the 3 column x 2 row video wall in NOC room as per the specifications.
- i. NOC room shall have stepped flooring arrangement.
- j. Wiring and cabling
- k. Any other utilities or equipment required to establish a state of the art NOC operations area shall be provided by the SI without any additional cost.

## 1.9 Helpdesk

SI shall provide the operational support for all the locations, through a suitable helpdesk system, to ensure that the solution is functioning as intended and that all problems associated with operation are resolved satisfactorily during the contract period. The SI shall provide a web enabled helpdesk management system with SMS and email based alert system for the Helpdesk Call management and SLA reporting. SI shall be required to setup a centralized helpdesk at two locations i.e. one at Command Control Center specifically for City Surveillance, and one at City Operation Center for rest of the solutions.

SI shall provision for the infrastructure necessary for managing the Help Desk including rent charges for Toll-free telephone line(s) at the Help Desk location. SI shall provide multiple channels to log a complaint such as Toll-free lines, landlines, helpdesk tool, E-mail, direct walk-in etc. Outage of any component shall be calculated as a time between logging the call and closing the call.

A helpdesk is envisaged to be provided for the resolution of technical queries by internal users. Typical helpdesk activities (indicative) shall include, but not limited to:

1. Deployment of sufficient manpower to attend the helpdesk requests for extending technical support on hardware, network, application etc. to users
2. Deployment of web-based tool for the helpdesk
3. Provide Help Desk facility for agreed SLAs for reporting technical incidents / issues / problems with the system. Help desk facility shall be provided through Toll-free lines, landlines, helpdesk tool, E-mail, direct walk-in etc.
4. Implement a call logging system in line with the severity levels as per the SLAs. The Help desk shall log user calls related to system and assign an incident/ call ID number. Severity shall be assigned to each call as per the SLAs.
5. Track each incident / call to resolution.
6. Escalate the calls, to the appropriate levels, if necessary as per the escalation matrix agreed upon with purchaser/authorized entity
7. Analyse the incident / call statistics and provide monthly reports including but not limited to:
  - i. Type of incidents / calls logged
  - ii. Incidents / calls resolved
  - iii. Incidents / calls open
8. Helpdesk Solution shall further have the capability to upload frequently asked questions and solutions.

Helpdesk becomes the central collection point for service staff contact and control of the problem, change, and service management processes. This includes both incident management and service request management. This shall be the first level of support (L1).

It is also expected that a second level of centralized support (L2) shall also be maintained at the same location from where the various zones/wards can be serviced in case of problem escalation. If a problem is not resolved by telephone/help desk tool and the User declares the problem to be of an emergency nature, SI shall dispatch a Field Service Staff member who shall provide On-site Support Service according to service levels given.

The Helpdesk shall act as a single point of contact for all users whether for service requests, incidents or problems. It shall encompass Helpdesk, Asset Management and Vendor Management. In addition, it shall offer a focused approach for delivering integrated Service Management and provide an interface for other functions in IT Services Continuity Management like Maintenance Contracts, Software Licenses etc.

SI shall implement effective Helpdesk Management procedures to leverage the knowledge gained in providing faster and better solutions, create knowledge bases and prevent recurrence of problems.

#### **i. Helpdesk Capacity**

SI is required to provide a minimum 3 seater helpdesk at Command Control Center and a minimum of 2 seater helpdesk at City Operation center during all operation hours as specified in the RFP. However, if the SI believes that in order to meet the SLAs, additional capacity is required, the same may be provided by the SI. It is also to be noted any supervisors required for the Helpdesk Operators shall be over and above the minimum operators mentioned above.

#### **ii. Shift Timings**

The SI shall operate the Central Helpdesk for the entire tenure of the Contract as follows:

<b>Category</b>	<b>Shift</b>	<b>Type of Helpdesk Support</b>	<b>Type of Field Support</b>
Helpdesk at Control Command Center	Shift 1	On-premise	On-call
	Shift 2	On-premise	On-call
	Shift 3 (night shift)	On-premise	On-call
Helpdesk at City Operation Center	Shift 1	On-premise	On-call
	Shift 2	On-premise	On-call
	Shift 3 (night shift)	On-call	On-call

#### **iii. Helpdesk Operators**

The SI is required to provide Operators at Helpdesk for operating and managing the Helpdesk as specified in this RFP. The Operators shall perform various activities including:

- Understanding the query/issue in the reported request. Query could be related to the following:
  - hardware including issues related to desktop/laptop, printer/multi-function device, local server, routers/switches
  - application including login and password issues, accessing a particular module, navigation assistance, report generation assistance
  - network including internet/intranet and end-user device connectivity
- Providing information / clarification on the spot in case of an informational query or providing necessary troubleshooting assistance in case of a logged issue
- In case of technical issues for which a resolution is not possible instantly, the operator shall submit the request into the system for escalation and further action by the SI's team

- Process all service requests, dispatch them to field personnel who shall perform the follow up

#### **iv. Field Support Staff**

The SI is required to provide Field Support Staff for undertaking all activities on field to complete a call logged by a User. SI is expected to deploy enough number of Field Support Staff to ensure that SLAs as specified in the RFP are met.

#### **v. IT / Non IT Infrastructure and application software for Helpdesk**

The SI shall be responsible for procurement, installation, commissioning and operations & maintenance of helpdesk including supply & installation of IT / Non IT infrastructure along with necessary application software (as per indicative BOM) required for the smooth functioning of the Central Helpdesk at both the location

### **1.10 Site Preparation for Command Control Center, Server Room, Network Operation Center, City Operation Center & Helpdesk**

The SI shall be required for complete site preparation, installation and commissioning for Command Control Center along with server room, City Operation Center along with server room, Network Operations Center and Helpdesk as per the requirement in consultation with the purchaser but not limited to the following:

#### **1.10.1.1.1 Civil and Architectural work**

The scope for civil work in this RFP is to furnish the Command Control Center, City Operation Center and Server Room, in all aspects. The furnishing includes but not limited to the following:

- Cutting and chipping of existing floors
- Trench works
- Masonry works
- Hardware and metals
- Glazing
- Paint work
- False flooring
- False ceiling
- Storage
- Portioning
- Doors and locks
- Painting
- Fire proofing all surfaces
- Cement concrete works
- Insulation

All material to be used shall be of fine quality ISI marked unless otherwise specified

#### **1.10.1.1.2 False Ceiling**

The SI shall install the top false ceiling with 1' 6" of space from the actual room ceiling. This false ceiling shall house A/C ducts (if required) and cables of electrical lighting, firefighting, and CCTV. Appropriate pest control measures shall be taken to keep pests at bay.

#### **1.10.1.1.3 Raised flooring**

The SI shall be responsible for raised flooring and provide for suitable pedestal and under structure designed to withstand various static and rolling loads subjected to it in server racks. The entire raised floor shall have laminated floor covering and beadings on all sides of the panel.

#### **1.10.1.1.4 Electrical Distribution System**

The SI shall be responsible for proper and uninterrupted working and shall ensure this by having the Server room power distribution system with redundancy at three levels:

- Two incoming HT feeder supply from different sub-stations. Even if one feeder is down, the other one keeps power available.
- Emergency Diesel- Generator backup on failure of both main feeders
- UPS system with battery bank for critical loads
- Connection between UPS system and the network switch racks shall be redundant. No single point of failure shall exist in the power connectivity between network racks and UPS system.

#### **1.10.1.1.5 Air Conditioning and Natural Convection**

Since server room is a critical area, precision air conditioning system shall be exclusively installed to maintain the required temperature. The A/C shall be capable of providing sensible cooling capacities at ambient temperature and humidity with adequate air flow. The task of the SI shall include (but not limited to):

- Connecting the indoor unit with the mains electrical point
- Connecting indoor and outdoor units mechanically ( with 18 G hard gauge copper piping)
- Connecting indoor and outdoor unit electrically

The air conditioner shall be linked to secondary power supply as well to prevent them from shutting down in case of power outage.

#### **1.10.1.1.6 UPS requirements and features**

UPS system shall provide a redundant power supply to the following needs:

- Servers and important network and storage equipment
- Access control, Fire Detection & suppression system and surveillance system

The system shall be automatic with power supply from the mains and automatic switchover to DG set as secondary source for the server room. The specifications of UPS are provided in this RFP.

#### **1.10.1.1.7 Diesel Generator set**

The diesel generator set shall be in N+1 redundancy mode where N = 1. Detailed minimum specifications of the DG set are provided in this RFP. The SI shall be responsible for regular operations and maintenance of the DG set. The SI shall be responsible for but not limited to:

- Fuel
- Preventive maintenance
- Corrective maintenance
- AMC, if any
- Replacement of any parts etc.

#### **1.10.1.1.8 Electrical work for Server room**

The electrical cabling work shall include the following:

- Main electrical panel in server room
- Power cabling
- UPS distribution board
- UPS point wiring
- Power cabling for utility component and utility points etc.
- Online UPS
- Separate Earth pits for the component
- The SI shall use fire retardant cables of rated capacity exceeding the power requirements of existing and proposed components to be used at maximum capacity.
- All materials to conform to IS standards as per industry practice

#### **1.10.1.1.9 Fire Detection and Suppression System**

The facility shall be equipped with adequate and advanced Fire Detection and Suppression system. The system shall raise an alarm in the event of smoke detection. The system shall have proper signage, response indicators and hooters in case of an emergency. The system shall be based as per NFPA standards.

The facility is to be equipped with gas based (Suitable for server room environments) fire suppression system appropriately sized for the given size of the server room.

#### **1.10.1.1.10 Access control system**

The Biometric/Access card based Access Control System shall be deployed with the objective of allowing entry and exit to and from the premises to authorized personnel only with appropriate door locks and controller assemble connected with BMS system. The system deployed shall be based on proximity as well as biometric technology for critical areas and proximity technology for non-critical areas.

#### **1.10.1.1.11 CCTV system**

The SI shall provide CCTV system within the Server room and Command and Control Center on 24X7 bases. All important areas of the Server room, Command and Control Center along with the non-critical areas like locations for DG sets, entry exit of Command Center, Entry and Exit of building premises need to be under constant video surveillance. Monitoring cameras shall be installed strategically to cover all the critical areas of all the respective locations.

#### **1.10.1.1.12 Water leak detection system**

The Water Leak Detection System shall be installed to detect any seepage of water into the critical area and alert the security control room for such leakage. It shall consist of water leak detection cable and alarm module. The cable shall be installed in the ceiling and floor areas around the periphery.

#### **1.10.1.1.13 Building Management system**

The Building Management System (BMS) shall be implemented for effective management, monitoring and integration of various components like Access Control System, fire detection system etc.

The BMS shall perform the following general functions including but not limited to:

- Building Management and control
- Data collection and archival
- Alarm event and management
- Trending
- Reports and MIS generation
- Maintenance and complaint management

The scope shall include designing, supplying and installation of Building Management System.

#### **1.10.1.1.14 Rodent Repellent**

The entry of rodents and other unwanted pests shall be controlled using non-chemical, non-toxic devices. Ultrasonic pest repellents shall be provided in the false flooring and ceiling to repel the pests without killing them. However the SI shall conduct periodic pest control using chemical spray once in a quarter as a contingency measure to effectively fight pests.

## **2. Handholding and Training**

In order to strengthen the staff, structured capacity building programmes 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 NMC & 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 CCC. These officers shall be handling emergency situations with very minimal turnaround time.

- a. SI shall prepare and submit detailed Training Plan and Training Manuals to purchaser/authorized entity for review and approval.
- b. Appropriate training shall be carried out as per the User Training Plan prepared in detail stating the number of training sessions to be held per batch of trainees, course work for the training program, coursework delivery methodologies and evaluation methodologies in detail.
- c. SI shall be responsible for necessary demonstration environment setup including setup of cameras, WiFi, kiosk and "Smart Strip" solutions to conduct end user training. End user training shall include all the equipment including but not limited to all the applications and infrastructure at CCC, SR, City Operation Center & Surveillance Locations. End user

training shall be conducted at a centralized location or any other location as identified by purchaser with inputs from the SI.

- d. SI 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.
- e. SI shall impart operational and technical training to internal users on solutions being implemented to allow them to effectively and efficiently use the surveillance system.
- f. SI shall prepare the solution specific training manuals and submit the same to purchaser for review and approval. Training Manuals, operation procedures, visual help-kit etc. shall be provided in English language.
- g. SI shall provide training to selected officers of the purchaser covering functional, technical aspects, usage and implementation of the products and solutions.
- h. SI 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.
- i. An annual training calendar shall be clearly chalked out and shared with the purchaser along with complete details of content of training, target audience for each year etc.
- j. SI 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.
- k. The SI 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 the SI.
- l. Systematic training shall be imparted to the designated trainees that shall help them to understand the concept of solution, the day-to-day operations of overall solution and maintenance and updating of the system to some extent. This shall be done under complete guidance of the trainers provided by the SI.
- m. Time Schedule and detailed program shall be prepared in consultation with NMC and respective authorized entity (Police). In addition to the above, while designing the training courses and manuals, SI 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.
- n. SI is required to deploy a Master Trainer who shall be responsible for planning, designing and conducting continuous training sessions.
- o. Training sessions and workshops shall comprise of presentations, demonstrations and hands-on mandatorily for the application modules.
- p. Purchaser shall be responsible for identifying and nominating users for the training. However, SI shall be responsible for facilitating and coordinating this entire process.
- q. SI shall be responsible for making the feedback available for the purchaser/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 SI shall re-conduct the same training at no extra cost.

**Types of Trainings:** Following training needs is identified for all the project stakeholders:

### **1. Basic IT training**

This module shall include components on fundamentals of:

1. Computer usage,



2. Network,
3. Desktop operations,
4. User admin,
5. Application installation,
6. Basic computer troubleshooting etc.

## **2. Initial Training as part of Project Implementation**

- I. Functional Training
  1. Basic IT skills
  2. Video Management Software, Video Analytics, ANPR, “Smart Strip” solutions etc.
  3. Software Applications (City Operation Center and Command & Control Center)
  4. Mobile Surveillance Vehicle
  5. Networking, Hardware Installation
  6. Centralized Helpdesk
  7. Feed monitoring
- II. Administrative Training
  1. System Administration Helpdesk, FMS, BMS Administration etc.
  2. Master trainer assistance and handling helpdesk requests etc.
- III. Senior Management Training
  1. Usage of all the proposed systems for monitoring, tracking and reporting,
  2. MIS reports, accessing various exception reports

## **3. Post-Implementation Training**

1. Refresher Trainings for the Senior Management
2. Functional/Operational training and IT basics for new operators
3. Refresher courses on System Administration
4. Change Management programs

### **3. Project Implementation Timelines, Deliverables and Payment Terms**

Purchaser intends to implement the project in phased manner approach, distributed in three phases as mentioned below:

#### **Phase I – T + 6 months (*T is the date of signing of the contract with SI*)**

- a) City WiFi - Supply, installation, commissioning, training & operationalization of City WiFi at 50% of total (136) identified locations
- b) City Kiosk - Supply, installation, commissioning, training & operationalization of City Kiosk at 50% of total (100) identified locations
- c) City Surveillance - Supply, installation, commissioning, training & operationalization of City Surveillance at 50% of total (700) identified locations
- d) "Smart Strip" - Supply, installation, commissioning, training & operationalization of Smart Strip
- e) City Network Backbone – Deployment, installation, commissioning, training and operationalization of zonal layer for city network backbone
- f) Design, supply, installation, commissioning including interior civil work & operationalization of Command Control Center and City Operation Center.

#### **Phase II – T + 10 months (*T is the date of signing of the contract with SI*)**

- a) City WiFi - Supply, installation, commissioning, training & operationalization of City WiFi at remaining 50% of total (136) identified locations
- b) City Kiosk - Supply, installation, commissioning, training & operationalization of City Kiosk at remaining 50% of total (100) identified locations
- c) City Surveillance - Supply, installation, commissioning, training & operationalization of City Surveillance at additional 50% of total (700) identified locations

#### **Phase III – T + 12 months (*T is the date of signing of the contract with SI*)**

- a) City Network Backbone –
  - Deployment, installation, commissioning, training and operationalization of ward layer for city network backbone
  - Go-live of City Network Backbone covering all locations of City WiFi, City Surveillance, City Kiosk and "Smart Strip" solutions

### 3.1 Project Deliverables, Milestones and Timelines

#	Milestone	Deliverables	Timelines (in months)
	<b>Phase 1</b>		<b>T +6 months</b>
	Project Initiation	<ul style="list-style-type: none"> <li>Detailed Survey Report including infrastructure assessment, phase wise location distribution, hardware deployment plans etc.</li> <li>Detailed Project Plan including Operations management, Contract management, Risk management, Information Security and Business Continuity</li> </ul>	
	<b>Smart Strip</b>		<b>T + 6 months</b>
	Supply, installation, commissioning, training & operationalization of Smart Strip	<ul style="list-style-type: none"> <li>Delivery Report, inspection reports (component - wise)</li> <li>Site Completion/readiness Report</li> <li>Software Licenses</li> <li>Training Completion Certificate</li> <li>Acceptance /Go Live Certificate from purchaser/authorized entity</li> </ul>	T + 6 months
	<b>City WiFi</b>		<b>T + 6 months</b>
	City WiFi - Supply, installation, commissioning, training & operationalization of City WiFi at 50% of total (136) identified locations	<ul style="list-style-type: none"> <li>Delivery Report, inspection reports (component - wise)</li> <li>Site Completion/ readiness Report</li> <li>Acceptance Certificate from purchaser/authorized entity</li> </ul>	T + 6 months
	<b>City Surveillance</b>		<b>T + 6 months</b>
	City Surveillance - Supply, installation, commissioning, training & operationalization of City Surveillance at 50% of total (700) identified locations	<ul style="list-style-type: none"> <li>Delivery Report, inspection reports (component - wise)</li> <li>Site Completion/ readiness Report</li> <li>Software Licenses</li> <li>Acceptance Certificate from purchaser/authorized entity</li> </ul>	T + 6 months
	<b>City Kiosk</b>		<b>T + 6 months</b>
	City Kiosk - Supply, installation, commissioning, training & operationalization of City Kiosk at 50% of total (100) identified locations	<ul style="list-style-type: none"> <li>Delivery Report, inspection reports (component - wise)</li> <li>Site Completion/ readiness Report</li> <li>Licenses</li> <li>Acceptance Certificate from purchaser/authorized entity</li> </ul>	T + 6 months
	<b>City Network Backbone</b>		<b>T + 6 months</b>
	City Network Backbone – Deployment, installation,	<ul style="list-style-type: none"> <li>Delivery Report, inspection reports (component - wise)</li> </ul>	T + 6 months

#	Milestone	Deliverables	Timelines (in months)
	commissioning, training and operationalization of zonal layer for city network backbone	<ul style="list-style-type: none"> <li>• Site Completion/readiness Report</li> <li>• Software Licenses</li> <li>• Acceptance Certificate from purchaser/authorized entity</li> </ul>	
<b>Command Control Center &amp; City Operation Center</b>			<b>T + 6 months</b>
	Design, supply, installation, commissioning including interior civil work & operationalization of Command Control Center and City Operation Center including Server Rooms, Network Operation Center and Helpdesks	<ul style="list-style-type: none"> <li>• Delivery Report, inspection reports (component - wise)</li> <li>• Site Completion/ readiness Report</li> <li>• Licenses</li> <li>• Acceptance Certificate from purchaser/authorized entity</li> </ul>	T + 6 months
<b>Phase 2</b>			<b>T + 10 months</b>
<b>City WiFi</b>			<b>T + 10 months</b>
	City WiFi - Supply, installation, commissioning, training, operationalization & Go Live of City WiFi at remaining 50% of total (136) identified locations	<ul style="list-style-type: none"> <li>• Delivery Report, inspection reports (component - wise)</li> <li>• Site Completion/ readiness Report</li> <li>• Licenses</li> <li>• Training Completion Certificate</li> <li>• Acceptance /Go Live Certificate from purchaser/authorized entity</li> </ul>	T + 10 months
<b>City Surveillance</b>			<b>T + 10 months</b>
	City Surveillance - Supply, installation, commissioning, training, operationalization & Go Live of City Surveillance at additional 50% of total (700) identified locations	<ul style="list-style-type: none"> <li>• Delivery Report, inspection reports (component - wise)</li> <li>• Site Completion/ readiness Report</li> <li>• Software Licenses</li> <li>• Acceptance /Go Live Certificate from purchaser/authorized entity</li> </ul>	T + 10 months
<b>City Kiosk</b>			<b>T + 10 months</b>
	City Kiosk - Supply, installation, commissioning, training, operationalization & Go Live of City Kiosk at remaining 50% of total (100) identified locations	<ul style="list-style-type: none"> <li>• Delivery Report, inspection reports (component - wise)</li> <li>• Site Completion/ readiness Report</li> <li>• Licenses</li> <li>• Training Completion Certificate</li> <li>• Acceptance /Go Live Certificate from purchaser/authorized entity</li> </ul>	T + 10 months
<b>Phase 3</b>			<b>T<sub>1</sub> = T + 12 months</b>
<b>City Network Backbone</b>			<b>T + 12 months</b>
	City Network Backbone –	<ul style="list-style-type: none"> <li>• Delivery Report, inspection reports (component - wise)</li> </ul>	T + 12 months

#	Milestone	Deliverables	Timelines (in months)
	<ul style="list-style-type: none"> <li>Deployment, installation, commissioning, training and operationalization of ward layer for city network backbone</li> <li>Go-live of City Network Backbone covering all locations of City WiFi, City Surveillance, City Kiosk and "Smart Strip" solutions</li> </ul>	<ul style="list-style-type: none"> <li>Site Completion/ readiness Report</li> <li>Licenses</li> <li>Training Completion Certificate</li> <li>Acceptance /Go Live Certificate from purchaser/authorized entity</li> </ul>	
<b><i>Operations and Maintenance phase</i></b>			<b>T<sub>1</sub> + 60 Months</b>
	Operation & Maintenance	SLA Compliance Report	Every quarter

**Note:**

- ***T is the date of signing of contract***
- ***T<sub>1</sub> is the date of Go Live of the last solution***
- ***SI shall provision for appropriate bandwidth as a service for City WiFi, City Surveillance, City kiosk and "Smart Strip" solutions till the time network backbone is operational.***

### 3.2 Payment Terms and Schedule

1. The request for payment shall be made to the purchaser in writing, accompanied by invoices (in triplicate) describing, as appropriate, the services performed, and by the required documents submitted pursuant to general conditions of the contract and upon fulfilment of all the obligations stipulated in the Contract.
2. Due payments shall be made promptly by the purchaser, generally within sixty (60) days after submission of an invoice or request for payment by SI
3. The currency or currencies in which payments shall be made to the SI under this Contract shall be Indian Rupees (INR) only.
4. All remittance charges shall be borne by the SI.
5. In case of disputed items, the disputed amount shall be withheld and shall be paid only after settlement of the dispute.
6. Any penalties/ liquidated damages, as applicable, for delay and non-performance, as mentioned in this RFP document, shall be deducted from the due payments of the respective milestones.
7. Taxes, as applicable, shall be deducted / paid, as per the prevalent rules and regulations

#### Payment Schedule

Payments to SI, after successful completion of the target milestones (including specified project deliverables), shall be made as under: -

S. No.	Scope of Work	Timelines	Payment
1.	Phase I Operationalization & Go Live	T + 6 Months	20% of contract value
2.	Phase II Operationalization & Go Live	T + 10 Months	10% of contract value
3.	Phase III Operationalization & Go Live	T <sub>1</sub> = T + 12 Months	10% of contract value
4.	Operations & Maintenance phase for a period of 60 months from the date of Go Live of the last solution	T <sub>1</sub> + 60 Months	60% of Contract Value in equal quarterly instalments i.e.

#### Note:

T is the date of signing of contract

T<sub>1</sub> is the date of Go Live of the last solution

## 4. Requirement Specifications (Technical / Functional)

### 1.1 City Network Backbone – (Network Infrastructure)

24 Core Optical Fibre Cable				
Sr. No.	Item	Minimum Requirement Description	Compliance (Yes / No)	Deviations / Remarks
FIBER.REQ.001	Cable Type	Optical Fiber Single Mode 24 Core		
FIBER.REQ.002	Core	24		
FIBER.REQ.003	Mode	Single Mode		
FIBER.REQ.004	Cladding diameter	125.0 $\mu\text{m} \pm 1.0$		
FIBER.REQ.005	Coated fibre diameter	245 $\mu\text{m} \pm 10$		
FIBER.REQ.006	Core/cladding concentricity error	$\leq 0.8\mu\text{m}$		
FIBER.REQ.007	Coating/cladding concentricity error	$\leq 12\mu\text{m}$		
FIBER.REQ.008	Cladding non-circularity	$\leq 1.0 \%$		
FIBER.REQ.009	Mode Field Diameter	9.3 $\mu\text{m} \pm 0.5$ at 1310nm		
FIBER.REQ.010	Attenuation (cable)	0.36dB/Km at 1310nm, 0.25dB/Km at 1550nm,		
FIBER.REQ.011	Zero-Dispersion Wavelength	1300 to 1322 nm		
FIBER.REQ.012	Zero-Dispersion Slope	$\leq 0.092$ ps/Sq. Nm .km		
FIBER.REQ.013	Zero-Dispersion Slope	$\leq 0.092$ ps/Sq. Nm .km		
FIBER.REQ.014	Cut-off Wavelength	$\leq 1260$ nm		
FIBER.REQ.015	Polarization Mode Dispersion Coefficient	$\leq 0.2$ at 1310nm		
FIBER.REQ.016	Fibre macro bend loss	$\leq 0.05\text{dB}$ at 1550 nm with 75 mm dia, 100 turns		
FIBER.REQ.017	Fibre macro bend loss	$\leq 0.5\text{dB}$ at 1550 nm with 32 mm dia, 1 turn		

<b>Core Router</b>				
<b>Sr. No.</b>	<b>Item</b>	<b>Minimum Requirement Description</b>	<b>Compliance (Yes / No)</b>	<b>Deviations / Remarks</b>
COR.REQ.001	Functional Requirements	The router shall facilitate all applications like voice, video and data to run over a converged IP infrastructure along with hardware assisted IPSEC & Network Address Translation (NAT) capability.		
COR.REQ.002	Functional Requirements	The Router shall have 1:1 router processor/control processor redundancy, PSU redundancy, service card redundancy. The Router should have minimum 8 linecard slots for future expansion.		
COR.REQ.003	Functional Requirements	The router line card must support following interface: Fast Ethernet, Gigabit Ethernet, Channelized STM1, STM1, STM16, STM64, 10G Ethernet, 40G Ethernet, POS, ATM, V.35 Serial Ports, E1, Chn E1, E3 Ports.		
COR.REQ.004	Functional Requirements	Backplane Architecture: The back plane architecture of the router must be modular and redundant. The back plane bandwidth must be 200 Gbps from day one (1) with minimum routing performance of 100 mpps from day one (1).		
COR.REQ.005	Hardware Architecture	The Router should have individual dedicated control plane processor and data plane processor module. Data plane Processor module should be independent of the control plane Processor. Control plane Processor should have support for internal memory to support multiple software images for backup purposes and future scalability. The router processor architecture must be multi-processor based and should support hardware accelerated, parallelized and programmable IP forwarding and switching.		
COR.REQ.006	Hardware Architecture	The router should support the IPv4 and IPv6 DUAL-stack in hardware and software. The router should support minimum 1 MN IPv4 & 1 MN ipv6 active FIB (Forwarding Information Base) routes from day oneso that these routes can be utilized for traffic forwarding		
COR.REQ.007	Protocol Support	The router shall have RIPv1, RIPv2, RIPv6, BGP, OSPFv2 & v3, Policy Based Routing for both IPv4 & IPv6, IP Multicast Routing Protocols including PIM SM, PIM SSM, GRE (Generic Routing Encapsulation) Tunneling with 1000 tunnels enabled from day one		



<b>Core Router</b>				
<b>Sr. No.</b>	<b>Item</b>	<b>Minimum Requirement Description</b>	<b>Compliance (Yes / No)</b>	<b>Deviations / Remarks</b>
COR.REQ.008	Protocol Support	Router should support following MPLS features – LDP, Layer 2 VPN such as EoMPLS with LDP signaling, Route Reflector (RR), Traffic Engineering with RSVP-TE, Fast Reroute Link Node & Path protection enabled from day one.		
COR.REQ.009	Protocol Support	The router shall have IPv6 Multicast protocols – Ipv6 MLD, PIM-Sparse Mode, and PIM – SSM, P6 Security Functions – ACL, SSH over IPv6, MPLS Support for IPv6 - IPv6 VPN over MPLS, Inter-AS options, IPv6 VPN over MPLS, IPv6 transport over MPLS, dual stack IPv6 on all interfaces and IPv6 over IPv4 tunneling with support for minimum 900 L3VPN from day one.		
COR.REQ.010	QoS	The router shall provide up to 200k queues for deployment of per-user per-application per-port QoS, 8 queues per port, support cRTP for VoIP traffic, QoS policy in the router shall support dual Strict Priority Queue or Low Latency Queue per policy so that voice and video traffic can be put in different queue. It also should have hierarchical QoS (Inbound and Outbound) to ensure bandwidth allocation for all type of traffic during congestion and non congestion scenario.		
COR.REQ.011	QoS	The router shall perform traffic Classification using various parameters like source physical interfaces, source/destination IP subnet, protocol types (IP/TCP/UDP), source/destination ports, IP Precedence, 802.1p, MPLS EXP, DSCP		
COR.REQ.012	Security	The router shall meet the following requirements for security: 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.		
COR.REQ.013	Security	The router should have hardware assisted NAT capability with NAT performance of 10Gbps from Day 1		
COR.REQ.014	Security	Router should have at least 15 Gbps of IPSEC throughput from day one. VPN box and router should be from the same OEM in case if bidder is positioning external VPN box. In case of external VPN box,		

<b>Core Router</b>				
<b>Sr. No.</b>	<b>Item</b>	<b>Minimum Requirement Description</b>	<b>Compliance (Yes / No)</b>	<b>Deviations / Remarks</b>
		bidder should propose the hardware with necessary 10G interface and redundant power supply. The proposed router should have embedded support for 4000 IPsec tunnels from day one.		
COR.REQ.015	Management	The router must support management through SNMPv1, v2 and v, support RADIUS and TACACS. The router must role based access to the system for configuration and monitoring. The router shall be provided with IETF standards based feature so that granular traffic analysis can be performed for advanced auditing, usage analysis, capacity planning or generating security telemetry events, also the router shall have SLA monitoring tools to measure state of the network in real time. The SLA operations shall provide information on TCP/UDP delay, jitter,, Packet Loss etc.		
COR.REQ.016	Physical Interface Support	Each Router should be provided with 2 x 40GE ports, 6 x10GE ports from Day 1. Bidder need to size the port & transceivers requirement as per their solution and if required need to include additional ports for the workability of solution		
COR.REQ.017	Certification	The Router should be minimum EAL2 or NDPP certified		
COR.REQ.018	Support	The system should not be end of life/end of service product		

<b>Core Switch</b>				
<b>Sr. No.</b>	<b>Item</b>	<b>Minimum Requirement Description</b>	<b>Compliance (Yes / No)</b>	<b>Deviations / Remarks</b>
CSW.REQ.001	Hardware features	Chassis based Multilayer Switch with sufficient modules/line cards to fit required transceivers/UTP ports. Chassis shall have minimum 8 payload slots. The switch must have front to back airflow.		
CSW.REQ.002	Hardware features	The total aggregate switching capacity shall be 3 Tbps or more		
CSW.REQ.003	Hardware features	There should not be any single point of failure in the switch. All the main components like CPU module, switching fabric, support module, system clock, power supplies and fans etc should be in redundant configuration. Components, like modules/power supplies/fan tray should be Hot Swappable		
CSW.REQ.004	Hardware features	The switch should have redundant CPU's working in an active-active or active-standby mode. There should not be any traffic disruption during the CPU fail-over/change-over and the fail-over time should be less than 1 sec.		
CSW.REQ.005	Hardware features	The proposed switch should have enough Memory (Flash and RAM) to hold the latest Software Release. It should support all features of switch and parameters like MAC Address Table, IP Routing Tables, VLANs etc. at their peak values as claimed in the Data Sheets of the Switch.		
CSW.REQ.006	Hardware features	The Switch should support non-blocking Layer 2 switching and Layer 3 routing.		
CSW.REQ.007	Hardware features	The Backplane should be 100% Passive. Preferably back plane free design to optimize the airflow and power consumption.		

<b>Core Switch</b>				
<b>Sr. No.</b>	<b>Item</b>	<b>Minimum Requirement Description</b>	<b>Compliance (Yes / No)</b>	<b>Deviations / Remarks</b>
CSW.REQ.008	Hardware features	The Switch should have a truly Distributed Architecture. All Interface Modules should have all the resources for switching and Routing and should offer True Local Switching (Intra-Module and Inter-Module).		
CSW.REQ.009	Interface Support	The switch must support 1/10G SFP+, 1/10 G Base-T and 40G QSFP based port line cards. The switch must scalability to support minimum 40 nos of 40G QSFP ports or more.		
CSW.REQ.010	Interface Support	The switch must support 100 Gig line cards from day1.		
CSW.REQ.011	Management features	Switch should be SNMP manageable with support for SNMP Version 1, 2 and 3.		
CSW.REQ.012	Management features	Switch should support TELNET and SSH Version-2 for Command Line Management.		
CSW.REQ.013	Management features	Switch should support 4 groups of embedded RMON (history, statistics, alarm and events).		
CSW.REQ.014	Management features	Support for Unidirectional Link Detection Protocol (UDLD) or equivalent to detect unidirectional links caused by incorrect fiber-optic wiring or port faults and disable on fiber-optic interfaces		
CSW.REQ.015	Management features	Layer 2 trace route or equivalent to ease troubleshooting by identifying the physical path that a packet takes from source to destination.		
CSW.REQ.016	Scalability	Should support Industry Standard Port/Link Aggregation for All Ports. Also Cross Module Link aggregation should be supported		
CSW.REQ.017	Scalability	Jumbo Frames support up to 9K Bytes on Gigabit / 10 G Ports		

<b>Core Switch</b>				
<b>Sr. No.</b>	<b>Item</b>	<b>Minimum Requirement Description</b>	<b>Compliance (Yes / No)</b>	<b>Deviations / Remarks</b>
CSW.REQ.018	Scalability	Support for broadcast, multicast and unknown unicast storm control to prevent degradation of switch performance from faulty end stations		
CSW.REQ.019	Scalability	Should support port, subnet based 802.1Q VLANs. The switch should support 4096 vlans. The switch must support Private VLAN or equivalent.		
CSW.REQ.020	Scalability	The switch should support minimum 50K no. of MAC addresses		
CSW.REQ.021	Scalability	The switch should support IEEE 802.1w RSTP and IEEE 802.1s MSTP.		
CSW.REQ.022	Scalability	Switch must support spine - leaf topology based on VXLAN and create large layer 2 domain.		
CSW.REQ.023	Scalability	Switch must support multi chassis ethernet channel or equivalent feature and work with any downstream switch, server from various vendors.		
CSW.REQ.024	Protocol Support	Should support routing protocol IP v4 - Static routing, OSPF v2, BGPv4, IS-IS and IP v6 - BGP, OSPF v3. The switch must support Bidirectional Forwarding detection. The total aggregate switching capacity shall be 3 Tbps or more		
CSW.REQ.025	Protocol Support	Switch must support IP v4 - HSRP/ VRRP and VRRP IPv6. It must also support DHCP Relay V4 and V6.		
CSW.REQ.026	Protocol Support	Switch should support VRF - Lite and VRF Route leaking functionality. The switch should support minimum 960 VRF instances.		
CSW.REQ.027	Scalability	Should support minimum 32K Route entries for IPv4 and IPv6 routes.		

<b>Core Switch</b>				
<b>Sr. No.</b>	<b>Item</b>	<b>Minimum Requirement Description</b>	<b>Compliance (Yes / No)</b>	<b>Deviations / Remarks</b>
CSW.REQ.028	Redundancy	Must Have Redundancy for Power Supply, FANs and clocks to minimise unavailability of switch. Online insertion and removal (OIR) support is must for modules, Power supply and FAN.		
CSW.REQ.029	Redundancy	Stateful Switchover to ensure that in case of failure of active CPU module the redundant CPU should start switching L2/L3 traffic in less than 1 sec (in case switch has redundant CPU).		
CSW.REQ.030	Redundancy	Should Support Hitless software upgrades (ISSU) to reduce downtime during software upgrade. The switch must support Fault isolation per process and process patching to enhance the switch availability		
CSW.REQ.031	QoS features	Should support Ingress/Egress Queuing.		
CSW.REQ.032	QoS features	Should support QoS scheduling with queues supported in hardware		
CSW.REQ.033	QoS features	Should support upto 4 queues per port		
CSW.REQ.034	QoS features	Should support ACL based traffic classification		
CSW.REQ.035	MultiCast feature	Should support H/W based IPv4 and IPv6 Multicasting		
CSW.REQ.036	MultiCast feature	Should Support IGMP v1, v2 , v3, IGMP Snooping		
CSW.REQ.037	MultiCast feature	Should support Protocol Independent Multicast - Sparse Mode and PIM - ASM for IPv4 and MSDP for IP v6. It should also support Anycast Routing Protocol (Anycast RP).		
CSW.REQ.038	MultiCast feature	Switch should support 8K Multicast route		

<b>Core Switch</b>				
<b>Sr. No.</b>	<b>Item</b>	<b>Minimum Requirement Description</b>	<b>Compliance (Yes / No)</b>	<b>Deviations / Remarks</b>
CSW.REQ.039	MultiCast feature	Switch should support 8K IGMP Group		
CSW.REQ.040	Management features	Switch should be manageable through NMS on per port/switch basis with common interface for all manageable devices on the network. Should Support SNMP, RMON/RMON-II, SSH, telnet, web management through network management software.		
CSW.REQ.041	Management features	Should support port mirroring feature for monitoring network traffic of a particular port/VLAN/group of ports/entire switch.		
CSW.REQ.042	Management features	Switch should support Syslog, XML (NetConf), SSHv2, Telnet, OOB Management port, Console Port.		
CSW.REQ.043	Management features	Should support Linux tools, Bash /Power Sheel/ Phython Shell/ XMPP Client		
CSW.REQ.044	Management features	The switch should support configuration verification and roll-back.		
CSW.REQ.045	Management features	The switch should support SNMP v1,v2c and V3		
CSW.REQ.046	Virtualisation	Switch must support IEEE 802.1BR (Bridge Port Extension) or bridge domain and virtual switching or equivalent technology to optimise cabling inside the data centre		
CSW.REQ.047	Virtualisation	Switch must support virtualization features like VXLAN Gateway/Bridging and routing functionality. It should be capable of supporting NVGRE.		

<b>Core Switch</b>				
<b>Sr. No.</b>	<b>Item</b>	<b>Minimum Requirement Description</b>	<b>Compliance (Yes / No)</b>	<b>Deviations / Remarks</b>
CSW.REQ.048	IEEE Standard support	IEEE 802.1D Bridging and Spanning Tree		
CSW.REQ.049	IEEE Standard support	IEEE 802.1p QoS/CoS		
CSW.REQ.050	IEEE Standard support	IEEE 802.1Q VLAN Tagging		
CSW.REQ.051	IEEE Standard support	IEEE 802.1w Rapid Spanning Tree		
CSW.REQ.052	IEEE Standard support	IEEE 802.1s Multiple Spanning Tree Protocol		
CSW.REQ.053	IEEE Standard support	IEEE 802.1AB Link Layer Discovery Protocol		
CSW.REQ.054	IEEE Standard support	IEEE 802.3ad Link Aggregation with LACP		
CSW.REQ.055	IEEE Standard support	IEEE 802.3x Flow Control		
CSW.REQ.056	IEEE Standard support	IEEE 802.3ab 1000BASE-T		
CSW.REQ.057	IEEE Standard support	IEEE 802.3z Gigabit Ethernet		
CSW.REQ.058	IEEE Standard support	IEEE 802.3ae 10 Gigabit Ethernet		



<b>Core Switch</b>				
<b>Sr. No.</b>	<b>Item</b>	<b>Minimum Requirement Description</b>	<b>Compliance (Yes / No)</b>	<b>Deviations / Remarks</b>
CSW.REQ.059	IEEE Standard support	IEEE 802.3ba 40 Gigabit Ethernet		
CSW.REQ.060	General Standard support	RFC 2460 IPv6		
CSW.REQ.061	General Standard support	RFC 2461 Neighbor Discovery for IPv6		
CSW.REQ.062	General Standard support	RFC 2462 IPv6 Stateless Address Autoconfiguration		
CSW.REQ.063	General Standard support	RFC 2463 ICMPv6		
CSW.REQ.064	Interface Requirement from Day 1	16-port 40GE QSFP+ ports with multimode cable transceivers 48-port 10 Gigabit Ethernet SFP+ ports with minimum 16 10G SR transceivers. The interface should be divided in 2 slots for redundancy. SI to include more transceivers if required as per the solution proposed.		
CSW.REQ.065	Product Support	The system should not be end of life/end of service product		

<b>Internet Router</b>				
<b>Sr. No.</b>	<b>Item</b>	<b>Minimum Requirement Description</b>	<b>Compliance (Yes / No)</b>	<b>Deviations / Remarks</b>
IR.REQ.001	Hardware features	Router should be chassis based and modular architecture with multicore processor for scalability		
IR.REQ.002	Hardware features	Router should have minimum of 6 nos. of SFP based ports and 2x10G SFP+ based ports		
IR.REQ.003	Hardware features	Router should have at least 1 open slot for additional LAN/ WAN modules other than asked ports.		
IR.REQ.004	Hardware features	Router should support STM-1, STM-4, Gigabit Ethernet and 10 Gigabit Ethernet modules in asked slot.		
IR.REQ.005	Hardware features	Router should have DES, 3DES and AES Standards through dedicated encryption module/processor. Should support IPsec with IKEv2		
IR.REQ.006	Hardware features	Router shall have hot swappable 1:1 redundant internal power supply		
IR.REQ.007	Hardware features	Router should have a minimum throughput of 20 Gbps. The Router should have minimum forwarding rate of 6 Mpps with concurrent services like ACL, QoS, and URPF		
IR.REQ.008	Hardware features	Router should have a minimum IPsec throughput of 5 Gbps		
IR.REQ.009	Routing Protocols	Router should support static Routes, OSPFv2, OSPFv3, BGP4, MBGP, BFD, Policy based routing, IPv4 and IPv6 tunnelling		
IR.REQ.010	Multicast Features	Router should support IGMP v1/v2/v3 and PIM multicast routing		
IR.REQ.011	Protocol Features	Should support other IP Services like GRE tunnel, IPv4 tunnel, IPv6 tunnel, Virtual Router Redundancy Protocol (VRRP), Network Address Translation (NAT), Access Control Lists (ACLs)		

<b>Internet Router</b>				
<b>Sr. No.</b>	<b>Item</b>	<b>Minimum Requirement Description</b>	<b>Compliance (Yes / No)</b>	<b>Deviations / Remarks</b>
IR.REQ.012	Qos Features	Shall have 802.1p class of service, IP differentiated service code point (DSCP) and IP precedence		
IR.REQ.013	Qos Features	Routers should support marking, classification, policing and shaping		
IR.REQ.014	Network Management Features	Router should support SSHv2, SNMPv2c, SNMPv3 and NTP		
IR.REQ.015	Network Management Features	Routers should support AAA using RADIUS and TACACS+		
IR.REQ.016	Network Management Features	Routers should support configuration rollback		
IR.REQ.017	Network Management Features	Router should support software upgrades		
IR.REQ.018	Network Management Features	Support for accounting of traffic flows for network planning and security purposes.		
IR.REQ.019	Management feature	Should support extensive support for IP SLA and best path selection for metrics like delay, latency, jitter, packet loss to assure business-critical IP applications.		
IR.REQ.020	Management feature	Router should support monitoring of network traffic with application level insight with deep packet visibility into web traffic, RTP-Based VoIP traffic and cRTP		
IR.REQ.021	Management feature	Router shall have traffic load balancing capability on dual WAN Links based on based on advanced criteria, such as reachability, delay, loss, jitter and bandwidth utilization.		
IR.REQ.022	Certification	Router shall conform to UL 60950 or IEC 60950 or CSA 60950 or EN 60950 Standards for Safety requirements of Information Technology Equipment.		
IR.REQ.023	Certification	Router shall conform to EN 55022 Class A/B or CISPR22 Class A/B or CE Class A/B or FCC Class A/B Standards for EMC (Electro Magnetic Compatibility) requirements.		

<b>Internet Router</b>				
<b>Sr. No.</b>	<b>Item</b>	<b>Minimum Requirement Description</b>	<b>Compliance (Yes / No)</b>	<b>Deviations / Remarks</b>
IR.REQ.024	Certification	Router / Router's Operating System should be tested and certified for EAL 2 or above or NDPP certified		

<b>Intranet Firewall</b>				
<b>Sr. No.</b>	<b>Item</b>	<b>Minimum Requirement Description</b>	<b>Compliance (Yes / No)</b>	<b>Deviations / Remarks</b>
INTRA.FW.REQ.001	General Requirements	The appliance based security platform with multicore CPU should be capable of providing firewall, URL Filtering, Application Visibility and Control (AVC) and VPN (IPSec and SSL) functionality		
INTRA.FW.REQ.002	General Requirements	The appliance should have min 6 no. of 10/100/1000 Base-T Gigabit Ethernet ports plus 4 x 10G SFP+ port and should be expandable to support additional 6 x 10/100/1000 GE + 4 x 10G no. of SFP+ ports with 10G SR Transceivers.		
INTRA.FW.REQ.003	General Requirements	The appliance hardware should be a multicore CPU architecture with a hardened 64 bit operating system to support higher memory		
INTRA.FW.REQ.004	General Requirements	Proposed Firewall should not be proprietary based in nature & should be open architecture based on multi-core cpu's to protect & scale against dynamic latest security threats.		
INTRA.FW.REQ.005	General Requirements	Firewall shall have hot swappable 1:1 redundant internal power supply		
INTRA.FW.REQ.006	General Requirements	Firewall should support stateful failover of sessions in Active/Standby and Active/Active mode		
INTRA.FW.REQ.007	General Requirements	Should support maximum Firewall througput of 40Gbps and Multi- protocol throughput of 20 gbps. Real world profile should include but not limited to HTTP, Bit Torrent, FTP , SMTP and IMAPv4		

<b>Intranet Firewall</b>				
<b>Sr. No.</b>	<b>Item</b>	<b>Minimum Requirement Description</b>	<b>Compliance (Yes / No)</b>	<b>Deviations / Remarks</b>
INTRA.FW.REQ.008	General Requirements	Firewall Should should support DES, 3DES/ AES IPSec VPN throughput of minimum 5 Gbps. Should support minimum5,000 cumulative VPN including IPSec / SSL		
INTRA.FW.REQ.009	General Requirements	Firewall should support minimum 10,000,000 concurrent sessions		
INTRA.FW.REQ.010	General Requirements	Firewall should support minimum 2,50,000 new connections per second		
INTRA.FW.REQ.011	General Requirements	Firewall should support atleast 1000 VLANs		
INTRA.FW.REQ.012	General Requirements	Firewall should support 2 virtual firewalls from day one and scalable to minimum 200 virtual firewalls as and when required with licenses.		
INTRA.FW.REQ.013	General Requirements	Firewall should support static Routes, RIPv1/RIPv2, OSPFv2, OSPFv3, BGP4		
INTRA.FW.REQ.014	General Requirements	Firewall should support PIM Multicast routing		
INTRA.FW.REQ.015	General Requirements	Firewall should support for Layer 3 and Layer 4 stateful firewall features, including access control, network address translation, and stateful inspection.		
INTRA.FW.REQ.016	General Requirements	Firewall should support creating access-rules with IPv4 & IPv6 objects simultaneously		
INTRA.FW.REQ.017	General Requirements	Firewall should support operating in routed and transparent mode		
INTRA.FW.REQ.018	General Requirements	In transparent mode firewall should support arp-inspection to prevent spoofing at Layer 2		
INTRA.FW.REQ.019	General Requirements	Firewall should provide application inspection for DNS, FTP, HTTP, SMTP, ESMTP, LDAP, MGCP, RTSP, SIP, SCCP, SQLNET, TFTP, H.323, SNMP etc.		

<b>Intranet Firewall</b>				
<b>Sr. No.</b>	<b>Item</b>	<b>Minimum Requirement Description</b>	<b>Compliance (Yes / No)</b>	<b>Deviations / Remarks</b>
INTRA.FW.REQ.020	General Requirements	Firewall should be able to create access policies based on the User/group info from the Active Directory either through clientless or agent based mechanism .		
INTRA.FW.REQ.021	General Requirements	Firewall should support static nat, pat, dynamic nat, pat & destination based nat		
INTRA.FW.REQ.022	General Requirements	Firewall should support integration with RADIUS, TACACS, RSA, LDAPv3 Directory Servers, Kerberos, NT server and Local Database		
INTRA.FW.REQ.023	General Requirements	Firewall should support IKEv2 and Suite B cryptography		
INTRA.FW.REQ.024	General Requirements	Firewall should support perfect forward secrecy & dead peer detection functionality		
INTRA.FW.REQ.025	General Requirements	Firewall should support NAT-T for IPSec VPN		
INTRA.FW.REQ.026	General Requirements	Centralized management console can be a separate appliance based solution or software installed on a server. Firewall & Centralized manager should be from same OEM.		
INTRA.FW.REQ.027	General Requirements	Firewall should support SSHv2, SNMPv2c, SNMPv3 and NTP		
INTRA.FW.REQ.028	General Requirements	Firewall should support AAA using RADIUS and TACACS+		
INTRA.FW.REQ.029	VPN Features	Firewall should support software upgrades		
INTRA.FW.REQ.030	VPN Features	The device should support IPSEC/IKEv2 for remote VPN access		
INTRA.FW.REQ.031	VPN Features	Firewall Should support IPSecv3 and enhanced IPSecv3		
INTRA.FW.REQ.032	VPN Features	The security appliance supports the following encryption standards for ESP: DES, 3DES, AES-128, AES-192, AES-256		

<b>Intranet Firewall</b>				
<b>Sr. No.</b>	<b>Item</b>	<b>Minimum Requirement Description</b>	<b>Compliance (Yes / No)</b>	<b>Deviations / Remarks</b>
INTRA.FW.REQ.033	VPN Features	The security appliance supports the following hashing algorithms: MD5, SHA		
INTRA.FW.REQ.034	VPN Features	Supports the use of SHA-2 compliant signature algorithms to authenticate SSL VPN connections that use digital certificates. Support for SHA-2 includes all three hash sizes: SHA-256, SHA-384, and SHA-512		
INTRA.FW.REQ.035	VPN Features			
INTRA.FW.REQ.036	Support	It should support IPSec VPN solution that is compliant with the following RFC: RFC 2408 - Internet Security Association and Key Management Protocol (ISAKMP) RFC 2409 - The Internet Key Exchange (IKE) RFC 2412		
INTRA.FW.REQ.037	Security	Should support Perfect forward secrecy using Diffie-Hellman (DH) groups 1,2,5 and 7		
INTRA.FW.REQ.038	Certification	The Intranet Firewall solution offered must be from the leaders or Challengers quadrant for Firewall published by Gartner as on the day of publication of this RFP		
INTRA.FW.REQ.039	Certification	The appliance should have certifications like EAL3/ NDPP or higher		

<b>Internet Firewall</b>				
<b>Sr. No.</b>	<b>Item</b>	<b>Minimum Requirement Description</b>	<b>Compliance (Yes / No)</b>	<b>Deviations Remarks /</b>
INTER.FW.REQ.001	General Hardware and Interface requirements	The appliance based security platform with multicore CPU should be capable of providing firewall, URL Filtering, VPN (IPSec / SSL) functionality		
INTER.FW.REQ.002	General Hardware and Interface requirements	The appliance should have min 6 no. of 10/100/1000 Base-T Gigabit Ethernet ports plus 4 x 10G SFP+ port and should be expandable to support additional 6 x 10/100/1000 GE + 4 x 10G no. of SFP+ ports with 10G SR Transceivers.		
INTER.FW.REQ.003	General Hardware and Interface requirements	The appliance hardware should be a multicore CPU architecture with a hardened 64 bit operating system to support higher memory		
INTER.FW.REQ.004	General Hardware and Interface requirements	Proposed Firewall should not be proprietary based in nature & should be open architecture based on multi-core cpu's to protect & scale against dynamic latest security threats.		
INTER.FW.REQ.005	General Hardware and Interface requirements	Firewall shall have hot swappable 1:1 redundant internal power supply		
INTER.FW.REQ.006	General Hardware and Interface requirements	Firewall should support stateful failover of sessions in Active/Standby and Active/Active mode		
INTER.FW.REQ.007	Performance Requirements	Should have maximum Firewall throughput of 20 Gbps and Multi-protocol throughput of 10 gbps. Real world profile should include but not limited to HTTP, Bit Torrent, FTP, SMTP and IMAPv4		
INTER.FW.REQ.008	Performance Requirements	Firewall Should should support DES, 3DES/ AES IPSec VPN throughput of minimum 3 Gbps. Should support minimum 10,000 cumulative VPN including IPSec and SSL (500 SSL licenses to be included from day 1)		
INTER.FW.REQ.009	Performance Requirements	Firewall should support minimum of 3,500,000 concurrent sessions		



<b>Internet Firewall</b>				
<b>Sr. No.</b>	<b>Item</b>	<b>Minimum Requirement Description</b>	<b>Compliance (Yes / No)</b>	<b>Deviations Remarks /</b>
INTER.FW.REQ.010	Performance Requirements	Firewall should support minimum 1,75,000 new connections per second		
INTER.FW.REQ.011	Performance Requirements	Firewall should support atleast 1000 VLANs		
INTER.FW.REQ.012	Performance Requirements	Firewall should support 2 virtual firewalls from day one and scalable to minimum of 200 virtual firewalls as and when required with licenses.		
INTER.FW.REQ.013	Routing Protocols	Firewall should support static Routes, RIPv1/RIPv2, OSPFv2, OSPFv3, BGP4		
INTER.FW.REQ.014	Routing Protocols	Firewall should support PIM Multicast routing		
INTER.FW.REQ.015	Firewall Features	Firewall should support for Layer 3 and Layer 4 stateful firewall features, including access control, network address translation, and stateful inspection.		
INTER.FW.REQ.016	Firewall Features	Firewall should support creating access-rules with IPv4 & IPv6 objects simultaneously		
INTER.FW.REQ.017	Firewall Features	Firewall should support operating in routed and transparent mode		
INTER.FW.REQ.018	Firewall Features	In transparent mode firewall should support arp-inspection to prevent spoofing at Layer 2		
INTER.FW.REQ.019	Firewall Features	Firewall should provide application inspection for DNS, FTP, HTTP, SMTP, ESMTP, LDAP, MGCP, RTSP, SIP, SCCP, SQLNET, TFTP, H.323, SNMP etc.		
INTER.FW.REQ.020	Firewall Features	Firewall should be able to create access policies based on the User/group		
INTER.FW.REQ.021	Firewall Features	Firewall should support static nat, pat, dynamic nat, pat & destination based nat		
INTER.FW.REQ.022	Firewall Features	Firewall should support integration with RADIUS, TACACS, RSA, LDAPv3 Directory Servers, Kerberos, NT server and Local Database		

<b>Internet Firewall</b>				
<b>Sr. No.</b>	<b>Item</b>	<b>Minimum Requirement Description</b>	<b>Compliance (Yes / No)</b>	<b>Deviations / Remarks</b>
INTER.FW.REQ.023	Firewall Features	Firewall should support IKEv2 Suite B cryptography		
INTER.FW.REQ.024	Firewall Features	Firewall should support perfect forward secrecy & dead peer detection functionality		
INTER.FW.REQ.025	Firewall Features	Firewall should support NAT-T for IPSec VPN		
INTER.FW.REQ.026	System Management and Administration	Centralized management console can be a separate appliance based solution or software installed on a server. Firewall & Centralized manager should be from same OEM.		
INTER.FW.REQ.027	System Management and Administration	Firewall should support SSHv2, SNMPv2c, SNMPv3 and NTP		
INTER.FW.REQ.028	System Management and Administration	Firewall should support AAA using RADIUS and TACACS+		
INTER.FW.REQ.029	System Management and Administration	Firewall should support software upgrades		
INTER.FW.REQ.030	VPN Features	The device should support IPSEC/IKEv2 for remote VPN access		
INTER.FW.REQ.031	VPN Features	Firewall Should support IPSec		
INTER.FW.REQ.032	VPN Features	The security appliance supports the following encryption standards for ESP: DES, 3DES, AES-128, AES-192, AES-256		
INTER.FW.REQ.033	VPN Features	The security appliance supports the following hashing algorithms: MD5, SHA		
INTER.FW.REQ.034	VPN Features	Supports the use of SHA-2 compliant signature algorithms to authenticate SSL VPN connections that use digital certificates. Support for SHA-2 includes all three hash sizes: SHA-256, SHA-384, and SHA-512		
INTER.FW.REQ.035	VPN Features	Firewall should support Suite B cryptography including ECDSA, ECDH & SHA- 2		
INTER.FW.REQ.036	VPN Features	It should support IPSec VPN solution that is compliant with the following RFC: RFC 2408 - Internet Security Association and Key		

<b>Internet Firewall</b>				
<b>Sr. No.</b>	<b>Item</b>	<b>Minimum Requirement Description</b>	<b>Compliance (Yes / No)</b>	<b>Deviations Remarks /</b>
		Management Protocol (ISAKMP) RFC 2409 - The Internet Key Exchange (IKE) RFC 2412		
INTER.FW.REQ.037	VPN Features	Should support Perfect forward secrecy using Diffie-Hellman (DH) groups 1,2,5 and 7		
INTER.FW.REQ.038	Evaluation Compliance	The Internet Firewall solution offered must be from the leaders or Challengers quadrant for Firewall published by Gartner as on the day of publication of this RFP		
INTER.FW.REQ.039	Evaluation Compliance	The appliance should have certifications like EAL/ NDPP or higher		

Intrusion Prevention System (IPS) / Intrusion Detection System (IDS)					
Sr. No.	Item		Minimum Requirement Description	Compliance (Yes / No)	Deviations Remarks /
INT.IPS.REQ.001	Hardware features		The proposed solution must be based on standard computer technology (not ASICs) so that future enhancements and protocols do not require hardware refresh to support		
INT.IPS.REQ.002	Advanced Protection	Threat	The proposed solution platform must be based on a hardened operating system.		
INT.IPS.REQ.003	Advanced Protection	Threat	The detection engine must be capable of operating in both passive (i.e., monitoring) and inline (i.e., blocking) modes.		
INT.IPS.REQ.004	Advanced Protection	Threat	Detection rules must be based on an extensible, open language that enables users to create their own rules, as well as to customize any vendor-provided rules.		
INT.IPS.REQ.005	Advanced Protection	Threat	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.).		
INT.IPS.REQ.006	Advanced Protection	Threat	The detection engine must incorporate multiple approaches for detecting threats, including at a minimum exploit-based signatures, vulnerability-based rules, protocol anomaly detection, and behavioral anomaly detection techniques. Identify and explain each type of detection mechanism supported.		
INT.IPS.REQ.007	Advanced Protection	Threat	The detection engine must inspect not only Network Layer details and information resident in packet headers, but a broad range of protocols across all layers of the computing stack and packet payloads as well.		

Intrusion Prevention System (IPS) / Intrusion Detection System (IDS)					
Sr. No.	Item		Minimum Requirement Description	Compliance (Yes / No)	Deviations Remarks /
INT.IPS.REQ.008	Advanced Protection	Threat	Sensors must be capable of performing packet-level forensics and capturing raw packet data in response to individual events without significant performance degradation.		
INT.IPS.REQ.009	Advanced Protection	Threat	The solution must be capable of detecting and blocking IPv6 attacks.		
INT.IPS.REQ.010	Advanced Protection	Threat	The solution must be capable of providing network-based detection of malware by checking the disposition of known files in the cloud/on premises using the SHA-256 file-hash as they transit the network (SHA-256 and target IP address should be given to aid remediation efforts).		
INT.IPS.REQ.011	Intelligent Automation	Security	The solution must provide full contextual awareness (user, application & content) with respect to malware detection, propagation and retrospective remediation		
INT.IPS.REQ.012	Intelligent Automation	Security	The solution must be able to track APTs that involve multiple threat elements and associate malware child processes to their parents		
INT.IPS.REQ.013	Intelligent Automation	Security	The solution must run in a stylized sandbox environment that can be used to identify the unknown malwares.		
INT.IPS.REQ.014	Intelligent Automation	Security	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.		

<b>Intrusion Prevention System (IPS) / Intrusion Detection System (IDS)</b>				
<b>Sr. No.</b>	<b>Item</b>	<b>Minimum Requirement Description</b>	<b>Compliance (Yes / No)</b>	<b>Deviations Remarks /</b>
INT.IPS.REQ.015	Control Compliance	The solution must be capable of employing an extensive set of contextual information (e.g., pertaining to the composition, configuration, and behavior of the network and its hosts) to improve the efficiency and accuracy of both manual and automatic analysis of detected events.		
INT.IPS.REQ.016	Control Compliance	The solution must be capable of dynamically tuning IDS/IPS sensors (e.g., selecting rules, configuring policies, updating policies, etc.) with minimal human intervention.		
INT.IPS.REQ.017	Control Compliance	The solution must be capable of automatically providing the appropriate inspections and protections for traffic sent over non-standard communications ports.		
INT.IPS.REQ.018	Control Compliance	The solution must support creation of user-defined application protocol detectors.		
INT.IPS.REQ.019	Control Compliance	The solution must have content awareness with comprehensive file detection policies and blocking of files by types, protocols and directions.		
INT.IPS.REQ.020	Control Compliance	- Protocols: HTTP, SMTP, IMAP, POP		
INT.IPS.REQ.021	Control Compliance	- Direction: Upload, Download, Both		
INT.IPS.REQ.022	Control Compliance	- File Types: Office Documents, Archive, Multimedia, Executable, PDF, Encoded, Graphics, and System Files.		
INT.IPS.REQ.023	Control Compliance	The management platform must be capable of centralized, life cycle management for all sensors.		
INT.IPS.REQ.024	Control Compliance	The management platform must be delivered in virtual appliance form factor (management system and UI must		

Intrusion Prevention System (IPS) / Intrusion Detection System (IDS)				
Sr. No.	Item	Minimum Requirement Description	Compliance (Yes / No)	Deviations Remarks /
		provide the same features and functions as in the physical appliance).		
INT.IPS.REQ.02 5	Management Usability and	The management platform must be accessible via a web-based interface and ideally with no need for additional client software.		
INT.IPS.REQ.02 6	Management Usability and	The management platform must be capable of integrating third party vulnerability information into threat policy adjustment routines and automated tuning workflows.		
INT.IPS.REQ.02 7	Management Usability and	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.		
INT.IPS.REQ.02 8	Management Usability and	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.		
INT.IPS.REQ.02 9	Management Usability and	Sensors must support built-in capability of failing open, such that communications traffic is still allowed to pass if the inline sensor goes down.		
INT.IPS.REQ.03 0	Management Usability and	The management platform must include an integration mechanism, preferably in the form of open APIs and/or standard interfaces, to enable automatic response to threats by external components and remediation applications, such as routers, firewalls, patch management systems, etc.		
INT.IPS.REQ.03 1	Reporting and Alerting (Evaluation Compliance)	The IPS solution offered must be must be from the leaders or Challengers quadrant for Network Intrusion Prevention System published by Gartner.		
INT.IPS.REQ.03 2	Reporting and Alerting (Performance)	Should have minimum IPS throughput of 15 Gbps		

<b>Intrusion Prevention System (IPS) / Intrusion Detection System (IDS)</b>				
<b>Sr. No.</b>	<b>Item</b>	<b>Minimum Requirement Description</b>	<b>Compliance (Yes / No)</b>	<b>Deviations Remarks /</b>
INT.IPS.REQ.03 3	Reporting and Alerting (Performance)	Should support minimum 10,000,000 Concurrent Connections and atleast 2,50,000 new connections per second		
INT.IPS.REQ.03 4	Reporting and Alerting (Interface)	Should have minimum 8 monitoring interface of 4x 1 Gbps Copper + 4 x 10G SR		
INT.IPS.REQ.03 5	Reliability and Availability (Performance)	Latency should be < 150 microseconds.		
INT.IPS.REQ.03 6	Reliability and Availability (Interface)	Must have dedicated 10/100/1000 RJ45 Management Interface.		
INT.IPS.REQ.03 7	Reliability and Availability (Security )	IPS is required to have the built-in capability to inspect SSL traffic		



<b>Aggregation Router</b>				
<b>Sr. No.</b>	<b>Item</b>	<b>Minimum Requirement Description</b>	<b>Compliance (Yes / No)</b>	<b>Deviations / Remarks</b>
AGG.ROU.001	Architecture	Router should be chassis based & modular architecture for scalability with Redundant Route Processor, Power supply, Switching fabric		
AGG.ROU.002	Architecture	Router should be provided with 1+1 route processor, and 1+1 or 1+N power supply redundancy		
AGG.ROU.003	Architecture	Should have two free full width payload slots for future expansion.		
AGG.ROU.004	Architecture	The router shall support following type of interfaces – 100GE, 10GE, 1GE interfaces.; POS - OC-3c/STM-1c, STM4, STM16, STM64, channelized STM-1,channelized STM-4, Channelized E1, E3, Circuit emulation E1, Circuit emulation E3, 10GE G.709 OTN, 10GE WAN PHY		
AGG.ROU.005	Architecture	The router 10 Gig interfaces for SR,LR & ZR are software configurable for LANPHY/WANPHY/OTU mode.		
AGG.ROU.006	Architecture	The operating system of the router shall have a microkernel-based architecture.		
AGG.ROU.007	Architecture	The modular operating system shall run all critical functions like various routing protocol, forwarding plane and management functions in separate memory protected modules. Failure of one module shall not impact operations of rest of the OS.In service bug patching should be available		
AGG.ROU.008	Architecture	The router should support line cards with timing protocol support such as 1588v2 (with boundary clock as well as ordinary clock (master and slave) and sync E		
AGG.ROU.009	Architecture	Router should support two free slots for future expansion		
AGG.ROU.010	Architecture	The 'slot' for any router means a main slot or full slot on the router chassis. Only such a slot shall be counted towards determining the number of free slots. Any sub slot or daughter slot shall not be considered as a slot.		
AGG.ROU.011	Architecture	The router shall have minimum of 200Gig Full Duplex capacity per slot with redundancy. Failure of any switch fabric should not degrade the per slot bandwidth.		

<b>Aggregation Router</b>				
<b>Sr. No.</b>	<b>Item</b>	<b>Minimum Requirement Description</b>	<b>Compliance (Yes / No)</b>	<b>Deviations / Remarks</b>
AGG.ROU.012	Architecture	Router Shall support non blocking capacity minimum of of 3.2 Tbps.		
AGG.ROU.013	Architecture	The router should have capability of minimum 2 million IPv4 routes considering the traffic and scalability requirements		
AGG.ROU.014	Architecture	The router should have capability of minimum 2 Million IPv6 routes		
AGG.ROU.015	Architecture	The router should support minimum 2 million MAC address, minimum 128k Pseudo wires.		
AGG.ROU.016	Performance	The proposed router should have minimum 10 GB DRAM and 8GB Flash and 28 GB storage in SSD		
AGG.ROU.017	Performance	Router should have 128k multicast routes.		
AGG.ROU.018	Performance	The router should support 32 way BGP load balancing and 32 way ECMP		
AGG.ROU.019	Performance	Shall support online insertion and removal (OIR) that is non-disruptive in nature. Online insertion and removal of one line card shall not lead to ANY packet loss for traffic flowing through other line cards for both unicast and multicast traffic.		
AGG.ROU.020	Performance	In case of a line card or Route Processor failure on the router; the multicast and Unicast routing, multicast and Unicast distribution and multicast replication architecture of the router shall ensure no impact & zero packet loss of multicast video, audio & data traffic running on rest of the line cards in the system		
AGG.ROU.021	Performance	if the any of the feature and functionality asked in the RFP is achieved using any service module that should be quoted in 1+1 redundancy.		
AGG.ROU.022	Performance			
AGG.ROU.023	Performance	Should have IPv4 Routing, IPv6 Routing, Border Gateway Protocol , Intermediate System-to-Intermediate System [IS-IS], and Open Shortest Path First [OSPF]), DHCPv6 and OSPFv3 for IPv6		

<b>Aggregation Router</b>				
<b>Sr. No.</b>	<b>Item</b>	<b>Minimum Requirement Description</b>	<b>Compliance (Yes / No)</b>	<b>Deviations / Remarks</b>
AGG.ROU.024	Performance	Shall support Multicast routing protocols IGMPv1, v2 ,v3, PIM-SM (RFC2362) and PIM-SSM,MSDP,IGMP v2 snooping,MPLS mVPN (Multicast VPN)		
AGG.ROU.025	High Bandwidth	Shall Support 6PE & 6VPE, MPLS VPN, , MPLS TE (Fast re-route), DiffServ-Aware TE, BGP Prefix Independent Convergence,Inter-AS VPN, Resource Reservation Protocol (RSVP),RFC 3107 of Carrying Label Information in BGP-4.		
AGG.ROU.026	High Bandwidth	Should support Route Policy Language (RPL), Hot Standby Router Protocol (HSRP)/Virtual Router Redundancy Protocol (VRRP), GRE (Generic Routing Encapsulation) Tunneling,		
AGG.ROU.027	High Bandwidth	Shall Support VPLS ,HVPLS, Ethernet over MPLS , CESoPSN and SAToP as per RFC 4553,		
AGG.ROU.028	High Bandwidth	Router shall support MPLS OAM, Ethernet OAM protocols - CFM (IEEE 802.1ag), Link OAM (IEEE 802.3ah) and ITU Y.1731.		
AGG.ROU.029	High Bandwidth	The routers shall support both L2 and L3 services on all interfaces		
AGG.ROU.030	High Bandwidth	Configuration Roll Back to recover the mis-configured router to last good configuration		
AGG.ROU.031	Protocol Support	Shall support the following:		
AGG.ROU.032	Protocol Support	Traffic Classification using various parameters like source physical interfaces, source/destination IP subnet, protocol types (IP/TCP/UDP), source/destination ports, IP Precedence, 802.1p, MPLS EXP, DSCP and by some well known application types through Application Recognition techniques.		
AGG.ROU.033	Protocol Support	Shall support Strict Priority Queuing or Low Latency Queuing to support real time application like Voice and Video with minimum delay and jitte, Congestion Management: WRED, Priority queuing, Class based weighted fair queuing		

<b>Aggregation Router</b>				
<b>Sr. No.</b>	<b>Item</b>	<b>Minimum Requirement Description</b>	<b>Compliance (Yes / No)</b>	<b>Deviations / Remarks</b>
AGG.ROU.034	Protocol Support	Shall support standards based RSVP for voice & video call admission control.		
AGG.ROU.035	Protocol Support	Ability to configure hierarchical queues in hardware for IP QoS at the egress to the edge. Minimum 128k egress and 64k ingress hardware queues per line card.		
AGG.ROU.036	Protocol Support	Platform must support nested hierarchical QOS policies .Router should have 4 level of scheduling for HQOS.		
AGG.ROU.037	Protocol Support	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., Time based ACL,AAA using radius or TACACS		
AGG.ROU.038	Protocol Support	The routers shall provide hardware accelerated IETF Netflow-v9/J-Flow/equivalent feature. This feature shall be available for all interfaces provisioned on the router with hardware acceleration.		
AGG.ROU.039	Protocol Support	Should Support MD-5 authentication for RIP, OSPF,IS-IS and BGP.		
AGG.ROU.040	Protocol Support	Also support URPF,DHCP snooping , control plane policing ,SNMPv3 authentication, SSHv2		
AGG.ROU.041	Protocol Support	Should have to support Out of band management through Console / external modem for remote management.		
AGG.ROU.042	Qos	Event and System logging: Event and system history logging functions shall be available. The Router shall generate system alarms on events. Facility to put selective logging of events onto a separate hardware here the analysis of log shall be available.		
AGG.ROU.043	Qos	16 x 10G SFP+ Ports Distributed across minimum two or more line cards and min of 20 x 1G SFP ports Distributed across minimum two or more line cards		
AGG.ROU.044	Qos	SI need to size the port & transceivers requirement as per their solution and if required need to include additional ports for the workability of solution		

<b>Aggregation Router</b>				
<b>Sr. No.</b>	<b>Item</b>	<b>Minimum Requirement Description</b>	<b>Compliance (Yes / No)</b>	<b>Deviations / Remarks</b>
AGG.ROU.045	Qos	The Router should be minimum EAL2 / NDPP/Applicable Protection Profile certified under the Common Criteria Evaluation Program		
AGG.ROU.046	Qos	The system should not be end of life/end of service product		

<b>Datacenter Network Switch</b>				
<b>Sr. No.</b>	<b>Item</b>	<b>Minimum Requirement Description</b>	<b>Compliance (Yes / No)</b>	<b>Deviations / Remarks</b>
DCNS.REQ.001	Hardware features	Proposed network device must be 19" rack mountable & Maximum 2 RU in size.		
DCNS.REQ.002	Hardware features	It is desirable that the network infrastructure is based on delivering front to back airflow.		
DCNS.REQ.003	Hardware features	Network Infrastructure equipment must use 240V AC power.		
DCNS.REQ.004	Hardware features	Must have Redundancy Power Supply Units (PSUs), Hot-swappable, field-replaceable power supplies, 1:1 power redundancy and Must have N:1 fan module redundancy.		
DCNS.REQ.005	Hardware features	All components (including elements such as I/O cards, Expansion Module, power supplies and fans) must be hot swappable with zero disruption to traffic forwarding (Unicast or multicast).		
DCNS.REQ.006	Hardware features	Must have minimum 48 x 1/10 G SFP+ and 6 X 40 G QSFP ports with multimode cable transceivers		
DCNS.REQ.007	Hardware features	Transceivers to be supplied as per the solution of the SI		
DCNS.REQ.008	Hardware features	Must be field upgradeable / license upgradeable to Layer 3 for investment protection.		
DCNS.REQ.009	Hardware features	Must have Line-rate traffic throughput on all ports at Layer 2.		

<b>Datacenter Network Switch</b>				
<b>Sr. No.</b>	<b>Item</b>	<b>Minimum Requirement Description</b>	<b>Compliance (Yes / No)</b>	<b>Deviations / Remarks</b>
DCNS.REQ.010	Hardware features	Must have Line-rate traffic throughput on all ports at Layer 3		
DCNS.REQ.011	Hardware features	Must have switching bandwidth of 1.4 Tbps		
DCNS.REQ.012	Scalability	Must support Bridge Extension Protocol (IEEE 802.1BR) or equivalent - to scale Gigabit & 10 Gigabit Ethernet ports		
DCNS.REQ.013	Scalability	Must allow to build very large L2 domain using Multi-Path Ethernet technologies.		
DCNS.REQ.014	Scalability	Must support port channeling across multi chassis.		
DCNS.REQ.015	Switch Features	Physical standards for Network Device:		
DCNS.REQ.016	Switch Features	Must support Fast Ethernet (IEEE 802.3u, 100BASE-TX)		
DCNS.REQ.017	Switch Features	Must support Gigabit Ethernet (IEEE 802.3z, 802.3ab)		
DCNS.REQ.018	Switch Features	Must support Ten Gigabit Ethernet (IEEE 802.3ae)		
DCNS.REQ.019	Switch Features	Software based standards for Network Device:		
DCNS.REQ.020	Switch Features	Must support IEEE 802.1d - Spanning-Tree Protocol		
DCNS.REQ.021	Switch Features	Must support IEEE 802.1w - Rapid Spanning Tree		
DCNS.REQ.022	Switch Features	Must support IEEE 802.1s - Multiple Spanning Tree Protocol		
DCNS.REQ.023	Switch Features	Must support IEEE 802.1q - VLAN encapsulation		
DCNS.REQ.024	Switch Features	Must support IEEE 802.3ad - Link Aggregation Control Protocol (LACP)		
DCNS.REQ.025	Switch Features	Must support IEEE 802.1ab - Link Layer Discovery Protocol (LLDP)		
DCNS.REQ.026	Switch Features	Must support IEEE 802.3x Flow Control		
DCNS.REQ.027	Switch Features	Routing protocol support when upgraded with Layer3 License:		
DCNS.REQ.028	Switch Features	Must support Static IP routing		
DCNS.REQ.029	Switch Features	Must support Open Shortest Path First (OSPF) v2 (RFC 2328)		
DCNS.REQ.030	Switch Features	Must support Protocol Independent Multicast Version 2 (PIMv2) sparse mode, Source Specific Multicast (SSM), Multicast Source Discovery Protocol (MSDP), and Internet Group Management Protocol Versions 2, and 3 (IGMP v2, and v3)		
DCNS.REQ.031	Switch Features	Must support Border Gateway Protocol - BGPv4 (RFC 1771)		

<b>Datacenter Network Switch</b>				
<b>Sr. No.</b>	<b>Item</b>	<b>Minimum Requirement Description</b>	<b>Compliance (Yes / No)</b>	<b>Deviations / Remarks</b>
DCNS.REQ.032	Switch Features	Must have Routed ports on platform interfaces, switch virtual interface (SVI), PortChannels, subinterfaces, and PortChannel subinterfaces for a total of 2048 entries		
DCNS.REQ.033	Switch Features	Should have minimum 8K multicast routes		
DCNS.REQ.034	Switch Features	Virtual Route Forwarding (VRF): VRF-lite (IP VPN); VRF-aware unicast; and BGP-, OSPF-, RIP-, and VRF-aware multicast		
DCNS.REQ.035	Switch Features	Must support 16-way equal-cost multipathing (ECMP)		
DCNS.REQ.036	Switch Features	Must support In-Service Software Upgrade (ISSU) for Layer 2 or equivalent		
DCNS.REQ.037	Switch Features	Must have Layer 2 IEEE 802.1p		
DCNS.REQ.038	Switch Features	Must have 4 hardware queues per port with per port QoS configuration		
DCNS.REQ.039	Switch Features	Must have Modular QoS classification compliance		
DCNS.REQ.040	Switch Features	Must support Jumbo Frame Size (9k)		
DCNS.REQ.041	Switch Features	IEEE 802.3ad Link Aggregation or equivalent capabilities		
DCNS.REQ.042	Switch Features	Switch must support VXLAN (Bridging and Routing) as well as NVGRE overlay encapsulation protocol in hardware to support multiple hypervisor deployment in the Data Center		
DCNS.REQ.043	Switch Features	Must be able to load balance across a logical bundle using the following algorithms:		
DCNS.REQ.044	Switch Features	Source IP		
DCNS.REQ.045	Switch Features	Destination IP		
DCNS.REQ.046	Switch Features	Source and Destination IP		
DCNS.REQ.047	Switch Features	Source MAC		
DCNS.REQ.048	Switch Features	Destination MAC		
DCNS.REQ.049	Switch Features	Source and Destination MAC		
DCNS.REQ.050	Switch Features	TCP Port (destination and/or source)		
DCNS.REQ.051	Switch Features	UDP Port (destination and/or source)		

<b>Datacenter Network Switch</b>				
<b>Sr. No.</b>	<b>Item</b>	<b>Minimum Requirement Description</b>	<b>Compliance (Yes / No)</b>	<b>Deviations / Remarks</b>
DCNS.REQ.052	Security Features	Must support multiple privilege levels for remote access (e.g. console or telnet access)		
DCNS.REQ.053	Security Features	Must support Remote Authentication Dial-In User Service (RADIUS) and/or Terminal Access Controller Access Control System Plus (TACACS+)		
DCNS.REQ.054	Security Features	Must support AAA using RADIUS (RFC 2138 & 2139) and/or TACACS+, enabling centralized control of the device and the ability to restrict unauthorized users from altering the configuration		
DCNS.REQ.055	Security Features	Must have following Access Control features		
DCNS.REQ.056	Security Features	Must support Ingress ACLs (Standard & Extended or equivalent) on Ethernet and virtual Ethernet ports		
DCNS.REQ.057	Security Features	Must support Standard and extended or equivalent Layer 2 ACLs: MAC addresses, protocol type, etc.		
DCNS.REQ.058	Security Features	Must support Standard and extended or equivalent Layer 3 to 4 ACLs: IPv4 and v6, Internet Control Message Protocol (ICMP), TCP, User Datagram Protocol (UDP), etc		
DCNS.REQ.059	Security Features	Must support VLAN based ACLs (VACLs) and Port-Based ACLs (PACLs)		
DCNS.REQ.060	Security Features	Must support ACL logging and statistics		
DCNS.REQ.061	Quality of Service	Must support IEEE 802.1p class-of-service (CoS) prioritization		
DCNS.REQ.062	Quality of Service	Must have Per-Port QoS configuration		
DCNS.REQ.063	Quality of Service	Must have CoS Trust		
DCNS.REQ.064	Quality of Service	Must have CoS-based egress queuing		
DCNS.REQ.065	Quality of Service	Must have Egress strict-priority queuing or equivalent		
DCNS.REQ.066	Quality of Service	Must have Modular QoS classification compliance or equivalent		
DCNS.REQ.067	Quality of Service	Must support Egress port-based scheduling: Weighted Round-Robin (WRR) or equivalent		
DCNS.REQ.068	Quality of Service	Must have ACL-based QoS classification (Layers 2, 3, and 4)		
DCNS.REQ.069	Management	Must provide management using 10/100/1000-Mbps management or console ports		
DCNS.REQ.070	Management	Must have CLI-based console to provide detailed out-of-band management		
DCNS.REQ.071	Management	Must have In-band switch management		



<b>Datacenter Network Switch</b>				
<b>Sr. No.</b>	<b>Item</b>	<b>Minimum Requirement Description</b>	<b>Compliance (Yes / No)</b>	<b>Deviations / Remarks</b>
DCNS.REQ.072	Management	Must have Configuration synchronization & Configuration rollback		
DCNS.REQ.073	Management	Must support Secure Shell Version 2 (SSHv2), Telnet & SNMPv1, v2, and v3		
DCNS.REQ.074	Management	Must support AAA, AAA with RBAC, Radius, TACACS+ for user authentication		
DCNS.REQ.075	Management	Must support RMON		
DCNS.REQ.076	Management	Must support XML (NETCONF)		
DCNS.REQ.077	Management	Must have Advanced Encryption Standard (AES) for management traffic		
DCNS.REQ.078	Management	Must support Unified username and passwords across CLI and SNMP		
DCNS.REQ.079	Management	Must support Microsoft Challenge Handshake Authentication Protocol (MS-CHAP)		
DCNS.REQ.080	Management	Must have Digital certificates for management between switch and RADIUS server		
DCNS.REQ.081	Management	Must have Switched Port Analyzer (SPAN) on physical, PortChannel, VLAN, and Fiber Channel interfaces		
DCNS.REQ.082	Troubleshooting Capabilities	Must provide Comprehensive bootup diagnostic tests		
DCNS.REQ.083	Troubleshooting Capabilities	Must have Ingress and egress packet counters per interface		
DCNS.REQ.084	Support	The system should not be end of life/end of service product and should be EAL2/NDPP certified		

<b>Access Router</b>				
<b>Sr. No.</b>	<b>Item</b>	<b>Minimum Requirement Description</b>	<b>Compliance (Yes / No)</b>	<b>Deviations / Remarks</b>
ACR.REQ.001	Hardware Requirements	Router shall support redundant Data and control Plane. There should not have impact to Data Plane traffic during software upgrade. Smallest RU factor would be preferred.		
ACR.REQ.002	Hardware Requirements	Router should have redundant controller cards and should support stateful switch over non stop forwarding, Non stop routing and Graceful restart.		
ACR.REQ.003	Hardware Requirements	Router should be CE2.0 and MEF14.0 certified.		
ACR.REQ.004	Hardware Requirements	Router shall support MEF for Ethernet based services like PW, VPLS or ATOM.		
ACR.REQ.005	Hardware Architecture	Router shall support sync any configurations from previous modules to new modules with hot-swap event occurred		
ACR.REQ.006	Hardware Architecture	The router shall support following type of interfaces – 10GE, 1GE interfaces with DWDM.; 10GE WAN PHY and 10G DWDM , Ch.STM1 and E1.		
ACR.REQ.007	Hardware Architecture	Router shall have minimum 2 free slots for future expansion.		
ACR.REQ.008	Router Performance	Router shall support non-blocking capacity of 128Gbps.		
ACR.REQ.009	Router Performance	Backplane of each slot should be minimum 20 Gbps.		
ACR.REQ.010	Router Performance	Router shall support 170 Mpps forwarding performance		
ACR.REQ.011	Hardware Architecture	Router shall support 16000 Mac addresses		
ACR.REQ.012	Router Performance	Router shall support 18000 IPv4 routes		
ACR.REQ.013	Router Performance	Router shall support 8000 queues and 128 MPLS VPN's		
ACR.REQ.014	Router Performance	Router shall support aggregation of links. Minimum 8 link should be supported as part of single aggregation.		

<b>Access Router</b>				
<b>Sr. No.</b>	<b>Item</b>	<b>Minimum Requirement Description</b>	<b>Compliance (Yes / No)</b>	<b>Deviations / Remarks</b>
ACR.REQ.015	Router Performance	Router shall support IPSLA or equivalent and Y.1731 for performance monitoring.		
ACR.REQ.016	Redundancy	Router should support Redundant Power Supply and should also support On line insetion and removal of same.		
ACR.REQ.017	Redundancy	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 Support hot-swappable for all modules. And secure normal operations when hot-swap event occurred		
ACR.REQ.018	Redundancy	All cards should be provided in redundancy.		
ACR.REQ.019	Redundancy	Router shall support MPLS-TE with FRR for sub 50 msec protection.		
ACR.REQ.020	Redundancy	Router must support Traffic Engineering for node and link protection.		
ACR.REQ.021	Protocol support	Router shall support IPV4, IPV6,ECMP,LDP,BGP,IS-IS,OSPFv2and V3		
ACR.REQ.022	Protocol support	Router shall support IGMP V2/V3,MLD,IGMP and PIM,,VRRP,Multicast layer3 VPN		
ACR.REQ.023	Protocol support	Router shall support 6PE and 6VPE mode for IPV6 transport over IPV4, ,BGP PIC(EDGE and Core) for IPV4 and IPV6,,Loop free alternate FRR (IPFRR). Traffic Engineering and RSVP.		
ACR.REQ.024	Protocol support	The Router should support Point to Point and Point to Multipoint LSP for Unicast and Multicast traffic.		
ACR.REQ.025	Protocol support	Router should support high availability for all BFD,BGP ,OSPF and IS-IS and no packet loss during controller switch over.		
ACR.REQ.026	Protocol support	Router shall support layer3 and layer2 MPLS VPN.		
ACR.REQ.027	Protocol support	Router shall support MPLSOAM, EthernetOAMprotocols-CFM(IEEE 802.1ag), Link OAM (IEEE 802.3ah) and ITU Y.1731		
ACR.REQ.028	Protocol support	The router along with respective line cards should be supplied with timing protocol support such as 1588v2 (with boundary clock as well as ordinary clock (master and slave) and syncE		
ACR.REQ.029	Protocol support	Router should support RFC 3107 of Carrying Label Information in BGP-4		
ACR.REQ.030	Quality of Service	Router shall support HQOS on all kind of interface in both ingress and egress direction. Similar QOS shall be supported for all type of		

<b>Access Router</b>				
<b>Sr. No.</b>	<b>Item</b>	<b>Minimum Requirement Description</b>	<b>Compliance (Yes / No)</b>	<b>Deviations / Remarks</b>
		interface including Bundled interfaces. The proposed router shall support 3 level H-QoS		
ACR.REQ.031	Quality of Service	Shall support Ingress classification, marking and 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		
ACR.REQ.032	Quality of Service	Shall support Strict Priority Queuing or Low Latency Queuing to support real time application like Voice and Video with minimum delay and jitter.		
ACR.REQ.033	Quality of Service	Congestion Management: WRED, Priority queuing, Class based weighted fair queuing		
ACR.REQ.034	Quality of Service	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		
ACR.REQ.035	Operating Temperature	For DC : 0°C to 65°C operating temperature and 5 to 95%, noncondensing		
ACR.REQ.036	Interface Requirements	4 x 10G SFP+ Ports Distributed across minimum two or more line cards and 24 x 1G SFP ports Distributed across minimum two or more line cards		
ACR.REQ.037	Interface Requirements	Bidder need to size the port & transceivers requirement as per their solution and if required need to include additional ports for the workability of solution		
ACR.REQ.038	Certification	The Router should be minimum EAL2 /NDPP/ Applicable Protection Profile certified under the Common Criteria Evaluation Program		
ACR.REQ.039	Product Support	The system should not be end of life/end of service product		

Network Switch Ruggedized				
Sr. No.	Item	Minimum Requirement Description	Compliance (Yes / No)	Deviations / Remarks
RNS.REQ.001	Switch Architecture and Performance	The switch should provide minimum 12 port 10/100/1000 Mbps ports for downlink out of which minimum eight should be POE/POE+ and switch should additionally have 2 GE SFP uplinks scalable to 4 within the same unit. Should be proposed with ruggedized transceivers as per SI solution.		
RNS.REQ.002	Switch Architecture and Performance	Switch should have wire rate switching fabric of minimum 20 Gbps or more.		
RNS.REQ.003	Switch Architecture and Performance	802. 1Q VLAN on all ports with support for minimum 500 active VLANs and minimum 1K Mac addresses		
RNS.REQ.004	Layer 2 Features	Spanning Tree Protocol as per IEEE 802.1d, 802.1s and 802.1w		
RNS.REQ.005	Switch Architecture and Performance	Should support Improved resiliency with support for ring protection protocol for ring topology		
RNS.REQ.006	Layer 2 Features	Link Aggregation Control Protocol (LACP) as per IEEE 802.3ad.		
RNS.REQ.007	Switch Architecture and Performance	Switch should support IGMP v1/v2/v3 as well as IGMP snooping and minimum 500 IGMP Multicast Groups		
RNS.REQ.008	Quality of Service (QoS) Features	Switch should support classification and scheduling as per IEEE 802.1P on all ports and four egress queues per port. Switch should also support Egress Queueing/shaping, Mechanism of applying Automatic QoS or equivalent mechanism		
RNS.REQ.009	Quality of Service (QoS) Features	Switch should support strict priority queuing or equivalent to guarantee that the highest-priority packets are serviced ahead of all other traffic.		

<b>Network Switch Ruggedized</b>				
<b>Sr. No.</b>	<b>Item</b>	<b>Minimum Requirement Description</b>	<b>Compliance (Yes / No)</b>	<b>Deviations / Remarks</b>
RNS.REQ.010	Security Features	Switch should support ACLs, TACACS+, RADIUS, "IP Route Filtering, ARP spoofing, DHCP snooping, DHCP Option 82, Dynamic ARP Inspection (DAI)		
RNS.REQ.011	Standards	IEEE 802.1ae, IEEE 802.3af and IEEE 802.3 at power over Ethernet (POE) standards on all ports.		
RNS.REQ.011	Management Features	Switch should have a console port, support for SNMP Version 1, 2 and 3, TELNET, SSHv2, 4 groups of embedded RMON, , DHCP server		
RNS.REQ.012	IPv6 Feature	The switch should support following IPv6 Features: 128-Bit Wide Unicast Addresses, DNS for IPv6, ICMPv6, Neighbor Discovery, SNMP and Syslog Over IPv6, HTTP over IPv6 and IPv6 MLD snooping		
RNS.REQ.013	Certification	RoHS Compliant Minimum QM333 or NEMA TS2		
RNS.REQ.014	Certification	ODVA Industrial EtherNet/IP, PROFINETv2, ABB IT Certificate minimum IP30		
RNS.REQ.015	Certification	CSA C22.2, UL/CSA 60950-1, EN60950-1, CB to IEC 60950-1,		
RNS.REQ.016	Switch Architecture and Performance	DIN rail mount		
RNS.REQ.017	Certification	FCC, IEC/EN 55022, RoHS		
RNS.REQ.018	Operating Temperature	0°C to +65°C with Enclosure, Enclosure to be provided as required		
RNS.REQ.019	Certification	IEC 60068-2-27 (Operational Shock, Non-Operational Shock)		
RNS.REQ.020	Certification	IEC 60068-2-6, IEC 60068-2-64, EN61373 (Operational Vibration, Non-operational Vibration)		
RNS.REQ.021	Operating Humidity	Relative Humidity of 10% or 85% Non-condensing, IEC 60068 -2-3, IEC 60068-2-30, IEC 60068-52-2		
RNS.REQ.022	Product Support	The system should not be end of life/end of service product		

<b>Network Access Switch</b>				
<b>Sr. No.</b>	<b>Item</b>	<b>Minimum Requirement Description</b>	<b>Compliance (Yes / No)</b>	<b>Deviations / Remarks</b>
AS.REQ.001	Switch Architecture and Performance	Min 24 * 10/100/1000T ports with 4 x GE SFP ports switches supporting various optical modules of SMF and MMF modules		
AS.REQ.002	Switch Architecture and Performance	IEEE 802.3ad link aggregation		
AS.REQ.003	Switch Architecture and Performance	IEEE 802.3x Flow control - full duplex operation		
AS.REQ.004	Switch Architecture and Performance	Should support stacking using dedicated stacking ports separate from uplink ports with support for minimum 4 switches in a single stack for high availability and quick resiliency		
AS.REQ.005	Switch Architecture and Performance	The switch should support a stacking bandwidth of minimum 50 Gbps		
AS.REQ.006	Performance Specifications	Wire speed Non-Blocking performance: Forwarding rate of minimum 45 Mpps and swithcing bandwidth of 56 Gbps		
AS.REQ.007	Resiliency	Should support Ring Protection technology as per the IEEE 802.17 or equivalent technology providing the convergence time of Sub 50 ms Convergence		
AS.REQ.008	Resiliency	Loop Detection and Loop protection		
AS.REQ.009	VLAN	GVRP / VTP or Equivalent		
AS.REQ.010	VLAN	Q In Q		
AS.REQ.011	VLAN	VRF Lite		
AS.REQ.012	Layer 3 Features	Shall support all the Layer 3 routing protocols like OSPF v3, BGP 4 , Policy based routing.		
AS.REQ.013	Layer 3 Features	Equal Cost Multi Path (ECMP) routing		
AS.REQ.014	Security	Access Control Lists (ACLs)		
AS.REQ.015	Security	DHCP snooping, IP source guard and Dynamic ARP Inspection (DAI). Should support IPv6 First Hop Security features like IPv6 snooping, IPv6 devicetracking,		

<b>Network Access Switch</b>				
<b>Sr. No.</b>	<b>Item</b>	<b>Minimum Requirement Description</b>	<b>Compliance (Yes / No)</b>	<b>Deviations / Remarks</b>
		neighbor discovery (ND) Inspection, IPv6 DHCP guard, IPv6 router advertisement (RA) guard		
AS.REQ.016	Security	Dynamic VLAN assignment		
AS.REQ.017	Security	MAC address filtering		
AS.REQ.018	Security	Private VLANs provide security and port isolation		
AS.REQ.019	Security	Secure Copy (SCP)		
AS.REQ.020	Security	Strong password security and encryption		
AS.REQ.021	Security	The switch should support flexible & multiple authentication mechanism, including 802.1X, MAC authentication bypass		
AS.REQ.022	Security	SSH and SCP		
AS.REQ.023	Security	Rate limiting is provided based on source and destination IP address, source and destination MAC address, Layer 4 TCP/UDP information		
AS.REQ.024	IPv6 Features	Shall support Ipv6 management and routing features.		
AS.REQ.025	Management Features	SNMPv1, v2c and v3		
AS.REQ.026	Management Features	IEEE 802.1AB Link Layer Discovery Protocol (LLDP)		
AS.REQ.027	Management Features	sFlow/Netflow/Jflow: a method for monitoring traffic in switched and Routed networks		
AS.REQ.028	Management Features	TFTP , NTP , Syslog		
AS.REQ.029	Management Features	Should support Unidirectional Link Detection Protocol (UDLD) that allows detection of unidirectional links caused by incorrect fiber-optic wiring or port faults		
AS.REQ.030	Multicast Support	IGMP snooping		
AS.REQ.031	Multicast Support	PIM-SM, PIM-DM, PIM-SSM		
AS.REQ.032	Multicast Support	Multicast Listener Discovery v2		
AS.REQ.033	Compliances	ROHS compliant is must		



<b>Network Access Switch</b>				
<b>Sr. No.</b>	<b>Item</b>	<b>Minimum Requirement Description</b>	<b>Compliance (Yes / No)</b>	<b>Deviations / Remarks</b>
AS.REQ.034	Compliances	IEEE 802.3az Energy Efficient Ethernet (EEE)		
AS.REQ.035	Compliances	UL,EN, IEC		
AS.REQ.036	Compliances	SFP module must be from the same OEM		

Junction Box				
Sr. No.	Item	Minimum Requirement Description	Compliance (Yes / No)	Deviations / Remarks
JB.REQ.001	General Requirement	All the junction boxes shall be out door type with <b>IP65</b> protection from rain, water. Provision for theft prevention. (Expected outdoor temperature 50°C).		
JB.REQ.002	General Requirement	<p>1.5 mm steel sheet, profiled frame construction consisting of 9 folded rolled hollow sections punched on a 25mm DIN Pitch pattern with load carrying capacity of 1000 Kgs.</p> <p>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. The hinges and retainers should be made of die cast, copper nickel chrome plated with SS hinge pins. The doors should be swapped to LH if required with door opening angle 130 deg to VDI.</p> <p>Top panel made of 1.5 mm thick sheet steel with PU foamed (Gasketing) bolttable from inside.</p> <p>Bottom panel made of 1.5 mm thick sheet steel with PU foamed (Gasketing) with provision for fixing 4 nos of PG 29 glands.</p> <p>Side panels in double walled construction with air gap of minimum 20 mm between two walls with PU foamed(Gasketing) for IP 55 protection.</p> <p>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 With 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>		

RFP for Selection of System Integrator for Implementation of Nagpur Smart City Solutions

<b>Junction Box</b>				
<b>Sr. No.</b>	<b>Item</b>	<b>Minimum Requirement Description</b>	<b>Compliance (Yes / No)</b>	<b>Deviations / Remarks</b>
JB.REQ.003	General Requirement	Should be outdoor type, Floor mounting with 3 point locking option, suitable to mount the switches and required UPS. The 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.		
JB.REQ.004	General Requirement	The cabinet will be provided with a dimension of 800mmW x 1200mmH (24UH) x 800mmD with 19" mounting arrangement suitable for the mounting of the associated network, power, UPS and Split Battery components securely and safely within the cabinet.		
JB.REQ.005	General Requirement	The junction box shall have floor mount type with required mounting accessories to provide a flexible solution for space constrained traffic applications.		
JB.REQ.006	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 the front door of the cabinet to provide ventilation to cool the equipment. Fan and Cabinet should be from same OEM for better SLA and provision to drive power for the camera is required.		
JB.REQ.007	General Requirement	75mm 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.		
JB.REQ.008	General Requirement	Small Junction box for mounting the electric meter with viewing window should be provided for mounting Electrical Meter and Fuse and MCB with separate lock for utility power connection, as per electricity board, rules.		
JB.REQ.009	General Requirement	Protection from ants, bugs and other small insects entering into the enclosure		
JB.REQ.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.		

## 1.2 City WiFi Solutions

Wireless Controller				
Sr. No.	Item	Minimum Requirement Description	Compliance (Yes / No)	Deviations / Remarks
WIC.REQ.001	Standards	Must be compliant with either IEEE CAPWAP controller-based or Autonomous based WLANs.		
WIC.REQ.002	Standards	WLAN Controller should support minimum of 5000 Access points in a single chassis. If any OEM/Bidder can't provide WLAN controller to support 5000 AP in 2RU form factor, multiple controllers must be proposed to meet the requirement from day one. Proposed controller should support N+N redundancy from day one		
WIC.REQ.003	Standards	Controller should be appliance based and must have at least 4 x 10Gbps of uplink interfaces.		
WIC.REQ.004	Standards	Controller shall support 30000 concurrent sessions per chassis.		
WIC.REQ.005	Standards	The controller shall support Cellular offload by PMIPv6/EoGRE tunneling to Mobile Core network		
WIC.REQ.006	Compatibility	Solution shall support wireless IPS feature		
WIC.REQ.007	High Availability	Must have feature for stateful recovery without re-authentication of the client in the event of LAN and WLAN infrastructure disruption to deliver a non-stop client session		
WIC.REQ.008	High Availability	Controller should have hot-swappable redundant power supplies.		
WIC.REQ.009	RF Management	Must support an ability to dynamically adjust channel and power settings based on the RF environment.		
WIC.REQ.010	RF Management	Radio coverage algorithm must allow adjacent APs to operate on different channels, in order to maximize available bandwidth and avoid interference		
WIC.REQ.011	RF Management	Must have Automatic 802.11 interference detection, identification, classification, and mitigation-		
WIC.REQ.012	RF Management	Must support coverage hole detection and correction that can be adjusted as per WLAN basis.		
WIC.REQ.013	RF Management	Must support RF Management with 20/40/80 MHz channels with 802.11a/b/g/n/ac		
WIC.REQ.014	IPv6 features	Solution should support L2 and L3 roaming of IPv6 clients		

<b>Wireless Controller</b>				
<b>Sr. No.</b>	<b>Item</b>	<b>Minimum Requirement Description</b>	<b>Compliance (Yes / No)</b>	<b>Deviations / Remarks</b>
WIC.REQ.015	IPv6 features	WLC should support IPv6 access control lists		
WIC.REQ.016	IPv6 features	WLC should support Guest-access functionality for IPv6 clients		
WIC.REQ.017	Performance	Solution performance must remain the same if encryption is on or off for wireless SSIDs.		
WIC.REQ.018	Performance	Should support ability to adjust Delivery Traffic Indicator Message (DTIM) or equivalent on a per WLAN basis to improve performance for latency sensitive applications		
WIC.REQ.019	Security	Should adhere to the strictest level of security standards, including 802.11i Wi-Fi Protected Access 2 (WPA2), WPA, Wired Equivalent Privacy (WEP), 802.1X with multiple Extensible Authentication Protocol (EAP) types, including Protected EAP (PEAP), EAP with Transport Layer Security (EAP-TLS), EAP with Tunnelled TLS (EAP-TTLS)		
WIC.REQ.020	Security	Should support Management frame protection for the authentication of 802.11 management frames by the wireless network infrastructure and must support data plane encryption		
WIC.REQ.021	Security	The solution should support a capability to shun / block WLAN client in collaboration with wired IPS on detecting malicious client traffic.		
WIC.REQ.022	Security	Controller should have rogue AP detection, classification and automatic containment feature		
WIC.REQ.023	Security	Controller should be able to detect attacks like Broadcast de-authentication, NULL probe, from day one for all access points		
WIC.REQ.024	Security	Controller should have profiling of devices based on protocols like HTTP, DHCP and more to identify the end devices on the network		
WIC.REQ.025	Functionality	Must be able to set a maximum per-user bandwidth limit on a per-SSID basis.		
WIC.REQ.026	Functionality	Must support user load balancing across Access Points.		
WIC.REQ.027	Functionality	Controller must provide Mesh capability for Mesh supported AP.		
WIC.REQ.028	Monitoring	Must be able to dedicate APs to monitor-only for Intrusion Prevention Services.		
WIC.REQ.029	Roaming:	Must support client roaming across controllers separated by a layer 3 routed boundary		

<b>Wireless Controller</b>				
<b>Sr. No.</b>	<b>Item</b>	<b>Minimum Requirement Description</b>	<b>Compliance (Yes / No)</b>	<b>Deviations / Remarks</b>
WIC.REQ.030	Roaming:	Solution proposed must support clients roaming across at least 500 APs.		
WIC.REQ.031	Operational:	Must support AP over-the-air packet capture for export to a tool such as Wire shark.		
WIC.REQ.032	Operational:	Shall support the ability to classify over 20 different types of interference with in 5 to 30 seconds.		
WIC.REQ.033	Operational:	Should provide a snapshot of air quality in terms of the performance and impact of interference on the wireless network identifying the problem areas.		
WIC.REQ.034	Operational:	Should provide an Air Quality rating on a per- radio basis to help gauge the impact of interference on the network		
WIC.REQ.035	Operational:	Should provide real-time charts showing interferers per access point, on a per-radio, per-channel basis.		
WIC.REQ.036	Operational:	Should support encrypted mechanism to securely upload/download software images to and from wireless controllers		
WIC.REQ.037	QOS:	Must support 802.11e (WMM)		
WIC.REQ.038	QOS:	Shall able to prioritize all traffic such as (Data ,voice and video)		
WIC.REQ.039	QOS:	Solution shall integrate with existing firewall or DPI device for deep packet inspection		
WIC.REQ.040	QOS:	Should have rate limiting per user and per SSID basis for encrypted tunnel mode		
WIC.REQ.041	QOS:	To deliver optimal bandwidth usage, reliable multicast must use single session between AP and Wireless Controller.		
WIC.REQ.042	Power	Should support both centralized as well as distributed traffic forwarding architecture with L3 roaming support from day 1 as well as should be IPV6 ready from day one		
WIC.REQ.043	Licensing	WLC should support AC and DC powering options		
WIC.REQ.044	Operational	WLC should support AP License Migration from one WLC to another		
WIC.REQ.045	Operational	Must support stateful switchover between active and standby controller in a sub second time frame.		

<b>Wireless Controller</b>				
<b>Sr. No.</b>	<b>Item</b>	<b>Minimum Requirement Description</b>	<b>Compliance (Yes / No)</b>	<b>Deviations / Remarks</b>
WIC.REQ.046	Operational	Solution shall be proposed with complete feature set including licensed feature.		
WIC.REQ.047	Security	Should support visibility and control based on the type of applications and should provide access or deny or rate-limit.		
WIC.REQ.048	Operational	Solution should have Deep Packet Inspection for Layer 4-7 traffic for user for all traffic across the network to analyses information about applications usage and prioritization		
WIC.REQ.049	Security	Should support AP Plug and Play (PnP) deployment with zero-configuration capability		
WIC.REQ.050	Operational	Should support encrypted mechanism to securely upload/download software image to and from Wireless controller.		
WIC.REQ.051	Wireless standard	Should support minimum 4000 VLANs		
WIC.REQ.052	Operational	Should support Hot Spot 2.0		
WIC.REQ.053	Operational	Should support minimum 500 WLANs		
WIC.REQ.054	Operational	Should support dynamic VLAN assignment		
WIC.REQ.055	Operational	Should able to do dynamic channel bonding based on interference detected on particular channel.		
WIC.REQ.056	Operational	Must support coverage hole detection and correction that can be adjusted on a per WLAN basis.		
WIC.REQ.057	Operational	Should provide visibility to Network airtime in order to set the airtime policy enforcement		
WIC.REQ.058	Security	Must support dynamic Airtime allocation on per WLAN, per AP, Per AP group basis.		
WIC.REQ.059	Security	Should support web-based authentication to provide a browser-based environment to authenticate clients that do not support the IEEE 802.1X supplicant.		

<b>Wireless Controller</b>				
<b>Sr. No.</b>	<b>Item</b>	<b>Minimum Requirement Description</b>	<b>Compliance (Yes / No)</b>	<b>Deviations / Remarks</b>
WIC.REQ.060	Security	Should support port-based and SSID-based IEEE 802.1X authentication.		
WIC.REQ.061	Security	Should support MAC authentication to provide simple authentication based on a user's MAC address.		
WIC.REQ.062	Security	Should support Rogue AP detection, classification and standard WIPS signatures.		
WIC.REQ.063	General	Should be able to exclude clients based on excessive/multiple authentication failure.		
WIC.REQ.064	General	The Wireless solution offered must be from the leaders or Challengers quadrant for Wired and Wireless access LAN Magic Quadrant published by Gartner as on the day of publication of this RFP		



<b>Wireless Intrusion Prevention System</b>				
<b>Sr. No.</b>	<b>Item</b>	<b>Minimum Requirement Description</b>	<b>Compliance (Yes / No)</b>	<b>Deviations / Remarks</b>
WIPS.REQ.001	Operational	The WIPS system needs to have dedicated wireless security devices for monitoring the air space, detecting unauthorized connections and a centralized server that analyses the data received from Sensor		
WIPS.REQ.002	Power	The sensor should be capable of handling wireless devices that are typically visible at a location in a large deployment (e.g., 200 to 500 APs, 200 to 500 clients)		
WIPS.REQ.003	Licensing	The sensor should completely support the IEEE 802.11a/b/g/n technology and support both the 2.4 & 5.0 GHz bands		
WIPS.REQ.004	Operational	The communication between the sensor and WIPS server should be secure		
WIPS.REQ.005	Operational	The WIPS system should support centralized policy management		
WIPS.REQ.006	Security	The WIPS system should support wireless LAN security policy definition		
WIPS.REQ.007	Security	WIPS Server & Sensors should not require frequent signature updates		
WIPS.REQ.008	Operational	WIPS System should have zero-day attack detection and prevention capabilities		
WIPS.REQ.009	Wireless standard	The WIPS system should be based on industry standards		
WIPS.REQ.010	Operational	The WIPS system should automatically detect & classify authorized NMC APs without any manual intervention		
WIPS.REQ.011	Operational	The WIPS system should support AP restriction by SSID, vendor type, protocol, encryption, authentication and the type of radio		
WIPS.REQ.012	Security	The WIPS system server should be accessible from anywhere using a web browser and provide access restriction to particular computers [IP pools etc.]		
WIPS.REQ.013	Security	The WIPS system should auto-classify APs as managed, external and rogue APs		

<b>Wireless Intrusion Prevention System</b>				
<b>Sr. No.</b>	<b>Item</b>	<b>Minimum Requirement Description</b>	<b>Compliance (Yes / No)</b>	<b>Deviations / Remarks</b>
WIPS.REQ.014	Security	The WIPS system should have the capability of auto-classifying Wi-Fi clients as authorized, guest, rogue or external in addition to manual classification w.r.t. NMC network		
WIPS.REQ.015	Security	The WIPS system should correctly detect Smart-devices connecting to NMC network and classify them as approved or unapproved.		
WIPS.REQ.016	Security	The WIPS system should support automatic detection of whether an AP is ON or OFF the NMC wired network		
WIPS.REQ.017	Operational	Layer-2 unencrypted and Layer-2 encrypted (WEP, WPA and WPAv2)		
WIPS.REQ.018	Operational	Smartphones and other Wi-Fi enabled devices tethering when connected to NMC Backbone network		
WIPS.REQ.019	Operational	The WIPS system should detect miss configured authorized NMC APs		
WIPS.REQ.020	Operational	The WIPS system should detect NMC's wireless client connecting to an outside AP		
WIPS.REQ.021	Operational	The WIPS system should detect an outside client trying to connect to the NMC's WLAN		
WIPS.REQ.022	Operational	The WIPS system should detect an Ad hoc connection involving NMC authorized Wi-Fi devices		
WIPS.REQ.023	Operational	The WIPS system should detect masquerading attacks on both APs and clients(MAC spoofing attacks)		
WIPS.REQ.024	Operational	The WIPS system should detect Honey Pot (aka "Evil-Twin") attacks		
WIPS.REQ.025	Operational	The WIPS system should detect AP MAC spoofing attacks across multiple locations and VLANs		
WIPS.REQ.026	Operational	The WIPS system should detect Layer-2 based wireless Denial of Service (DoS) attacks on NMC WLAN		
WIPS.REQ.027	Operational	The WIPS system should have configurable intrusion alert severity levels		
WIPS.REQ.028	Operational	The WIPS system should support location tracking of a DoS attacker		

<b>Wireless Intrusion Prevention System</b>				
<b>Sr. No.</b>	<b>Item</b>	<b>Minimum Requirement Description</b>	<b>Compliance (Yes / No)</b>	<b>Deviations / Remarks</b>
WIPS.REQ.029	Operational	The WIPS system should detect APs configured for multiple SSIDs		
WIPS.REQ.030	Operational	The WIPS system should be able to detect a NMC Client bridging its Wired and Wireless interfaces or participating in ICS		
WIPS.REQ.031	Operational	The WIPS system should be capable of automatic prevention		
WIPS.REQ.032	Operational	The WIPS system should prevent any Layer-2 based wireless Denial of Service (DoS) attacks		
WIPS.REQ.033	Operational	The WIPS system should NOT affect the operation of an external (i.e. neighbours) or a managed access point while preventing a rogue AP on the same channel		
WIPS.REQ.034	Operational	The WIPS system should allow a manual override for Intrusion Prevention		
WIPS.REQ.035	Operational	A single sensor should simultaneously block any attacks and continue to scan/detect new vulnerabilities		
WIPS.REQ.036	Operational	The WIPS system should prevent aggressive client connections		
WIPS.REQ.037	Operational	A single sensor should simultaneously block multiple threats on multiple channels		
WIPS.REQ.038	Operational	The WIPS system should locate APs on live coverage maps		
WIPS.REQ.039	Operational	The WIPS system should locate clients (including ad hoc clients) on live coverage map		
WIPS.REQ.040	Operational	The WIPS system should provide notification mechanisms via email and Syslog messages for critical security breaches (i.e. a new rogue AP found)		
WIPS.REQ.041	Operational	The WIPS system should send notifications based on location and alarm type		
WIPS.REQ.042	Operational	The WIPS system should support addition of tags and notes to devices		
WIPS.REQ.043	Operational	The WIPS system support addition of acknowledgement notes to system alerts		

<b>Wireless Intrusion Prevention System</b>				
<b>Sr. No.</b>	<b>Item</b>	<b>Minimum Requirement Description</b>	<b>Compliance (Yes / No)</b>	<b>Deviations / Remarks</b>
WIPS.REQ.044	Operational	The WIPS system should provide a device summary (for APs, sensors, and clients) report per location		
WIPS.REQ.045	Operational	The WIPS system should provide an event summary report		
WIPS.REQ.046	Operational	The WIPS system should categorize events by location (for ease of management)		
WIPS.REQ.047	Operational	The WIPS system should allow customization of existing reports and creation of new reports by end-user		
WIPS.REQ.048	Operational	Should Automatically blacklist clients based on DoS/MITM attacks		
WIPS.REQ.049	Operational	Should detect rough clients/ AP on Wired network by querying routers and switches		
WIPS.REQ.050	Operational	Should support for Off-channel rogue containment		
WIPS.REQ.051	Operational	Should support historic data retention		
WIPS.REQ.052	Operational	Should provide Integrated PCI reports for easy auditing		
WIPS.REQ.053	Operational	Must support RFID asset tags for location tracking.		
WIPS.REQ.054	Operational	Should provide Open APIs / SDK for app development		
WIPS.REQ.055	Operational	Should be able to provide location accuracy within 3 meters without requiring any special client App.		
WIPS.REQ.056	Operational	Clients and tags should be tracked in indoor, indoor high-ceiling, and outdoor environments		
WIPS.REQ.057	Operational	The system shall offers analytic dashboard for guest access usage info		
WIPS.REQ.058	Operational	The system shall provides location Analytic service that provides real-time live analytic of demograhic infomation		
WIPS.REQ.059	Operational	Analytics dashboard should provide real-time information on Wi-Fi client count and Client Dwell-Time		
WIPS.REQ.060	Operational	Should support creating logical zones within a venue to understand relative utilization of different areas and to identify trends such as foot traffic in different parts of a store		

<b>Wireless Intrusion Prevention System</b>				
<b>Sr. No.</b>	<b>Item</b>	<b>Minimum Requirement Description</b>	<b>Compliance (Yes / No)</b>	<b>Deviations / Remarks</b>
WIPS.REQ.061	Operational	Historical data on the elements being tracked should be collected and stored for for drawing up trends and faster troubleshooting		

<b>Centralized WiFi Management System</b>				
<b>Sr. No.</b>	<b>Item</b>	<b>Minimum Requirement Description</b>	<b>Compliance (Yes / No)</b>	<b>Deviations / Remarks</b>
CWS.REQ.001	General	NMC proposes to procure a centralized authentication system for its proposed Wi-Fi network. The system shall authenticate the City WiFi users of NMC. The system shall also provide facilities like web self-care.		
CWS.REQ.002	General	The system shall comply to the DoT guidelines regarding provision of Wi-Fi internet service under un-licensed frequency band		
CWS.REQ.003	General	The Solution Shall Support Captive portal having customizable GUI. This portal should be available to any client coming into the Wi-Fi zone of NMC		
CWS.REQ.004	General	Captive portal shall allow local branding and content as per the location.		
CWS.REQ.005	General	Solution shall be able to restrict the bandwidth as per the policies. Solution shall have configurable GUI for Policy management to differentiate location wise Bandwidth policies		
CWS.REQ.006	General	The solution shall support Usage based as well as Time duration based accounting. It shall support real time disconnection on completion of allotted resources i.e. Time or Data		
CWS.REQ.007	General	The solution shall support centralized server for User authentication		
CWS.REQ.008	General	The application should be IPv4 and IPv6 compliant.		
CWS.REQ.009	Administration	GUI based management console for system administration, policy / package creation, backup and restore accounting data, SMS gateway configuration etc.,		

<b>Centralized WiFi Management System</b>				
<b>Sr. No.</b>	<b>Item</b>	<b>Minimum Requirement Description</b>	<b>Compliance (Yes / No)</b>	<b>Deviations / Remarks</b>
CWS.REQ.010	Administration	Tool for Troubleshooting and Health Diagnostic		
CWS.REQ.011	Administration	Creation of batches in advance and activation upon first usage		
CWS.REQ.012	Administration	Generation of report of usage and accounting, real time usage of USER as per the location.		
CWS.REQ.013	Administration	Access Control List for different accounting and report related activities		
CWS.REQ.014	Administration	Management of different Packages.		
CWS.REQ.015	Administration	Centralized system shall available in Failover mode		
CWS.REQ.016	Administration	Policy based access control for administrative activities		
CWS.REQ.017	Administration	Login and session details, browsing history and audit trails		
CWS.REQ.018	Subscriber Management	Creation of subscribers as per the required packages. Activation of subscribers as per the usage		
CWS.REQ.019	Subscriber Management	Renewal / Registration of the subscriber.		
CWS.REQ.020	Subscriber Management	Portal providing Self registration.		
CWS.REQ.021	Accounting and Billing features	Creation of various packages		
CWS.REQ.022	Accounting and Billing features	Real time accounting of the usage		
CWS.REQ.023	Accounting and Billing features	Location wise usage and billing detail		

<b>Centralized WiFi Management System</b>				
<b>Sr. No.</b>	<b>Item</b>	<b>Minimum Requirement Description</b>	<b>Compliance (Yes / No)</b>	<b>Deviations / Remarks</b>
CWS.REQ.024	Subscriber Management System & database	It shall offer complete subscriber management features in Subscriber Management options which mainly focuses on creating, editing, updating, renewing, deleting, and managing of accounts for all subscribers.		
CWS.REQ.025	Subscriber Management System & database	It shall support multiple Login Controls		
CWS.REQ.026	Subscriber Management System & database	It shall support Guest Management.		
CWS.REQ.027	Subscriber Management System & database	It shall support bulk username and password creation		
CWS.REQ.028	Subscriber Management System & database	It shall support centralized Profile creation & Subscriber Provisioning		
CWS.REQ.029	Subscriber Management System & database	It shall support Web self-care for subscriber to track usage summary		
CWS.REQ.030	Subscriber Management System & database	It shall support different customer acquisition process for Public WiFi users		
CWS.REQ.031	Subscriber Management System & database	It shall support time bound username & password generation for WiFi users		

<b>Centralized WiFi Management System</b>				
<b>Sr. No.</b>	<b>Item</b>	<b>Minimum Requirement Description</b>	<b>Compliance (Yes / No)</b>	<b>Deviations / Remarks</b>
CWS.REQ.032	Subscriber Management System & database	It shall be able to bind the MAC of WiFi users		
CWS.REQ.033	Subscriber Management System & database	It shall have centralized Database which enables administrator easily manage database from a single point in distributed Architecture		
CWS.REQ.034	Subscriber Management System & database	It shall allow administrator to define whether the subscriber has to be added to the existing customer database or added as a fresh customer. Multiple subscribers shall be added under same customer. Administrator can define the username & password by which the subscriber can login.		
CWS.REQ.035	Subscriber Management System & database	It shall allow administrator to lists down the complete subscriber list in the system and allows updating or modifying subscriber information as required. Administrator can select the customer name from the list and update details.		
CWS.REQ.036	Subscriber Management System & database	The database for the system is to be provided by the vendor along with the required hardware, software, etc to maintain logs as per TRAI guidelines issued time to time.		
CWS.REQ.037	Self Service Portal	This shall work as interface between NMC and City Wi-Fi user. Any prospective user coming into NMC public hotspot shall be presented a webpage portal giving details of Wi-Fi services, tariffs and procedure to subscribe to the services. Citizen should be able to make payment through this portal		
CWS.REQ.038	Self Service Portal	The subscriber shall be able to check his Wi-Fi account details		
CWS.REQ.039	Self Service Portal	Shall be able to change his password		
CWS.REQ.040	Self Service Portal	Shall be able to create new WiFi accounts through Captive/Web portal		



<b>Centralized WiFi Management System</b>				
<b>Sr. No.</b>	<b>Item</b>	<b>Minimum Requirement Description</b>	<b>Compliance (Yes / No)</b>	<b>Deviations / Remarks</b>
CWS.REQ.041	Self Service Portal	Shall be able to display the complete information includes IP address using which the subscriber logged in as well as the MAC address of the subscriber (if MAC binding option is selected).		
CWS.REQ.042	Self Service Portal	For security reasons it shall suggest subscribers to regularly change or update their password.		
CWS.REQ.043	Self Service Portal	It shall allow subscribers to update personal details and contact information		

<b>Access Point - Outdoor</b>				
<b>Sr. No.</b>	<b>Item</b>	<b>Minimum Requirement Description</b>	<b>Compliance (Yes / No)</b>	<b>Deviations / Remarks</b>
APO.REQ.001	Hardware	Must have a robust design for durability, without visible vents		
APO.REQ.002	Hardware	Must include dual band Internal / External antennas to support both the 2.4GHz and 5GHz operations simultaneously from single antenna.		
APO.REQ.003	Hardware	Mounting kit should be from OEM which shall be used for mounting access point		
APO.REQ.004	Hardware	Access point shall support pole, wall, and roof mounting options.		
APO.REQ.005	Hardware	Access Points proposed must include radios for both 2.4 GHz and 5 GHz.		
APO.REQ.006	Wireless Standard	Must support 2X2 multiple-input multiple-output (MIMO) with TWO spatial streams		
APO.REQ.007	Wireless Standard	Must support simultaneous 802.11n on both the 2.4 GHz and 5 GHz radios.		

<b>Access Point - Outdoor</b>				
<b>Sr. No.</b>	<b>Item</b>	<b>Minimum Requirement Description</b>	<b>Compliance (Yes / No)</b>	<b>Deviations / Remarks</b>
APO.REQ.008	Wireless Standard	Must support data rates upto 300 Mbps		
APO.REQ.009	Wireless Standard	Must support 40 MHz wide channels in 5 GHz and 20 MHz wide channel in 20 GHz		
APO.REQ.010	Wireless Standard	Must support upto 27dbm of transmit power in both 2.4Ghz and 5Ghz radios		
APO.REQ.011	RF	The Wireless AP should have the technology to improve downlink performance.		
APO.REQ.012	RF	The AP shall be able to load-balance between 2.4Ghz and 5Ghz band.		
APO.REQ.013	RF	Must incorporate radio resource management for power, channel, no grey areas and performance optimization		
APO.REQ.014	RF	Must have -93 dB or better Receiver Sensitivity.		
APO.REQ.015	Mesh	The Wireless Backhaul shall operate in 5Ghz		
APO.REQ.016	Mesh	Support Encrypted and authenticated connectivity between all backhaul components		
APO.REQ.017	Mesh	Should have two RJ-45 auto-sensing 10/100/1000 Mbps port and a console port.		
APO.REQ.018	Mesh	Mesh should support QoS for voice over wireless.		
APO.REQ.019	Roaming	Must support Proactive Key Caching and/or other methods for Fast Secure Roaming.		
APO.REQ.020	Security	shall support 802.11w standard for communication between AP and controller		
APO.REQ.021	Security	Should support locally-significant certificates on the APs using a Public Key Infrastructure (PKI).		
APO.REQ.022	Security	Provision of Wireless IPS to filter malicious traffic		

<b>Access Point - Outdoor</b>				
<b>Sr. No.</b>	<b>Item</b>	<b>Minimum Requirement Description</b>	<b>Compliance (Yes / No)</b>	<b>Deviations / Remarks</b>
APO.REQ.023	Encryption	Access Points must support a distributed encryption/decryption model.		
APO.REQ.024	Encryption	Access Points must support hardware based encryption		
APO.REQ.025	Monitoring	Must support the ability to serve clients and monitor the RF environment.		
APO.REQ.026	Flexibility:	Must support 16 WLANs per AP for SSID deployment flexibility.		
APO.REQ.027	Operational	Must support telnet or SSH or console login to APs directly for troubleshooting flexibility.		
APO.REQ.028	Operational	Must support locking option for Theft Protection or equivalent		
APO.REQ.029	Operational	Proposed access point shall support MDO ( Mobile Data offload)		
APO.REQ.030	Power:	Must support Power over Ethernet (802.3af ) / 802.3at		
APO.REQ.031	Quality of Service:	shall have the support of 802.11e and WMM		
APO.REQ.032	Quality of Service:	Must support Reliable Multicast Video to maintain video quality		
APO.REQ.033	Quality of Service:	Must support QoS to prioritize video ,voice and Data traffic		
APO.REQ.035	Environmental and Electrical Specifications	Geographic orientation flexibility – tilt angle for pole, wall, and roof mounting units		
APO.REQ.036	Environmental and Electrical Specifications	The equipment shall support up to 100 MPH sustained winds &140 MPH wind gusts.		
APO.REQ.037	Environmental and Electrical Specifications	The Access point shall be IP67 certified. The quoted wireless Access point should be WPC – ETA approved.		

<b>Access Point - Outdoor</b>				
<b>Sr. No.</b>	<b>Item</b>	<b>Minimum Requirement Description</b>	<b>Compliance (Yes / No)</b>	<b>Deviations / Remarks</b>
APO.REQ.038	Environmental and Electrical Specifications	The Access point shall be rated for operation over an ambient temperature range of 0° C to + 60° C		
APO.REQ.039	Operational	Should be able to support LTE & WiMAX Signal Rejection		
APO.REQ.040	Power	Should be able to support PoE, DC powering option		
APO.REQ.041	Operational	Should support both centrally controlled mode (configured and updated via wireless controller) and autonomous mode (without controller) which is software selectable		
APO.REQ.042	Wireless Standard	Certified for interoperability with all IEEE 802.11a/b/g/n client devices.		

<b>Access Point - Indoor</b>				
<b>Sr. No.</b>	<b>Item</b>	<b>Minimum Requirement Description</b>	<b>Compliance (Yes / No)</b>	<b>Deviations / Remarks</b>
API.REQ.001	Hardware	Must have a robust design for durability, without visible vents		
API.REQ.002	Hardware	Must include dual band antennas to support both the 2.4GHz and 5GHz operations simultaneously from single antenna.		
API.REQ.003	Hardware	Mounting kit should be from OEM which shall be used for mounting access point		
API.REQ.004	Hardware	Access point shall support pole, wall, and roof mounting options.		
API.REQ.005	Hardware	Access Points proposed must include radios for both 2.4 GHz and 5 GHz.		
API.REQ.006	Wireless Standard	Must support 2x2 or 3x3 multiple-input multiple-output (MIMO) with TWO spatial streams		
API.REQ.007	Wireless Standard	Must support simultaneous 802.11n on both the 2.4 GHz and 5 GHz radios and 802.11ac on 5ghz.		
API.REQ.008	Wireless Standard	Must support data rates upto 860 Mbps on 5Ghz radio and 144 mbps on 2.4Ghz radio.		
API.REQ.009	Wireless Standard	Must support 40 MHz wide channels in 5 GHz and 20 MHz wide channel in 20 GHz		
API.REQ.010	Wireless Standard	Must support up to 22dbm of transmit power in both 2.4Ghz and 5Ghz radios		
API.REQ.011	RF	The Wireless AP should support technology to improve downlink performance		
API.REQ.012	RF	The AP shall be able to load-balance between 2.4Ghz and 5Ghz band.		
API.REQ.013	RF	Must incorporate radio resource management for power, channel, no grey areas and performance optimization		
API.REQ.014	RF	Must have -100B or better Receiver Sensitivity.		
API.REQ.015	Mesh	The Wireless Backhaul shall operate in 5Ghz		
API.REQ.016	Mesh	Support Encrypted and authenticated connectivity between all backhaul components		

<b>Access Point - Indoor</b>				
<b>Sr. No.</b>	<b>Item</b>	<b>Minimum Requirement Description</b>	<b>Compliance (Yes / No)</b>	<b>Deviations / Remarks</b>
API.REQ.017	Mesh	Access point must have two 10/100/1000BASE-T Ethernet, autosensing (RJ-45) interface		
API.REQ.018	Mesh	Mesh should support QoS for voice over wireless.		
API.REQ.019	Roaming	Must support Proactive Key Caching and/or other methods for Fast Secure Roaming.		
API.REQ.020	Security	Shall support 802.11w standard for communication between AP and controller		
API.REQ.021	Security	Should support locally-significant certificates on the APs using a Public Key Infrastructure (PKI).		
API.REQ.022	Security	Provision of Wireless IPS to filter malicious traffic		
API.REQ.023	Encryption	Access Points must support a distributed encryption/decryption model.		
API.REQ.024	Encryption	Access Points must support encryption		
API.REQ.025	Monitoring	Must support the ability to serve clients and monitor the RF environment concurrently.		
API.REQ.026	Flexibility:	Must support 16 WLANs per AP for SSID deployment flexibility.		
API.REQ.027	Operational	Must support telnet or SSH or console login to APs directly for troubleshooting flexibility.		
API.REQ.028	Operational	Must support locking option for Theft Protection or equivalent		
API.REQ.029	Operational	Proposed access point shall support MDO ( Mobile Data offload)		
API.REQ.030	Power:	Must support Power over Ethernet (802.3af / at)		
API.REQ.031	Quality of Service:	shall have the support of 802.11e and WMM		
API.REQ.032	Quality of Service:	Must support Reliable Multicast Video to maintain video quality		
API.REQ.033	Quality of Service:	Must support QoS to prioritize video ,voice and Data traffic		
API.REQ.034	Certifications and standard	The quoted wireless Access point should be WPC – ETA approved.		
API.REQ.035	Flexibility:	Same model AP that serves clients must be able to be dedicated to monitoring the RF environment.		
API.REQ.036	Flexibility:	Must support Controller-based and standalone (autonomous) deployments		

Access Point - Indoor				
Sr. No.	Item	Minimum Requirement Description	Compliance (Yes / No)	Deviations / Remarks
API.REQ.037	Operational	Should have capability to detect and classify non-Wi-Fi wireless transmissions while simultaneously serving network traffic		
API.REQ.038	Operational	Each radio to have a dedicated memory and CPU		
API.REQ.039	Power	Must support Power over Ethernet, power adaptor, and power injectors.		
API.REQ.040	Operational	Must be plenum-rated (UL2043)		

### 1.3 City Surveillance

Fixed Box Surveillance Camera (HD)				
Sr. No.	Item	Minimum Requirement Description	Compliance (Yes / No)	Deviations / Remarks
FBC.REQ.001	General Requirements	The camera should be manufacturer's official product line designed for commercial / industrial 24x7x365 use. The camera and camera firmware should be designed and developed by same OEM		
FBC.REQ.002	Image Sensor with WDR	1/3.2" with True WDR, Progressive CMOS Sensor or better		
FBC.REQ.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.REQ.004	Resolution	Active Pixels 1920(w) x 1080(h)		
FBC.REQ.005	Minimum illumination	Colour: 0.3 lux or better, B/W: 0.05 lux or better		
FBC.REQ.006	Video Encoder	H.264, Motion JPEG		
FBC.REQ.007	Frame Rate	min. 25 FPS or higher		
FBC.REQ.008	Local Storage	32 GB SD Card or higher		
FBC.REQ.009	Ethernet	10/100/ Base-T ports		
FBC.REQ.010	Image Compression	H.264, MJPEG		
FBC.REQ.011	Protocols	Minimum of the following protocols to be supported RTSP, RTP/TCP, RTP/UDP, HTTP, HTTPS, DHCP		
FBC.REQ.012	Industry Standards	ONVIF Compliant		
FBC.REQ.013	Power Supply	POE IEE 802.3af compliant		
FBC.REQ.014	Operating Temperature	0° C to 50° C or better		
FBC.REQ.015	Operating Humidity	0% to 90% for cameras		



<b>Fixed Box Surveillance Camera (HD)</b>				
<b>Sr. No.</b>	<b>Item</b>	<b>Minimum Requirement Description</b>	<b>Compliance (Yes / No)</b>	<b>Deviations / Remarks</b>
FBC.REQ.016	Enclosure	IP 66		
FBC.REQ.017	Certifications	UL, CE, FCC, ONVIF 2.x/S		
FBC.REQ.018	Support	The system should not be an end of life / end of service product.		
FBC.REQ.019	Streaming	The camera shall be able to setup and stream out minimum two (2) stream profiles. Each stream profile can has its own compression, resolution, frame rate and quality independently.		
FBC.REQ.020	White Balance	Auto / Manual		
FBC.REQ.021	Back Light Compensation	Auto		
FBC.REQ.022	Security	Security Password protection		
FBC.REQ.023	Miscellaneous	Vandal and impact resistant housing, IK 10, IP66/ NEMA 4X		
FBC.REQ.024		Detection of camera tampering and Detection of Motion should be possible using either camera or VMS		

<b>Surveillance Camera - PTZ (HD)</b>				
<b>Sr. No.</b>	<b>Item</b>	<b>Minimum Requirement Description</b>	<b>Compliance (Yes / No)</b>	<b>Deviations / Remarks</b>
PTZ.REQ.001	General Requirements	The camera should be manufacturer's official product line designed for 24x7x365 use. The camera and camera firmware should be designed and developed by same OEM.		
PTZ.REQ.002	General Requirements	The camera should be based upon standard components and proven technology using open and published protocols		
PTZ.REQ.003	Image Sensor with WDR	1/3.2" with True WDR, Progressive CMOS Sensor or better		
PTZ.REQ.004	Resolution	Camera should be HD PTZ 1920 (w) x1080 (h)		
PTZ.REQ.005	lens specs	Compatible to image sensor, Focal length 4.7–94m, Auto Iris, Full HD (1080P), F/1.6, IR Corrected – Day / Night mode- Colour		
PTZ.REQ.006	Minimum illumination	Colour: 0.3 lux, B/W: 0.05 lux or better		
PTZ.REQ.007	Pre-set Positions	100 or better, Pre-set tour		
PTZ.REQ.008	Pan	360° endless, 450°/s		
PTZ.REQ.009	Tilt Range	Manual/programmable; speed : 450°/sec; angle :0-180° or proportional speed needs to be provided		
PTZ.REQ.010	Zoom	20x optical zoom and should support digital zoom feature		
PTZ.REQ.011	General	The camera shall be able to setup and stream out minimum two (2) stream profiles. Each stream profile can has its own compression, resolution, frame rate and quality independently.		
PTZ.REQ.012	Outdoor Protection	The camera should be complete with IP 66 rated housing, Connectors, Camera Mounts, Power Supply and all Ancillary Equipment & all accessories.		
PTZ.REQ.013	Protocol	IPv4, TCP/IP, HTTPS, FTP, SMTP, SNMP, RTP, RTSP, DDNS, DHCP, DNS, NTP, UDP		

<b>Surveillance Camera - PTZ (HD)</b>					
<b>Sr. No.</b>	<b>Item</b>	<b>Minimum Requirement Description</b>	<b>Compliance (Yes / No)</b>	<b>Deviations / Remarks</b>	
PTZ.REQ.014	Compression Capability	H.264 @ 25fps and Motion JPEG compression			
PTZ.REQ.015	Certificate	FCC, CE, UL, ONVIF 2.x/S			
PTZ.REQ.016	Industry Standards	ONVIF Compliant			
PTZ.REQ.017	Miscellaneous	Compliance to Vandal and impact resistant housing – IP66 / NEMA 4X, IK10			
PTZ.REQ.018		Power Supply : External 12V /24V/48V DC/ POE			
PTZ.REQ.019		Connectors: 10Base-T/100Base-TX			
PTZ.REQ.020		Cable routing through base or rear of housing			
PTZ.REQ.021		Operating conditions unit: 0° C to 50° C or better, humidity 0% to 90% non-condensing			
PTZ.REQ.022		Tamper Proof			
PTZ.REQ.023		Detection of camera tampering and Detection of Motion should be possible using either camera or VMS			
PTZ.REQ.024		Support	The system should not be an end of life / end of service product.		
PTZ.REQ.025		Audio	Audio capture Capability		
PTZ.REQ.026	Local Storage	32GB or higher			
PTZ.REQ.027	Security	Password Protection			

IP Dome Camera				
Sr. No.	Item	Minimum Requirement Description	Compliance (Yes / No)	Deviations / Remarks
IPDC.REQ.001	Image Sensor with WDR	1/3.2" with True WDR, Progressive CMOS Sensor or better		
IPDC.REQ.002	Maximum resolution	2 MP HD		
IPDC.REQ.003	Minimum Illumination	0.3 lux in colour mode; 0.2 lux or better in B/W with IR		
IPDC.REQ.004	Lens	min 3 to 10 mm fixed/verifocal lense with Remote focus		
IPDC.REQ.005	Ethernet	10/100/ Base-T ports		
IPDC.REQ.006	Frame Rate	min 25fps or better		
IPDC.REQ.007	Image Compression	H.264, MJPEG		
IPDC.REQ.008	Protocols	Minimum of the following RTSP, RTP/TCP, RTP/UDP, HTTP, DHCP protocols to be supported		
IPDC.REQ.009	Operating Temperature	0° C to 50° C degrees or better		
IPDC.REQ.010	Power supply	POE IEE 802.3af compliant		
IPDC.REQ.011	Support	The system should not be an end of life / end of service product.		
IPDC.REQ.012	Industry Standards	ONVIF Compliant		
IPDC.REQ.013	Certifications	UL, CE, FCC, ONVIF 2.X/S		
IPDC.REQ.014	Storage	32 GB or higher		
IPDC.REQ.015	White Balance	Auto / Manual		
IPDC.REQ.016	BLC	ON/OFF		
IPDC.REQ.017	Security	Password protection		
IPDC.REQ.018	Casing	IP 66 vandal resistant		
IPDC.REQ.019	Camera Tampering	Detection of camera tampering and Detection of Motion should be possible using camera. Functionality to be enabled vide VMS		
IPDC.REQ.020	Streaming	The camera shall be able to setup and stream out minimum two (2) stream profiles. Each stream profile can has its own compression, resolution, frame rate and quality independently.		

<b>MultiSensor 360° Camera</b>				
<b>Sr. No.</b>	<b>Item</b>	<b>Minimum Requirement Description</b>	<b>Compliance (Yes / No)</b>	<b>Deviations / Remarks</b>
MSC.REQ.001	General Requirements	The camera should be manufacturer's official product line designed for commercial / industrial 24x7x365 use. The camera and camera firmware should be designed and developed by same OEM.		
MSC.REQ.002	General Requirements	The camera should be based upon standard components and proven technology using open and published protocols		
MSC.REQ.003	Image Sensor	Minimum 4 x 3MP, 1/3.2" CMOS - (Total) 12MP or better		
MSC.REQ.004	Lens Specs	F2.0, IR Corrected; Options of 2.8/4/8/12/16 MM Lens		
MSC.REQ.005	Maximum Resolution	8192(H) x 1536(V)		
MSC.REQ.006	Minimum illumination	Colour: 0.6 lux or better, Monochrome: 0.05 Lux or better with IR		
MSC.REQ.007	Video Compression	H.264, Motion JPEG		
MSC.REQ.008	Frame Rate	15fps or better		
MSC.REQ.009	Wide Dynamic Range	100 dB or better		
MSC.REQ.010	Network Interface	100 Base-T ports		
MSC.REQ.011	Power Supply	POE IEE 802.3af compliant		
MSC.REQ.012	Industry Standards	ONVIF Compliant		
MSC.REQ.013	Certifications	UL, FCC		
MSC.REQ.014	Enclosure Type	IP66; IK 10		
MSC.REQ.015	Operating Temperature	0° C to 50° C or better		
MSC.REQ.016	Operating Humidity	0 - 90%		
MSC.REQ.017	Supported Network protocols	Minimum of the following RTSP, RTP/TCP, RTP/UDP, HTTP, DHCP protocols to be supported		
MSC.REQ.018	Support	The system should not be an end of life / end of service product.		

IR Illuminator - Field Location				
Sr. No.	Item	Minimum Requirement Description	Compliance (Yes / No)	Deviations / Remarks
IRI.REQ.001	Range Distance	Minimum 50 Mtrs		
IRI.REQ.002	Adaptive illumination	10 to 80 degrees using lens; High sensitivity at Zero lux		
IRI.REQ.003	Power	Input 100-240V AC, or 12/24 V AC/DC		
IRI.REQ.004	Casing	IP66 rated / NEMA 4X vandal resistance		
IRI.REQ.005	Operating Condition	0° to 50°C or better		
IRI.REQ.006	Certification	CE,FCC, EN/UL, RoHS		
IRI.REQ.007	Lighting	High Definition LED's		
IRI.REQ.008	Required Accessories	Power Supply, Mounting Clamps, U-bracket		
IRI.REQ.009	Support	The system should not be an end of life / end of service product.		

<b>Thermal Cameras</b>				
<b>Sr. No.</b>	<b>Item</b>	<b>Minimum Requirement Description</b>	<b>Compliance (Yes / No)</b>	<b>Deviations / Remarks</b>
ThC.REQ.001	Type	Multi Sensor		
ThC.REQ.002	Video Compression	MJPEG, MPEG-4 / H.264		
ThC.REQ.003	Thermal Sensor Resolution	320 x 240, 7.5HZ		
ThC.REQ.004	Thermal Sensor	320 x 240 pixels Focal Plan Array, uncooled Vanadium Oxide (VOx) / Amorphous Silicon Microbolometer		
ThC.REQ.005	Thermal Lens	Minimum 90 mm		
ThC.REQ.006	Thermal Sensitivity	<=50 mK or better		
ThC.REQ.007	Pixel Pitch	<=25µm		
ThC.REQ.008	Thermal Detection Range	Should detect an object of size 2.5m X 2.5m for minimum 6Km and Human for minimum 2.2Km		
ThC.REQ.009	Thermal Minimum Illumination	Suitable for pitch-dark conditions (Zero Lux)		
ThC.REQ.010	Visible Sensor Resolution	Minimum 375,000 pixels		
ThC.REQ.011	Visual Sensor Lens	3.4mm to 119mm 35X optical zoom or better		
ThC.REQ.012	Output Type	IP (ONVIF Compliant) and Analogue		
ThC.REQ.013	Pan and Tilt	Pan: 360°; 0.2° to 60°/s, Tilt: +90° to -90° range; Minimum 30°/s		
ThC.REQ.014	Prest Positions	64 Presets		
ThC.REQ.015	Casing	NEMA 4X / IP-66 rated with built-in heater		
ThC.REQ.016	Operating conditions	-5° to 50°C		
ThC.REQ.017	Certification	UL / CE / FCC / EN		

Variable Message Sign Board – VaMS				
Sr. No.	Item	Minimum Requirement Description	Compliance (Yes / No)	Deviations / Remarks
VaMS.REQ.001	Dimension Requirements	VaMS shall be full-matrix type (adjustable text size and allow both upper and lower case).		
VaMS.REQ.002	Display Requirements	Electronic-High Luminosity wide viewing angle oval LEDs (Only Nichia LED) for outdoor ambient light shall be used.		
VaMS.REQ.003	Display Requirements	Long life LEDs with minimum working of 1,00,000 hours to Half Life		
VaMS.REQ.004	Display Requirements	VMS shall automatically adjust their brightness under varying light conditions to maintain legibility		
VaMS.REQ.005	Display Requirements	The luminance of VaMS's should meet industry criteria for daytime and night time conditions		
VaMS.REQ.006	Display Requirements	The VaMS unit shall have the provision to display online messages received from the command control centre for the duration specified by the user.		
VaMS.REQ.007	Display Requirements	The minimum vertical clearance between the finished road surface and the bottom of the support structure/bottom of the VaMS (whichever is lower) shall be <b>6.5m</b> .		
VaMS.REQ.008	Required Size for Surveillance	2.88 mtrs x 0.96 mtrs		



Variable Message Sign Board – VaMS				
Sr. No.	Item	Minimum Requirement Description	Compliance (Yes / No)	Deviations / Remarks
VaMS.REQ.009	Required Size for Smart strip	1.92 mtrs x 0.96 mtrs		
VaMS.REQ.010	Refresh Rate	Minimum 800 Hz		
VaMS.REQ.011	Temp Range	0 to +40 Degrees		
VaMS.REQ.012	Native Brightness	Minimum 5000 NITs		
VaMS.REQ.013	Contrast Ratio	Minimum 1200:1		
VaMS.REQ.014	Pixel Requirements	The pixel pitch shall be not more than 16 mm.		
VaMS.REQ.015	Pixel Density	Minimum 3096 pixel / sq mtr		
VaMS.REQ.016	LED Configuration	R/G/B 3 in 1 SMD		
VaMS.REQ.017	Power Input	100 ~ 240 VAC ,		
VaMS.REQ.018	Max Power Consumption	≤ 1000 W/Tile		
VaMS.REQ.019	Dimming Capabilities	Minimum 64 Levels		
VaMS.REQ.020	Humidity	10% ~ 90%		

<b>Variable Message Sign Board – VaMS</b>				
<b>Sr. No.</b>	<b>Item</b>	<b>Minimum Requirement Description</b>	<b>Compliance (Yes / No)</b>	<b>Deviations / Remarks</b>
VaMS.REQ.021	IP Level	IP65 Front IP54 Rear		
VaMS.REQ.022	Image Processor for Each LED Wall Display	Signal Input – DVI; Signal Output - RJ - 45		
VaMS.REQ.023	Communication	The communication protocols supported shall be TCP/IP, RS 232		
VaMS.REQ.024	Communication	The signboard unit shall be able to communicate with the central command centre computer using GSM data channel (GPRS) / Ethernet will be used to send online messages.		
VaMS.REQ.025	Communication	GPRS/ Ethernet port shall also be extended to ground level using necessary cables for local trouble shooting.		
VaMS.REQ.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.REQ.027	Communication	The VMS shall have self-test diagnostics features to test the VMS for correct operation during power on.		
VaMS.REQ.028	Display Protection	The front of VMS display board should be weather resistant IP 65 rated w.r.t various climatic conditions		
VaMS.REQ.029	Power Requirements	230V AC + 15%, 50 Hz single phase power supply (Automatically re-start in the event of an electricity failure)		
VaMS.REQ.030	Power Requirements	The equipment components shall have adequate surge and lightning protection.		

Variable Message Sign Board – VaMS				
Sr. No.	Item	Minimum Requirement Description	Compliance (Yes / No)	Deviations / Remarks
VaMS.REQ.031	Power Requirements	Necessary earthing for electrical and lightning protection to be provisioned as per the industry standards		
VaMS.REQ.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.REQ.033	Power Requirements	The enclosure for the inverter and battery should be pole mountable with IP65 protected housing and shall be lockable.		
VaMS.REQ.034	Components Requirement	Should include all related components. These components include the SNMP Manageable VMS controller with 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 and back-up batteries), communication ports, cable termination, enclosure and mounting accessories.		
VaMS.REQ.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.REQ.036	Power Distribution	Suitable Power Distribution Board to be provided for individual LED Wall		

<b>Support Structure for Variable Message Signboards</b>				
<b>Sr. No.</b>	<b>Item</b>	<b>Minimum Requirement Description</b>	<b>Compliance (Yes / No)</b>	<b>Deviations / Remarks</b>
SSVMS.REQ.001	General Requirement	The support structure for the VaMS shall be of MS IS: 2062 Gantry type		
SSVMS.REQ.002	General Requirement	The structure should be supported on the ground (shoulder/foot-path) on both the sides of the road through appropriate concrete foundation.		
SSVMS.REQ.003	General Requirement	The 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 NHAI guidelines		
SSVMS.REQ.004	General Requirement	The 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.REQ.005	Load Requirement	The structure for display board mounting should withstand wind-speeds upto <b>150km/hr</b> and support the weight of at least two VMS along with structure's self-weight. This should be certified by a structure engineer		
SSVMS.REQ.006	Load Requirement	The display board should be secured sufficiently with fasteners and fixtures to the support structure to withstand the mentioned loads.		
SSVMS.REQ.007	Painting	The 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.REQ.008	General Requirement	The 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.REQ.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.		

Public Address System				
Sr. No.	Item	Minimum Requirement Description	Compliance (Yes / No)	Deviations / Remarks
PAS.REQ.001	General Requirements	The system should allow streaming in both local network and internet and operable from Central command centre. System should have the capability to control individual PAS i.e. to make an announcement at select location (1:1) and all location (1: many) simultaneously. The PAS should also support both, Live and Recorded inputs		
PAS.REQ.002		Unlimited number of both sources and incomers of stream in the system		
PAS.REQ.003		Division of the speakers into independently controlled groups, Minimum 2 Speaker, to be used for public address system.		
PAS.REQ.004		Possibility to setup an independent operating		
PAS.REQ.005		Audio playback from a file or an external source		
PAS.REQ.006		Audio streams mixing - playlist creation support		
PAS.REQ.007	Net Speaker	IP and PC based solution – easy to use and maintain		
PAS.REQ.008		Easy to deploy and use		
PAS.REQ.009		Event scheduling		
PAS.REQ.010		Integrated 14W amplifier		
PAS.REQ.011		Remote configuration and administration		
PAS.REQ.012		External interface		
PAS.REQ.013		POE or 12V power		
PAS.REQ.014		10/100Base-TX Ethernet		
PAS.REQ.015		The output of the amplifier		
PAS.REQ.016		The output of Line out/ Headphones		
PAS.REQ.017		2 user buttons		
PAS.REQ.018		The sensor for remote control		

<b>Public Address System</b>				
<b>Sr. No.</b>	<b>Item</b>	<b>Minimum Requirement Description</b>	<b>Compliance (Yes / No)</b>	<b>Deviations / Remarks</b>
PAS.REQ.019		The slot for Micro SD card		
PAS.REQ.020		1x digital input and output		
PAS.REQ.021	Support	The system should not be an end of life / end of service product.		
PAS.REQ.022	Operating Conditions	0 to 50 Centigrade		

<b>Pole for Cameras</b>				
<b>Sr. No.</b>	<b>Item</b>	<b>Minimum Requirement Description</b>	<b>Compliance (Yes / No)</b>	<b>Deviations / Remarks</b>
POLE.REQ.001	General Requirement	Shall be minimum 20ft (6.5mts) height as per NHAH norms		
POLE.REQ.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 50m/sec with suitable arm bracket and with J type foundation bolts . Fabrication in accordance with IS 2713 (1980)		
POLE.REQ.003	Foundation	The pole would be fixed on an adequate and strong foundation so as to withstand city weather conditions and wind speed of 150km / hr		
POLE.REQ.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 100cms or better		
POLE.REQ.005	Protection	Lighting arrestors with proper grounding		
POLE.REQ.006	Sign Board with number plate	Sign board depicting the area under surveillance and with the serial number of the pole		
POLE.REQ.007	Height	The height of the pole shall be as per requirement of the location varying from 6.Mts to 12/15 Mts.		

Storage Server				
Sr. No.	Item	Minimum Requirement Description	Compliance (Yes / No)	Deviations / Remarks
STGVR.REQ.001	Architecture	Vendor may propose external SAN / NAS / VSA to store Video. Total Usable storage capacity should be 6 PB at Raid 5 => Bit Rate minimum 4Mbps => Minimum 25 FPS => Storage duration 15 days for 24Hrs continuous recording		
STGVR.REQ.002	Architecture	Should provide Minimum dual Controllers / nodes		
STGVR.REQ.003	Memory	Each node/controller node should provide 48 GB or more memory / cache.		
STGVR.REQ.004	Scalability	Controller / nodes should be upgradeable without having to change the entire chassis		
STGVR.REQ.005	Storage	Should support RAID 0, 1, 5, 6 raid Levels. Should configure for minimum double disk failure and with one hotspare in each storage node.		
STGVR.REQ.006	Storage	Should support hot swappable drives so that individual drives can be replaced without impacting any other drives		
STGVR.REQ.007	Storage	Should use 4 TB or less capacity SAS/NL-SAS 7.2K RPM drives.		
STGVR.REQ.008	Storage	Support onboard Flash Based Write Cache of minimum 4 GB		
STGVR.REQ.009	Interface Requirements	Minimum 2*10GBps per controller/node.		
STGVR.REQ.010	Redundancy	Should have redundant power supply and fans		



<b>Video Management System – VMS</b>				
<b>Sr. No.</b>	<b>Item</b>	<b>Minimum Requirement Description</b>	<b>Compliance (Yes / No)</b>	<b>Deviations / Remarks</b>
VMS.REQ.001	General Requirements	VMS shall work on ONVIF Open Platform catering to all the security needs of the city		
VMS.REQ.002	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.REQ.003	General Requirements	VMS shall support interoperability of IP cameras from multiple suppliers / vendors		
VMS.REQ.004	General Requirements	Bidders shall clearly mention in their proposal the brands and models integrated into VMS		
VMS.REQ.005	General Requirements	The VMS system shall be compatible to single and multiple processor servers. The server processor & hardware shall be optimized in all cases.		
VMS.REQ.006	General Requirements	The 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.REQ.007	General Requirements	The system shall allow the frame rate, bit rate and resolution of each camera to be configured independently for recording.		
VMS.REQ.008	General Requirements	The system shall support H.264 and MJPEG compression formats for all IP cameras connected to the system.		
VMS.REQ.009	General Requirements	The Video Management System shall support high availability of recording servers. A failover option shall provide standby support for recording servers with automatic synchronization to ensure maximum uptime and minimum risk of lost data.		
VMS.REQ.010	General Requirements	The Video Management System software shall have multicast and multi-streaming support. It shall definitely have the ability to take a snapshot from any online live camera and export to a standard graphic file format.		

<b>Video Management System – VMS</b>				
<b>Sr. No.</b>	<b>Item</b>	<b>Minimum Requirement Description</b>	<b>Compliance (Yes / No)</b>	<b>Deviations / Remarks</b>
VMS.REQ.011	General Requirements	The Video Management System 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.REQ.012	General Requirements	The 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.REQ.013	General Requirements	The System should support Maps integration with below features; i. Adding Image Layers to the location map ii. Define the location map for each location iii. Add cameras to the map images iv. Add image layers to the map v. Add a Maps Server vi. System should support raster format images of jpeg/jpg and png file and Vector (shape files)		
VMS.REQ.014	General Requirements	The 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.REQ.015	General Requirements	VMS shall be ONVIF compatible		
VMS.REQ.016	General Requirements	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.REQ.017	General Requirements	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.REQ.018	General Requirements	VMS shall be open to any standard storage technologies integration.		

<b>Video Management System – VMS</b>				
<b>Sr. No.</b>	<b>Item</b>	<b>Minimum Requirement Description</b>	<b>Compliance (Yes / No)</b>	<b>Deviations / Remarks</b>
VMS.REQ.019	General Requirements	VMS shall already support Storage system from multiple vendors.		
VMS.REQ.020	General Requirements	VMS shall provide the ability to save any event that was tagged as an alarm (video motion detection, video loss or input) received, to be saved in a manner in which it cannot be overwritten.		
VMS.REQ.021	General Requirements	VMS shall be open to any video wall system integration		
VMS.REQ.022	General Requirements	VMS shall offer the possibility to integrate external Video Analytics systems.		
VMS.REQ.023	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.REQ.024	Distributed Architecture	VMS shall be designed to offer a full IP based distributed architecture		
VMS.REQ.025	Distributed Architecture	VMS shall have the capability to handle software clients (operators) connected in different locations on the same network.		
VMS.REQ.026	Distributed Architecture	Simultaneous quantity of operators per location shall not be limited		
VMS.REQ.027	Management	VMS shall store the system's configuration in a relational database, either on the management server computer or on the network.		
VMS.REQ.028	Management	VMS shall authenticate user access, user rights and privileges of all operators through Active Directory		
VMS.REQ.029	Management	Access rights and privileges shall consist in but not limited to a. Visibility of devices, live view, playback, <b>AVI/ ASF/ MP4</b> export, JPEG export, database export, sequences, smart search, input status, output control. b. PTZ control, PTZ priority, PTZ preset control		

<b>Video Management System – VMS</b>				
<b>Sr. No.</b>	<b>Item</b>	<b>Minimum Requirement Description</b>	<b>Compliance (Yes / No)</b>	<b>Deviations / Remarks</b>
		<ul style="list-style-type: none"> <li>c. Smart/Remote Client, live playback/setup, status API, service registration API and</li> <li>d. Privileges for the map feature</li> </ul>		
VMS.REQ.030	Management	Registration of the system shall allow for on line activation and off line activation of licenses		
VMS.REQ.031	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. 5 servers that shall take over in the event that one of a group of designated Recording Servers fails. Recordings shall be synchronized back to the original Recording Server once it is back online		
VMS.REQ.032	Management	VMS shall operate in multicast / unicast / bandwidth throttling protocol to minimize the network bandwidth		
VMS.REQ.033	Multicasting	VMS shall support video streams up to at least 25fps		
VMS.REQ.034	Multicasting	Monitoring module shall allow for continuous monitoring of the operational status and event-triggered alarms from servers, cameras and other devices.		
VMS.REQ.035	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.REQ.036	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.REQ.037	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.REQ.038	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 64 cameras from multiple servers at a time.		

<b>Video Management System – VMS</b>				
<b>Sr. No.</b>	<b>Item</b>	<b>Minimum Requirement Description</b>	<b>Compliance (Yes / No)</b>	<b>Deviations / Remarks</b>
VMS.REQ.039	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.REQ.040	VMS Storage	It shall be possible to schedule recording on per camera basis (Continuous, manual or motion based)		
VMS.REQ.041	VMS Storage	VMS shall allow the control of the amount of used disk space.		
VMS.REQ.042	VMS Storage	It shall be possible to protect specific video streams against any deletion and for any period of time		
VMS.REQ.043	Log Management	The system log shall be searchable by Level, Source and Event Type.		
VMS.REQ.044	Log Management	The Alert Log records alerts triggered by rules (searchable by Alert type, Source and Event type)		
VMS.REQ.045	Management	The 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.REQ.046	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.REQ.047	Management	System should support thumbnail search, Thumbnail Search to quickly locate specific scenes or events in recorded video without fast-forwarding or rewinding. Thumbnail Search should display a range of video as thumbnail images, should allow to identify a portion of the recording to review.		
VMS.REQ.048	Management	System should support Clip Management—Use Clip Management to view, download and delete clips. that are stored on the server.		
VMS.REQ.049	Management	No of operators shall not be software licenses dependant. In case of emergency situation, threats, natural catastrophe the control room shall be able to reconfigure the VMS by adding more operators without any Contractor's intervention.		
VMS.REQ.050	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		

<b>Video Management System – VMS</b>				
<b>Sr. No.</b>	<b>Item</b>	<b>Minimum Requirement Description</b>	<b>Compliance (Yes / No)</b>	<b>Deviations / Remarks</b>
		authorised personnel have access to critical information, prevent man-in-the-middle attacks, and that the data is kept private.		

<b>Video Content Analytics Requirement</b>				
<b>Sr. No.</b>	<b>Item</b>	<b>Minimum Requirement Description</b>	<b>Compliance (Yes / No)</b>	<b>Deviations / Remarks</b>
VAS.REQ.001	General Requirements	The System shall be a real-time video analytics engine that utilizes advanced image processing algorithms to turn video into actionable intelligence.		
VAS.REQ.002	General Requirements	The 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.REQ.003	General Requirements	The system shall facilitate creating multiple zones and lines in a single scene to trigger various alerts		
VAS.REQ.004	General Requirements	The system shall allow the configuration of applicable rules and manage them.		
VAS.REQ.005	General Requirements	The system shall also enable editing the Zones and lines to the desired shape or size.		
VAS.REQ.006	General Requirements	The 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.REQ.007	General Requirements	The system shall enable masking of areas which interfere detection zones in other areas of the scene		
VAS.REQ.008	General Requirements	The system shall enable detecting rules in the defined areas (zones/ lines)		
VAS.REQ.009	General Requirements	The system shall provide a functionality for configuring timelines for various events such as abandoned object, camera tampering etc		
VAS.REQ.010	General Requirements	The system shall be able to filter large amounts of video and focus on human attention appropriately		

<b>Video Content Analytics Requirement</b>				
<b>Sr. No.</b>	<b>Item</b>	<b>Minimum Requirement Description</b>	<b>Compliance (Yes / No)</b>	<b>Deviations / Remarks</b>
VAS.REQ.011	General Requirements	The system shall allow classification of different objects like animals, vehicles, people etc.,		
VAS.REQ.012	General Requirements	The System shall have Automated PTZ camera control for zooming in on interesting events like motion Detection etc. as picked up by Camera without the need for human intervention.		
VAS.REQ.013	General Requirements	VCA shall provide secured feeds with encryption, watermarking for data authenticity		
VAS.REQ.014	General Requirements	VCA shall be able to trigger alerts for the vehicle direction, vehicle speed, vehicle parked in defined zones etc.,		
VAS.REQ.015	General Requirements	The system shall have a reporting generation functionality to provide inputs on various instances of events triggered in the system		
VAS.REQ.016	General Requirements	VAS should allow to add, edit, delete or disable and enable Policies.		
VAS.REQ.017	Features	The definable and available triggers should be for;		
		The city wide surveillance system needs to have the capability to deploy intelligent video analytics software on any of selected cameras. This software should have the capability to provide various alarms & triggers. The solution should offer following triggers from Day1:		
		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. Traffic flow/Congestion		
8. Traffic Volume estimation and statistical counts				



<b>Video Content Analytics Requirement</b>				
<b>Sr. No.</b>	<b>Item</b>	<b>Minimum Requirement Description</b>	<b>Compliance (Yes / No)</b>	<b>Deviations / Remarks</b>
		9. People tracking		
VAS.REQ.018	General Requirements	Motion Detection component that automatically detects moving objects in the field of view of a camera, and is capable of filtering out movement in configurable directions and movement due to camera motion (e.g. from wind)		
VAS.REQ.019	General Requirements	System shall have a sophisticated rule-based engine with powerful analytics capabilities that provides automatic event notification,		
VAS.REQ.020	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.		

<b>Automatic Number Plate Recognition (ANPR)</b>				
<b>Sr. No.</b>	<b>Item</b>	<b>Minimum Requirement Description</b>	<b>Compliance (Yes / No)</b>	<b>Deviations / Remarks</b>
ANPR.REQ.001	General Requirements	Cameras shall cover single lanes of 3.5m each. For places where more than two lanes is to be monitored, the lane cameras to be increased in proportion to the lane		
ANPR.REQ.002	General Requirements	The 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.REQ.003	General Requirements	The system should have the facility to provide the live feed of the camera at the central command centre or as per user requirement.		
ANPR.REQ.004	General Requirements	The system should be able to provide video clips of the transaction from the ANPR lane cameras as evidence		
ANPR.REQ.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.REQ.006	General Requirements	The system should perform ANPR on all the vehicles passing the site and send alert to the central command centre on detection of any Hot-listed vehicles (whose numbers have been marked as Stolen, Wanted, etc. at the Central server).		
ANPR.REQ.007	General Requirements	With the detected number plate text, picture should also be sent of hot listed vehicle. It is highly likely to misread similar alphabets like 7/1/L or 8/B		
ANPR.REQ.008	General Requirements	The system should work 24 x 7 in both day and night conditions with good accuracy for the duration of the project		
ANPR.REQ.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.REQ.010	General Requirements	The system should have ANPR/ OCR to address the Alpha numerical character of irregular font sizes.		

<b>Automatic Number Plate Recognition (ANPR)</b>				
<b>Sr. No.</b>	<b>Item</b>	<b>Minimum Requirement Description</b>	<b>Compliance (Yes / No)</b>	<b>Deviations / Remarks</b>
ANPR.REQ.011	General Requirements	The system should capture standard vehicle's number plates with an accuracy of at least 70% at day time and at least with an accuracy of 60% at night time. (On basis of number of vehicles)		
ANPR.REQ.012	General Requirements	The 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.REQ.013	General Requirements	Bidder to provide system with local processing unit at site and send only processed data		
ANPR.REQ.014	General Requirements	Local processing unit should be industrial grade type. capable of working up to 70°		
ANPR.REQ.015	Vehicle detection by Colour	The system shall have options to search historical records for post event analysis by the vehicle colour or the vehicle colour with license plate and date time combinations		
ANPR.REQ.016	Alert Generation	The system should have option to input certain license plates according to the hot listed categories like "Wanted", "Suspicious", "Stolen", etc. by authorized personnel.		
ANPR.REQ.017	Alert Generation	The 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.REQ.018	Logs	The system shall enable easy and quick retrieval of snapshots, video and other data for post incident analysis and investigations.		
ANPR.REQ.019	Logs	The 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.		

<b>Automatic Number Plate Recognition (ANPR)</b>				
<b>Sr. No.</b>	<b>Item</b>	<b>Minimum Requirement Description</b>	<b>Compliance (Yes / No)</b>	<b>Deviations / Remarks</b>
ANPR.REQ.020	Logs	The 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.		
ANPR.REQ.021	Logs	The system shall have option to save custom reports for subsequent use. The system shall have option to export report being viewed to common format for use outside of the ANPRS or exporting into other systems.		

<b>Red Light Violation Detection (RLVD)</b>				
<b>Sr. No.</b>	<b>Item</b>	<b>Minimum Requirement Description</b>	<b>Compliance (Yes / No)</b>	<b>Deviations / Remarks</b>
RLVD REQ.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 REQ.002	General Requirements	The system should have the facility to provide the live feed of the camera at the central command centre as per user requirement.		
RLVD REQ.003	General Requirements	The system should generate Alarms at control room software if any signal is found not turning RED within a specific duration of time.		
RLVD REQ.004	General Requirements	The system should be able to provide video clips of the transaction from the overview and lane cameras as evidence		
RLVD REQ.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, phase of light(red, amber), time since phase change (red, amber).		
RLVD REQ.006	General Requirements	The system should not use signal from traffic controller but use sensors instead. Should work without any lane based intuitive sensors like loops, piezo etc.		

<b>Red Light Violation Detection (RLVD)</b>				
<b>Sr. No.</b>	<b>Item</b>	<b>Minimum Requirement Description</b>	<b>Compliance (Yes / No)</b>	<b>Deviations / Remarks</b>
RLVD REQ.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 REQ.008	General Requirements	ANPR provided with RLVD should be capable of also searching for hot listed vehicles during green light. Accuracy of 70% in Day and 60% in Night.		
RLVD REQ.009	General Requirements	Local processing unit should be industrial grade type (700 C)		
RLVD REQ.010	General Requirements	The local sites 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 REQ.011	General Requirements	The system should provide facility to search for the cases of violations occurred during any specific span of time, and provide a statistical analysis of the number of such incidences occurring during various days of the month, various months of the year in graphical forms. A report of all such incidences should be available and transferable in hard copy during any selected span of time.		
RLVD REQ.012	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) in form of Video popup		

<b>Face Recognition System</b>				
<b>Sr. No.</b>	<b>Item</b>	<b>Minimum Requirement Description</b>	<b>Compliance (Yes / No)</b>	<b>Deviations / Remarks</b>
FR.REQ.001	General Requirements	The facial recognition system should be able to integrate with IP Video Cameras as required in the solution and shall be able to identify multiple persons of interest in real-time, through leading-edge face recognition technology. The system shall be able to recognize subjects appearing simultaneously in multiple live video streams retrieved from IP surveillance cameras. The Facial recognition system should seamlessly be integrated to the network video recorders and the video management system.		
FR.REQ.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		
FR.REQ.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.		
FR.REQ.004	General Requirements	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.		
FR.REQ.005	General Requirements	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.		
FR.REQ.006	General Requirements	The algorithm for facial recognition or the forensic tool should be able to recognise partial faces with varying angles		
FR.REQ.007	General Requirements	The system should be able to detect multiple faces from live single video feed		
FR.REQ.008	General Requirements	The system should have combination of eye-zone extraction and facial recognition		
FR.REQ.009	General Requirements	The system should have short processing time and high recognition rate		

<b>Face Recognition System</b>				
<b>Sr. No.</b>	<b>Item</b>	<b>Minimum Requirement Description</b>	<b>Compliance (Yes / No)</b>	<b>Deviations / Remarks</b>
FR.REQ.010	General Requirements	The system should be able to recognize faces regardless of vantage point and any facial accessories/ hair (glasses, beard, expressions)		
FR.REQ.011	General Requirements	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.		
FR.REQ.012	General Requirements	The system should be able to identify and authenticate based on individual facial features		
FR.REQ.013	General Requirements	The system should be compatible with the video management system being proposed by the system integrator		
FR.REQ.014	General Requirements	The system should have capability for 1:1 verification and 1:N identification matching		
FR.REQ.015	General Requirements	The system should be able to integrate with other systems in the future such as 'Automatic fingerprint identification system (AFIS)' etc.		
FR.REQ.016	General Requirements	The system should be able to support diverse industry standard graphic and video formats as well as live cameras		
FR.REQ.017	General Requirements	The system should be able to match faces from recorded media.		
FR.REQ.018	General Requirements	The system should be able to detect a face from a group photo		
FR.REQ.019	General Requirements	The system should be able to detect a face from stored videos of any format		
FR.REQ.020	General Requirements	The system should have bulk process of adding faces in the system		
FR.REQ.021	General Requirements	The system should be an independent system, with capability to integrate with industry standard Video Management Systems (VMS) for alert viewing.		
FR.REQ.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		

<b>Face Recognition System</b>				
<b>Sr. No.</b>	<b>Item</b>	<b>Minimum Requirement Description</b>	<b>Compliance (Yes / No)</b>	<b>Deviations / Remarks</b>
		OS to capture a face on the field and get the matching result from the backend server.		
FR.REQ.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.		
FR.REQ.024	General Requirements	The system shall be able to detect faces in different environmental changes like rain, wind, fog and poor light.		
FR.REQ.025	General Requirements	The system should have the facility to categorize the images like "Remember this person" or "hit-list" or "wanted".		
FR.REQ.026	General Requirements	The OEM should have deployed the solution in India		



Drone				
Sr. No.	Item	Minimum Requirement Description	Compliance (Yes / No)	Deviations / Remarks
DRO.REQ.001	Performance Characteristics	The system shall have a minimum 60 minutes with either payload @ MSL		
DRO.REQ.002	Performance Characteristics	The system shall function in a range of minimum 5 km LOS (Line-of-sight)		
DRO.REQ.003	Performance Characteristics	The system shall have a maximum launch altitude of 2000m AMSL (Above Mean Sea Level) or more		
DRO.REQ.004	Performance Characteristics	The system shall have a maximum operating altitude of 500m AGL (Above Ground Level) or more		
DRO.REQ.005	Performance Characteristics	The system shall have the function in the temperature range of -10°C to +50°C		
DRO.REQ.006	Performance Characteristics	The system shall support IP53 rating or better		
DRO.REQ.007	Performance Characteristics	The system shall prevail under wind conditions of 16 knots or more		
DRO.REQ.008	Operational Characteristics	The system should be able to recognize faces regardless of vantage point and any facial accessories/ hair (glasses, beard, expressions)		
DRO.REQ.009	Operational Characteristics	System shall have Autonomous Vertical Take-Off & Landing (VTOL) launch & recovery mechanism		
DRO.REQ.010	Operational Characteristics	The system shall have a maximum space recovery of 25m x 25m open area		
DRO.REQ.012	Operational Characteristics	The system shall have following types of flight modes:		
		a) Fully autonomous from Take-off to Landing without using any R/C controller		
		b) Altitude Hold		
		c) Hover at a defined waypoint		
		d) Autonomous Waypoint Navigation (pre- defined as well as dynamically adjustable waypoints during flight)		
e) Remotely Piloted mode for video based navigation (RPV Mode)				
DRO.REQ.013	System Configuration	The system shall have following configurations:		

Drone				
Sr. No.	Item	Minimum Requirement Description	Compliance (Yes / No)	Deviations / Remarks
		a) One Daylight Payload		
		b) One Thermal Payload		
		c) One GCS with Communication System		
		d) One Field repair kit		
		e) One Set of Accessories		
		f) Waterproof Backpack		
		g) Ruggedized Carrying Case		
DRO.REQ.014	Video	a) Video shall be recorded in commonly portable video format (AVI/MP4 etc.) on the GCS.		
		b) Video of the full flight should be recorded by default with option to turn recording off		
		c) System should have the capability to take image snapshots with on-screen display parameters at any time during flight		
DRO.REQ.015	Maps	The system shall have:		
		a) The capability to download maps automatically after specifying location GPS co- ordinates		
		b) Integrate with any available maps		
		c) Integrate with geo-referenced raster maps provided in at least one of the commonly used digital map formats (gif, tiff etc.)		
DRO.REQ.016	User Controls	System shall have the following features:		
		a) One-click Take-off/Land/Hover		
		b) Set altitude of the UAV		
		c) Waypoint navigation		
		d) Dynamic flight plan adjustment		

Drone				
Sr. No.	Item	Minimum Requirement Description	Compliance (Yes / No)	Deviations / Remarks
		e) Point payload to ground co-ordinate function		
		f) Switch on/off Night Recovery Beacon		
DRO.REQ.017	Joystick Controls	System shall have full camera controls including:		
		a) Pan/Tilt		
		b) Zoom In/Out		
		c) Black/White Hot		
		d) RPV mode		
		e) Altitude control		
DRO.REQ.018	GUI Display parameters	System shall have a Geographic Map along with location, trajectory, camera view polygon, waypoints and flight plan.		
		Real-time video from the system with on-screen display of important parameters like its co-ordinates, target (payload) co-ordinates and range from the system, true North indication, Distance from HOME etc.		
		System shall display Real-time video at all times during the flight and the Artificial Horizon indicating UAV attitude		
DRO.REQ.019	UAV Weight	The system shall weigh < 3 Kg		
DRO.REQ.020	Technical Life of UAV	The system shall be certified for Minimum 500 landings (Test results to be submitted)		
DRO.REQ.021	Failsafe features	The system shall have following failsafe features built in:		
		Return to home on communication failure		
		Return to home on low battery		
		Multiple GPS on board for GPS failure redundancy		
DRO.REQ.022	Aural Signature	The aural signature of the system shall be Nil at slant range of 500 meters		
DRO.REQ.023	Camera Specifications	Daylight: Resolution: Minimum 1920 x 1080; 10x Optical Zoom		

Drone				
Sr. No.	Item	Minimum Requirement Description	Compliance (Yes / No)	Deviations / Remarks
		Night: Resolution: Minimum 320 x 240; 4x Digital Zoom; Modes: White Hot and Black Hot		
DRO.REQ.024	Payload freedom	Pan: 360 degrees continuous		
		Tilt: 90 degrees		
DRO.REQ.025	Stabilisation	Following stabilisation shall be employed in the system:		
		Gimbal stabilisation		
		Electronics stabilisation of video output at all zoom levels in real time		
DRO.REQ.026	Target Tracking	The system shall be capable of Real time vision based autonomous tracking of static and moving targets		
DRO.REQ.027	Video Link	The system shall have Digital and Encrypted video link with the ground control station		
DRO.REQ.028	Frequency Band	2.4 GHz uplink and down link; minimum 4 channels selectable		

<b>Server</b>				
<b>Sr. No.</b>	<b>Item</b>	<b>Minimum Requirement Description</b>	<b>Compliance (Yes / No)</b>	<b>Deviations / Remarks</b>
SEV.REQ.001	Processor	Latest Generation x86-64 Bit Minimum 2.20 GHz with min. 10 Core and 16MB Cache or more. Offered Server should be configured with at least 2 Processors		
SEV.REQ.002	Number of Processors	Offered Server should be configured with at least 2 Processors		
SEV.REQ.003	Memory	Should be configured with 8 GB Per core RAM. Memory should be scalable to double the capacity configured		
SEV.REQ.004	Internal HDD	Minimum 2* 600GB Internal SAS HDD Per Server		
SEV.REQ.005	DVD	Should support internally, externally or virtually on network		
SEV.REQ.006	Power Supplies	Redundant Hot-Swappable Power Supplies at chasis level		
SEV.REQ.007	Fans	Redundant Hot Swappable Fans		
SEV.REQ.008	OS & Virtualization Infrastructure Support	Should support MS Windows, Enterprise Linux and common hypervisors such as Oracle Virtualisation / VMWare & Microsoft HyperV		
SEV.REQ.009	Interface Port	Blade server should provide Ethernet and fibre channel connectivity OR Converged Network Adapters in lieu of the same		
SEV.REQ.010	RAID	RAID Controller should be able to do RAID 1, 0		
SEV.REQ.011	Warranty	Critical Components like CPU, Memory, SSD / HDD, Motherboard should be covered		
SEV.REQ.012	Power Supply Redundancy	The supporting chassis should have redundant power supply.		

<b>Server</b>				
<b>Sr. No.</b>	<b>Item</b>	<b>Minimum Requirement Description</b>	<b>Compliance (Yes / No)</b>	<b>Deviations / Remarks</b>
SEV.REQ.013	Keyboard and Mouse	Should support Remote KVM / Virtual KVM		
SEV.REQ.014	Redundancy	The Blade servers should be hot pluggable		
SEV.REQ.015	Connectivity	The uplink connectivity from the chassis should have up to 160 Gb bandwidth and 20 Gb per server blade		
SEV.REQ.016	Operating Temperature	Operating Temperature support from 10 to 35°C and Non-operating Temperature from 0 to 50°C		

<b>Blade Chassis</b>				
<b>Sr. No.</b>	<b>Item</b>	<b>Minimum Requirement Description</b>	<b>Compliance (Yes / No)</b>	<b>Deviations / Remarks</b>
BCH.REQ.001	Blade Chassis	Blade chassis shall be 19" standard Width rack mountable and provide appropriate rack mount kit.		
BCH.REQ.002	Blade Chassis	The power supply modules should be hot pluggable		
BCH.REQ.003	Blade Chassis (Redundancy)	The power subsystem should support all of the following modes of power redundancy ( No redundancy, N+1 , N+N or grid )		
BCH.REQ.004	Blade Chassis (Redundancy)	The power subsystem should be support N + N power redundancy for a fully populated chassis with the 2 socket (CPU) servers		
BCH.REQ.005	Blade Chassis (Redundancy)	Should be configured to provide full redundant cooling to all blade slots		
BCH.REQ.006	Fibre Channel Interconnects	The uplink from the chassis should support FCoE ( Fibre Channel over Ethernet ) technology		
BCH.REQ.007	Management	It should support remote KVM / virtual KVM capability for management and administration.		
BCH.REQ.008	Blade Chassis (DVD)	Should support virtual DVD and virtual floppy internally / externally		
BCH.REQ.009	Interface	The Fabric switches should support the direct connection to FCoE enabled storage arrays		
BCH.REQ.010	Management	Support a stateless environment where server identity is created by the administrator who defines the server		
BCH.REQ.011	Blade Chassis	Servers can be automatically assigned to the resource pools based on qualification criteria		
BCH.REQ.012	Management	Must support the ability to rollback firmware from current active versions to the previous version for the Server BIOS, Adapter firmware and bootcode versions , individual server management chips from the same console		

<b>Blade Chassis</b>				
<b>Sr. No.</b>	<b>Item</b>	<b>Minimum Requirement Description</b>	<b>Compliance (Yes / No)</b>	<b>Deviations / Remarks</b>
BCH.REQ.013	Management	Role Based Access Control so that the resources can be managed by respective resource administrator.		
BCH.REQ.014	Server Management	Movement of server identity from one slot to another in the event of server failure		
BCH.REQ.015	Power Management	Administrators have the flexibility to define power policies so that the power can be limited to a specific server		
BCH.REQ.016	Power Management	Administrators should be able to decide the threshold / cap on the maximum power that the chassis can draw .		
BCH.REQ.017	Server Management	Supports multiple level of authentication methods such as RADIUS / TACACs+ and LDAP		
BCH.REQ.018	Server Management	Movement of server identity from one slot to another in the event of server failure		
BCH.REQ.019	Support	The system should not be an end of life / end of service product.		



<b>DG Set for Command Control Centre</b>				
<b>Sr. No.</b>	<b>Item</b>	<b>Requirement Description</b>	<b>Compliance (Yes / No)</b>	<b>Deviations / Remarks</b>
DGS.REQ.001	General Specifications	Auto Starting DG Set Mounted on a common based frame with AVM (Anti-Vibration) pads, residential silencer with exhaust piping, complete conforming to ISO 8528 specifications and CPCB certified for emissions. KVA rating as per the requirement.		
DGS.REQ.002	Capacity	Minimum 250 KVA		
DGS.REQ.003	Fuel	High Speed Diesel (HSD) With 30 Ltr Tank Capacity or better. It should be sufficient and suitable for containing fuel for 12 hours continuous operation, Complete with level indicator, fuel inlet and outlet, air vent, drain plug, inlet arrangement for direct filling and set of fuel hoses for inlet and return.		
DGS.REQ.004	Power Factor	0.8		
DGS.REQ.005	Engine	Engine should support electric auto start, water cooled, multi cylinder, maximum 1500 rpm with electronic/manual governor and electrical starting arrangement complete with battery, 4 stroke multiple cylinders/single and diesel operated conforming to BS 5514/ ISO 3046/ IS 10002		
DGS.REQ.006	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.		

<b>DG Set for Command Control Centre</b>				
<b>Sr. No.</b>	<b>Item</b>	<b>Requirement Description</b>	<b>Compliance (Yes / No)</b>	<b>Deviations / Remarks</b>
DGS.REQ.007	AMF (Auto Main Failure) Panel	AMF Panel fitted inside the enclosure, with the following meters/indicators: <ul style="list-style-type: none"> <li>• Incoming and outgoing voltage</li> <li>• Current in all phases</li> <li>• Frequency</li> <li>• KVA and power factor</li> <li>• Time indication for hours/ minutes of operation</li> <li>• Fuel Level in field tank, low fuel indication</li> <li>• Emergency Stop button</li> <li>• Auto/Manual/Test selector switch</li> <li>• MCCB/Circuit breaker for short-circuit and overload protection</li> <li>• Control Fuses</li> <li>• Earth Terminal</li> <li>• Any other switch, instrument, relay etc essential for Automatic functioning of DG set with AMF panel</li> </ul>		
DGS.REQ.008	Acoustic Enclosure	<ul style="list-style-type: none"> <li>• The DG set shall be provided with acoustic enclosure / canopy to reduce the sound level and to house the entire DG set (Engine &amp; Alternator set) assembly outside (open-air).</li> <li>• The enclosure shall be weather resistant powder coated, with insulation designed to meet latest MOEF/CPCB norms for DG sets, capable to withstand Mumbai climate. The enclosure shall have ventilation system, doors for easy access for maintenance, secure locking arrangement, complete</li> </ul>		
DGS.REQ.009	Output Frequency	50 Hz		
DGS.REQ.010	Tolerance	+/- 5% as defined in BSS-649-1958		
DGS.REQ.011	Enclosure	Acoustic enclosure with provision for a fuel tank		
DGS.REQ.012	Indicators	Over speed /under speed/High water temperature/low lube oil etc.		
DGS.REQ.013	Intake system	Naturally Aspirated		
DGS.REQ.014	Certifications	ISO 9001/9002, relevant BS and IS standard.		

<b>Video Wall for Command Control Centre (DLP Based)</b>				
<b>Sr. No.</b>	<b>Item</b>	<b>Minimum Requirement Description</b>	<b>Compliance (Yes / No)</b>	<b>Deviations / Remarks</b>
VWCCC.REQ.001	General	Video Wall and Controller from the same make is preferred		
VWCCC.REQ.002	Video wall	50 Cubes ( LED Based projection) - 8X4 for Command Control Centre - 6X4 for City Operation Center		
VWCCC.REQ.003	Technology	Single chip DLP Technology		
VWCCC.REQ.004	Resolution	1920x1080		
VWCCC.REQ.005	Brightness	240 Cd/m <sup>2</sup> or better		
VWCCC.REQ.006	On-screen contrast	1,200,000:1 (dynamic) or better		
VWCCC.REQ.007	Display technology	DLP rear projection with DMD Chip		
VWCCC.REQ.008	Colour gamut	>15 mill		
VWCCC.REQ.009	Brightness uniformity	>90% or better		
VWCCC.REQ.010	Screen	180° viewing angle screen		
VWCCC.REQ.011	Screen Gap	Less than 1 mm at ambient temperature in Control room		
VWCCC.REQ.012	Colour stability	Self-calibration with advanced colour sensor		
VWCCC.REQ.013	Dimensions	Diagonal: 50 "		
VWCCC.REQ.014	Light source	LED - 6x redundancy		
VWCCC.REQ.015	Light source lifetime	> 60,000h Typical usage mode		
VWCCC.REQ.016		> 80,000h Economy usage mode		
VWCCC.REQ.017	Conditions for operation	10°C-40°C, 80% humidity (Non Condensing)		
VWCCC.REQ.018	Input voltage	90 – 240 V, 50-60Hz		
VWCCC.REQ.019	Signal input/output	Single I link DVI in / Singlelink DVI out		
VWCCC.REQ.020	Direct Ethernet access	IP control		

<b>Video Wall for Command Control Centre (DLP Based)</b>				
<b>Sr. No.</b>	<b>Item</b>	<b>Minimum Requirement Description</b>	<b>Compliance (Yes / No)</b>	<b>Deviations / Remarks</b>
VWCCC.REQ.021	Graphical user interface	All settings and operational parameters		
VWCCC.REQ.022	Third party interface	Should be open to third party interface		
VWCCC.REQ.023	Warranty	5 years		

<b>Video Wall Controller</b>				
<b>Sr. No.</b>	<b>Item</b>	<b>Minimum Requirement Description</b>	<b>Compliance (Yes / No)</b>	<b>Deviations / Remarks</b>
VWC.REQ.001	Operating System	Windows 7 64bit Ultimate Version		
VWC.REQ.002	CPU Processing	Intel® Core™ i7 Quad Core 3.0 GHz processor or better		
VWC.REQ.003	Memory	16 GB RAM		
VWC.REQ.004	Hard disk	2x 600 GB RAID-1, Hot-plug redundant		
VWC.REQ.005	Optical drive	DVD R/W		
VWC.REQ.006	Network	2x 1 Gb/s LAN		
VWC.REQ.007	System backplane	PCI express 3.0 backplane (min 10 slots)		
VWC.REQ.008	Graphics card	- Support for 4 Ch Graphic card with DVI outputs - Should support Display Port (max resolution: 2560x1600@60Hz) - 1920x1200@60 Hz (DVI)		
VWC.REQ.009	DVI Input	Supporting DVI, RGB Signals		
VWC.REQ.010	Dimensions	19" Rack mount		
VWC.REQ.011	Power Supply	100-240VAC, 50/60Hz, Hot-plug redundant		
VWC.REQ.012	Operating Conditions	0°C to 35°C or better		
VWC.REQ.013	Form Factor	3U 1/2 19" Rack mount housing		
VWC.REQ.014	Storage Temperature	0°C to 40°C		

<b>Video Wall Management Software</b>				
<b>Sr. No.</b>	<b>Nature of Requirement</b>	<b>Minimum Requirement Description</b>	<b>Compliance (Yes / No)</b>	<b>Deviations / Remarks</b>
WMS.REQ.001	General Requirements	The software should be able pre configure various display layouts and access them at any time with a simple mouse click or based on the timer		
WMS.REQ.002	General Requirements	The software should enable the users to see the desktop of the graphics display wall remotely on the any PC connected with the Display Controller over the Ethernet and change the size and position of the various windows being shown.		
WMS.REQ.003	General Requirements	The wall management software shall be having interoperability with Video management system.		
WMS.REQ.004	General Requirements	The wall management software may be centrally Server based or local controller based architecture.		
WMS.REQ.005	General Requirements	The 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.REQ.006	General Requirements	The software should copy the screen content of the PC / workstation 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.REQ.007	General Requirements	The wall management software should enable system integrators to integrate it with their Software.		
WMS.REQ.008	General Requirements	Key features of Wall management Software a. Central configuration database		
WMS.REQ.009	General Requirements	The 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		

<b>Video Wall Management Software</b>				
<b>Sr. No.</b>	<b>Nature of Requirement</b>	<b>Minimum Requirement Description</b>	<b>Compliance (Yes / No)</b>	<b>Deviations / Remarks</b>
WMS.REQ.010	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.REQ.012	General Requirements	Log file functions		

## Mobile Surveillance

UPS				
Sr. No.	Item	indicative Requirement Description	Compliance (Yes / No)	Deviations / Remarks
UPS.REQ.001	Capacity	3 KVA		
UPS.REQ.002	Technology	True ONLINE (Double Conversion) PWM technology using IGBTs for switching at high frequency (>15 KHz)		
UPS.REQ.003	Connector	SNMP Connectivity		
UPS.REQ.004	Electrical Input	Single Phase, 230 V AC with an option to select three phase		
UPS.REQ.005	Electrical Input	Voltage Range 155 – 280 V on Full Load Voltage Range 110 – 280 V on less than 70% Load		
UPS.REQ.006	Electrical Input	Frequency Range 45 – 55 Hz		
UPS.REQ.007	Electrical Input	Efficiency AC to AC: > 85% (AC to AC)		
UPS.REQ.008	Electrical Output	230V AC		
UPS.REQ.009	Electrical Output	Frequency: 50 Hz + 0.25Hz (free running); + 2Hz (sync mode)		
UPS.REQ.010	Electrical Output	Voltage Regulation: +1% on mains/batteries		
UPS.REQ.011	Electrical Output	Overload Capacity: 125% for 5 min., 110% for 10 mins.		
UPS.REQ.012	Electrical Output	Waveform; Pure Sine wave		
UPS.REQ.013	Protection	Electronic Overload Sensing and circuit breaker protection.		
UPS.REQ.014	Protection	Overheating, Output short circuit, low battery, input over/under voltage etc.		
UPS.REQ.015	Battery Type	Sealed Maintenance Free Battery, Mains & Battery with necessary indicators, alarms and protection with proper battery storage stand		
UPS.REQ.016	Backup Time	Minimum 2 hour backup on rated load		
UPS.REQ.017	DC Voltage	MIN. : 240 V		
UPS.REQ.018	Charging Features	Adjusted to about 10% of battery capacity for fast charging. 1. Boost/trickle charging facility		



UPS				
Sr. No.	Item	indicative Requirement Description	Compliance (Yes / No)	Deviations / Remarks
		2. Uncontrolled rectifier with high efficiency and reliability. 3. Low battery protection to avoid deep discharging of batteries. 4. Self-test diagnostic feature		
UPS.REQ.019	Other Features	UPS Bypass Automatic on Overload or UPS Failure		
UPS.REQ.020	Other Features	Monitoring panel with LCD display to provide following information:- 1. Input/output voltage 2. Input/output frequency 3. Load current 4. Charging current LED display for: - UPS on, battery operation, bypass, alarm battery charge level, etc. Alarms for :- Mains failure, low battery, overload etc.		
UPS.REQ.021	Other Features	RS 232 Standard Interface port in conjunction with UPS monitoring software provides information about UPS health, status, battery backup etc.		
UPS.REQ.022	Environmental	Temperature 0-40°C operating, 0 to + 60° C		
UPS.REQ.023	Environmental	Humidity 0 – 95% RH non-condensing		
UPS.REQ.024	Environmental	Audible noise < 50 dB (A)		
UPS.REQ.025	Mandatory Compliance	Safety certified to IEC standards or as per applicable in Indian law		
UPS.REQ.026	Mandatory Compliance	EMC certified to IEC standards.		
UPS.REQ.027	Mandatory Compliance	ISO 9001:2000 and ISO 14001 certified ETDC/ERTL test reports for above specifications.		
UPS.REQ.028	Mandatory Compliance	Dimension Light Weight/Smaller Footprint		

<b>Generator</b>				
<b>Sr. No.</b>	<b>Item</b>	<b>indicative Requirement Description</b>	<b>Compliance (Yes / No)</b>	<b>Deviations / Remarks</b>
GNT.REQ.001	General Specifications	Auto Starting Petrol Generator. Recoil & Electric starting system. Stopping system should be ignition primary circuit ground.\ KVA rating as per the requirement.		
GNT.REQ.002	Capacity	Minimum 3 KVA		
GNT.REQ.003	Fuel	Minimum 1.78 (litres / hr). 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.		
GNT.REQ.004	Fuel Tank Capacity (Litres)	13		
GNT.REQ.005	Power Factor	0.8		
GNT.REQ.006	Operating Noise Level	52 dB		
GNT.REQ.007	Maximum AC output	3000 VA		
GNT.REQ.008	DC output	12 A		
GNT.REQ.009	Generator Type	Multipole field rotation type (inverter)		
GNT.REQ.010	Rated Voltage	240 V		
GNT.REQ.011	Fuel gauge	Required		
GNT.REQ.012	Ac circuit breaker	Required		
GNT.REQ.013	Dc circuit breaker	Required		
GNT.REQ.014	Auto throttle	Required		
GNT.REQ.015	Large capacity air Cleaner	Required		
GNT.REQ.016	Air cleaner	Required		

RFP for Selection of System Integrator for Implementation of Nagpur Smart City Solutions

Generator				
Sr. No.	Item	indicative Requirement Description	Compliance (Yes / No)	Deviations / Remarks
GNT.REQ.017	Pilot lamp	Required		
GNT.REQ.018	Engine	Engine should support electric auto start, water cooled, multi cylinder, and maximum 3600 rpm with electronic/manual governor and electrical starting arrangement complete with battery.		
GNT.REQ.019	AMF (Auto Main Failure) Panel	AMF Panel fitted inside the enclosure, with the following: It should have the following meters/indicators <ul style="list-style-type: none"> <li>• Incoming and outgoing voltage</li> <li>• Current in all phases</li> <li>• Frequency</li> <li>• KVA and power factor</li> <li>• Time indication for hours/ minutes of operation</li> <li>• Fuel Level in fuel tank, low fuel indication</li> <li>• Emergency Stop button</li> <li>• Auto/Manual/Test selector switch</li> <li>• MCCB/Circuit breaker for short-circuit and overload protection</li> <li>• Control Fuses</li> <li>• Earth Terminal</li> </ul>		
GNT.REQ.020	Output Frequency	50 Hz		
GNT.REQ.021	Enclosure	Acoustic enclosure with provision for a fuel tank		
GNT.REQ.022	Indicators	Over speed /under speed/High water temperature/low lube oil etc.		
GNT.REQ.023	Intake system	Naturally Aspirated		
GNT.REQ.024	Certifications	ISO 9001/9002, relevant BS and IS standard.		

## 1.4 City Smart Kiosk

Kiosk				
Sr. No.	Item	indicative Requirement Description	Compliance (Yes / No)	Deviations / Remarks
KIO.REQ.001	Screen	<ul style="list-style-type: none"> <li>i. Minimum 15" LCD touch screen,</li> <li>ii. Shall support 1280x1024 Resolution or better,</li> <li>iii. Support for following features: Wide Viewing Angle, Low Power Consumption, High Contrast Ratio, High Aperture Ratio, Short Response Time;</li> <li>iv. Capacitive Touch Display,</li> <li>v. All-glass touch-screen with a transparent metallic conductive coating is preferred</li> </ul>		
KIO.REQ.002	Computing module	<ul style="list-style-type: none"> <li>i. Platform shall support leading operating systems</li> <li>ii. Processor speed minimum of 1.6 GHz Intel@/equivalent Processor or better</li> <li>iii. Min 2 GB RAM</li> <li>iv. Internal persistent storage capacity of minimum 20 GB</li> <li>v. Slots and support for connecting other components as required</li> </ul>		
KIO.REQ.003	Keyboard	<ul style="list-style-type: none"> <li>i. Alphanumeric keyboard with minimum of 50 keys</li> </ul> <p>* This may be replaced with an onscreen keyboard, depending on the design</p>		
KIO.REQ.004	Speakers	<ul style="list-style-type: none"> <li>i. Output: 20 Watts or better</li> <li>ii. Shall be able to deliver clear stereo sound</li> </ul>		
KIO.REQ.005	Microphone	<ul style="list-style-type: none"> <li>i. Shall support speech based interaction during video conferencing when enabled through kiosk</li> <li>ii. Shall be able to isolate the main sound source and minimize background noise, highlighting the performance</li> </ul>		
KIO.REQ.006	Open city card reader and writer	<ul style="list-style-type: none"> <li>i. Shall support of a EMV based open city card which shall be soon proposed for Nagpur city</li> <li>ii. Shall be capable of reading/writing / updating certain data within the card</li> </ul>		

RFP for Selection of System Integrator for Implementation of Nagpur Smart City Solutions

Kiosk				
Sr. No.	Item	indicative Requirement Description	Compliance (Yes / No)	Deviations / Remarks
		<i>It is understood that this component may not be made available in the initial set up, however, as and when open city card is made operations during course of contract, this functionality shall have to be enabled.</i>		
KIO.REQ.007	Credit / Debit card reader	<ul style="list-style-type: none"> <li>i. Shall accept all major credit / debit cards from major payment gateways including Visa, MasterCard, Rupay, American Express and others</li> <li>ii. Shall be capable of reading latest magnetic strip and chip-based cards</li> </ul>		
KIO.REQ.008	QR scanner	<ul style="list-style-type: none"> <li>i. Shall be able to read Quick Response Code from Mobile phones, tablets and paper prints</li> </ul>		
KIO.REQ.009	NFC based payments	<ul style="list-style-type: none"> <li>i. Shall be compliant with applicable ISO/IEC standards and also shall be able to accept payments from multiple vendors based on industry standards</li> </ul> <p><i>It is understood that this component may not be made available in the initial setup, however, as and when NFC based payments are made available during course of contract, this functionality shall have to be enabled.</i></p>		
KIO.REQ.010	Currency acceptor	<ul style="list-style-type: none"> <li>i. Shall be able to read INR notes of various denominations including 10, 20, 50, 100, 500 &amp; 1000</li> <li>ii. Shall have capabilities to identify fake notes</li> <li>iii. Shall be able to dispense change as per mutually agreed terms</li> </ul>		
KIO.REQ.011	Printer	<ul style="list-style-type: none"> <li>i. Type: DMP / Thermal or suitable printing</li> <li>ii. Shall be able to print receipts, which may be preserved for a period of 12 months</li> <li>iii. Width: Type A 76mm or more</li> </ul>		
KIO.REQ.012	Physical form	<ul style="list-style-type: none"> <li>i. Kiosk body enclosed in a protective shell made of robust weather proof material</li> </ul>		
KIO.REQ.013	Security requirements	<ul style="list-style-type: none"> <li>i. Kiosk machine shall ensure that any data stored within or being transferred is encrypted as per industry standards. Machine shall ensure no data loss to the extent possible.</li> </ul>		

Kiosk				
Sr. No.	Item	indicative Requirement Description	Compliance (Yes / No)	Deviations / Remarks
		ii. Kiosk machine shall be equipped with sufficient tamper-proof mechanisms to ensure detection in case of physical tampering to the kiosk		
KIO.REQ.014	Other requirements	i. Kiosk shall be upgradable through a central system remotely over internet ii. It shall be possible to monitor critical parameters related to health of the kiosk device remotely iii. Kiosk shall be able to provide details related to inventory requirements to central system iv. Multilingual support: Shall necessarily offer support for multiple languages including English, Hindi and Marathi (min) v. Kiosk shall provide for custom branding complete with signage and digital displays vi. Kiosk shall work fine under following operating conditions: <ul style="list-style-type: none"> <li>• Temperature 0°-50°C</li> <li>• Humidity 10%~90% RH Ta&lt;40°C</li> <li>• Power: DC +12V, 100~240 V@ 60/50Hz</li> </ul>		

## 1.5 “Smart Strip”

GPS Device Unit				
Sr. No.	Category	Minimum Requirement Description	Compliance (Yes / No)	Deviations / Remarks
GPS.REQ.001	GPS Receiver	Minimum 16 channels		
GPS.REQ.002	GPS re-acquisition functionality	Cold start <= 42 Sec, Warm Start < 35 sec, Hot Start <= 2 Sec		
GPS.REQ.003	GPS Tracking Sensitivity	-165 dBmtyp		
GPS.REQ.004	GPS Velocity Accuracy	< 0.01 m/sec		
GPS.REQ.005	GPS Navigation Sensitivity	-148 dBmtyp		
GPS.REQ.006	GPS Navigation Update	1 Second		
GPS.REQ.007	GPS Data Format	Support WGS – 84		
GPS.REQ.008	GSM/GPRS Band	GSM/GPRS SMT quad band and UMTS (3G)		
GPS.REQ.009	GSM/GPRS Network Support	Support all GSM Network		
GPS.REQ.010	Data Acquisition and Transmission	Data packets shall have configurable fields - Unit ID, Latitude, Longitude, Speed, Time Stamp, Orientation, GPS fix, Alert Status.		
GPS.REQ.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.REQ.012	Data Acquisition and Transmission	Shall support GPS data storage upto 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.REQ.013	Data Acquisition and Transmission	Shall transmit data in SMS mode when GPRS is not available		

GPS Device Unit				
Sr. No.	Category	Minimum Requirement Description	Compliance (Yes / No)	Deviations / Remarks
GPS.REQ.014	Micro Controller Module support for Interface	16 bit RISC architecture based Micro Controller system for interface with various sub systems		
GPS.REQ.015	Antennas	Built -in GPS and GSM Antenna.		
GPS.REQ.016	Audio Interface	16 Watts Audio Amplifiers 4 Loud Speaker ( 4 Watts each)		
GPS.REQ.017	Power Supply	Power Supply input support 7 V to 32 V DC battery and shall be powered by vehicle battery and not ignition		
GPS.REQ.018	Internal Battery Back Up	6-8 hours backup		
GPS.REQ.019	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.REQ.019	Status LEDs	Power, GPS, GSM, VMU Status		
GPS.REQ.020	Alerts & Notifications	Shall be programmed to provide Alerts on power supply disconnect, speed violation, device tampering etc.		
GPS.REQ.021	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.REQ.022	Packaging & Accessories	Dimensions : 121mm (L) x 102mm (W) x 30mm (H) with power supply cable		
GPS.REQ.023	Rating	22 tracking / 66 acquisition minimum		
GPS.REQ.024	General Requirement	The GPS tracking device should have adequate intelligence and programability to run custom edge applications and analytics on the edge device.		
GPS.REQ.025	General Requirement	The GPS tracking device should have embeded storage and compute and should offer SDK/API for custom tools and application portability into the same.		





LED Display 2 Line				
Sr. No.	Category	Minimum Requirement Description	Compliance (Yes / No)	Deviations / Remarks
LED.2Line.REQ.001	Size	2 Line LED Display Front minimum 200x1800 mm Rear and side: minimum 200x900 mm Inner : minimum 100x800 mm		
LED.2Line.REQ.002	Pitch	13 mm (H) * 13 mm (V)		
LED.2Line.REQ.003	Colour	Amber coloured LED - Day Light Readable		
LED.2Line.REQ.004	Minimum & maximum viewing distance and angle of viewing	Viewing distance 5-30 meters Angle of viewing - Minimum 60°V – 110°H		
LED.2Line.REQ.005	Length of the message for a particular route; information that needs to be displayed in English & Marathi	Route No.: The vehicle route identity Destination STA, ETA		
LED.2Line.REQ.006	Vibration standard AIS 12/AIS:062 -10g	2g		
LED.2Line.REQ.007	Storage capacity inside the Display	20 Route Information		
LED.2Line.REQ.008	Communication protocol	GPRS		
LED.2Line.REQ.009	Controller and antenna	Inbuilt		
LED.2Line.REQ.010	Environmental specifications	(a) Temperature: 0 to +55 deg C (b) Thermal cycling: 5 deg C/mt (c) Humidity: 5% to 95% RH (d) Sealing: IP 65 (Front), IP 54 (Rear)		
LED.2Line.REQ.011	Minimum life	50,000 Hrs		
LED.2Line.REQ.012	Data format	Bitmap or Unicode		
LED.2Line.REQ.013	Power supply	90 V to 250 V AC; 50 VA		
LED.2Line.REQ.014	Frequency	5~50Hz and return to 5Hz at a linear sweep period of 1 minute/complete sweep Cycle		

LED Display 2 Line				
Sr. No.	Category	Minimum Requirement Description	Compliance (Yes / No)	Deviations / Remarks
LED.2Line.REQ.015	Excursion	1.6 mm peak to peak over the specified frequency range		
LED.2Line.REQ.016	Display Format	Multimedia content, text in Hindi, English and Marathi with presentation in tables, fixed and scrolling text		
LED.2Line.REQ.017	Structure	Front side and rear signs: light weight structure with toughened glass fixed with UV resistant adhesive in front Inner sign: light weight structure with poly glass /acrylic/toughened glass		
LED.2Line.REQ.018	Compliance	IS /IEC 60947-1:2004 in conjunction with IS/IEC 60529:2001		

LED Display 4 Line				
Sr. No.	Category	Minimum Requirement Description	Compliance (Yes / No)	Deviations / Remarks
LED.4Line.REQ.001	Size	4 Line LED Display - Minimum 400x3600 mm		
LED.4Line.REQ.002	Pitch	13 mm (H) * 13 mm (V)		
LED.4Line.REQ.003	Colour	Amber coloured LED - Day Light Readable		
LED.4Line.REQ.004	Minimum & maximum viewing distance and angle of viewing	Viewing distance 20-100 meters Angle of viewing - Minimum 60°V – 110°H		
LED.4Line.REQ.005	Length of the message for a particular route; information that needs to be displayed in English & Marathi	Route No.: The vehicle route identity Destination STA, ETA		
LED.4Line.REQ.006	Vibration standard AIS 12/AIS:062 -10g	2g		
LED.4Line.REQ.007	Storage capacity inside the Display	20 Route Information		
LED.4Line.REQ.008	Communication protocol	GPRS		
LED.4Line.REQ.009	Controller and antenna	Inbuilt		
LED.4Line.REQ.010	Environmental specifications	(a) Temperature: 0 to +55 deg C (b) Thermal cycling: 5 deg C/mt (c) Humidity: 5% to 95% RH (d) Sealing: IP 65 (Front), IP 54 (Rear)		
LED.4Line.REQ.011	Minimum life	50,000 Hrs		
LED.4Line.REQ.012	Data format	Bitmap or Unicode		
LED.4Line.REQ.013	Power supply	90 V to 250 V AC; 50 VA		
LED.4Line.REQ.014	Frequency	5~50Hz and return to 5Hz at a linear sweep period of 1 minute/complete sweep Cycle		

LED Display 4 Line				
Sr. No.	Category	Minimum Requirement Description	Compliance (Yes / No)	Deviations / Remarks
LED.4Line.REQ.015	Excursion	1.6 mm peak to peak over the specified frequency range		
LED.4Line.REQ.016	Update of Information	Real time (configurable refresh rate)		
LED.4Line.REQ.017	Display Format	Multimedia content, text in Hindi, English and Marathi with presentation in tables, fixed and scrolling text		
LED.4Line.REQ.018	Structure	Light weight structure with toughened glass fixed with UV resistant adhesive in front		
LED.4Line.REQ.019	Compliance	IS /IEC 60947-1:2004 in conjunction with IS/IEC 60529:2001		

RFID Reader				
Sr. No.	Category	Minimum Requirement Description	Compliance (Yes / No)	Deviations / Remarks
RFIDR.REQ.001	Protocol	ISO18000-6C EPC GEN2		
RFIDR.REQ.002	Configuration	Shall support Over The Air (OTA) firmware upgrade Shall be configurable for mixed or single tag-type operation		
RFIDR.REQ.003	Frequency Range	Standard ISM 902 928MHz or 915 MHz (US FCC), 865 MHz (ETSI 302-208), and 869 MHz (ETSI 300-220)		
RFIDR.REQ.004	Operation Mode	FHSS		
RFIDR.REQ.005	RF Power	0~30dBm, software adjustable		
RFIDR.REQ.006	Reading Speed	Software Programmable Average Reading per 64Bits <6ms		
RFIDR.REQ.007	Reading Mode	Timing or Touch, Software Programmable (reading shall be such that the reader does reads two tags at a time)		
RFIDR.REQ.008	Communication Mode with central server	TCP/IP and GPRS/GSM/2G or higher		
RFIDR.REQ.009	Data Input Port	Trigger input one time		
RFIDR.REQ.010	Reading Range	Max 12 m (able to calibrate)		
RFIDR.REQ.011	Communication Interface	RS232		
RFIDR.REQ.012	Accessories	Vehicle-mount DC power cable kit Antennas, and antenna cables		
RFIDR.REQ.013	Environmental Rating	IP68		
RFIDR.REQ.014	Humidity	10% to 90%		
RFIDR.REQ.015	Shock and Vibration Protection	Withstands standard material handling vehicle environments. Meets or exceeds MIL STD 810F		
RFIDR.REQ.016	Operating Temperature:	0°C to 55°C		
RFIDR.REQ.017	Storage Temperature:	0°C to 65°C		
RFIDR.REQ.018	Power Supply	Vehicle DC power 12 to 60V, 4.5 A maximum		

RFID TAG				
Sr. No.	Category	Minimum Requirement Description	Compliance (Yes / No)	Deviations / Remarks
RFIDTAG.REQ.001	Type	ABS, High Quality Engineering Plastic		
RFIDTAG.REQ.002	Supported Transponders	ISO18000-6C EPC Class 1 GEN2		
RFIDTAG.REQ.003	Frequency Range	ISM 865~928 MHz		
RFIDTAG.REQ.004	Operation Mode	Fixed Frequency or FHSS Software Programmable		
RFIDTAG.REQ.005	Memory capacity	The 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.REQ.006	Reading Rate	Software Programmable, Average Reading per 64 Bits < 10ms		
RFIDTAG.REQ.007	Tags material	Metal material		
RFIDTAG.REQ.008	Reading Range	Shall be able to be calibrated (to be kept as 4 - 6 m max) based on the site visit		
RFIDTAG.REQ.009	Operation Temp	0°C to 60°C		
RFIDTAG.REQ.010	IP Classification	IP 68		
RFIDTAG.REQ.011	Weather	Heat, dust proof, UV resistant & sea water resistant		
RFIDTAG.REQ.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		

<b>Bin Weight &amp; Volume Sensor System</b>				
<b>Sr. No.</b>	<b>Category</b>	<b>Minimum Requirement Description</b>	<b>Compliance (Yes / No)</b>	<b>Deviations / Remarks</b>
WGHTSEN.REQ.001	Weight Sensor	Load Cell based weight & volume sensor		
WGHTSEN.REQ.002	Functional Specification	When the bin weight & volume reaches to the threshold value, alert/sms shall be sent to the concerned person through suitable medium		



<b>Mobile Device (Smart Phone)</b>				
<b>Sr. No.</b>	<b>Item</b>	<b>Minimum Requirement Description</b>	<b>Compliance (Yes / No)</b>	<b>Deviations / Remarks</b>
MDT.REQ.001	Processor	At least Dual core, 1 GHz or more		
MDT.REQ.002	Memory	RAM at least 1 GB or better		
MDT.REQ.003	Storage	At least 8 GB or higher		
MDT.REQ.004	Operating System	Android v 4.1 and above		
MDT.REQ.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.REQ.006	Display	Capacitive touchscreen, 16M colours Resolution: 480 x 800 pixels (~217 ppi pixel density)		
MDT.REQ.007	Generation	2G and 3G support		
MDT.REQ.009	GSM	Yes		
MDT.REQ.010	Screen size	minimum 4" with touch support		
MDT.REQ.011	Camera & Video	at least 3MP Front & 5 MP rear with LED Flash (integrated) Geo-tagging, face/smile detection Video: Yes		
MDT.REQ.013	Feature	Should work as Location Tracker device for Attendance Management System		
MDT.REQ.014	Screen luminosity	Daylight readable		
MDT.REQ.016	Speakerphone	Hands free Support		
MDT.REQ.017	Keyboard	Virtual on Screen		
MDT.REQ.019	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.REQ.021	Audio Playing Format	With 3.5 mm Jack MP3,wav files format etc.		
MDT.REQ.022	Ports	Micro USB * 1 version 2.0 and above and same for charging and Headset port etc.		

<b>Mobile Device (Smart Phone)</b>				
<b>Sr. No.</b>	<b>Item</b>	<b>Minimum Requirement Description</b>	<b>Compliance (Yes / No)</b>	<b>Deviations / Remarks</b>
MDT.REQ.024	Power Supply	230V, 50 Hz AC Supply		
MDT.REQ.025	Bluetooth	Yes		
MDT.REQ.035	Battery	minimum 1500 mAh and above		
MDT.REQ.036	Charger	Suitable charger shall be supplied, Built-in rechargeable battery pack/battery. USB Charger		
MDT.REQ.037	Mobile Device Monitoring	Should support the ability to disable access to public App Stores based on a policy configuration		
MDT.REQ.038	Mobile Device Monitoring	Should have configuration Policies to allow individual components of the mobile device to be enabled or disabled.		

Smart Light				
Sr. No.	Category	Minimum Requirement Description	Compliance (Yes / No)	Deviations / Remarks
SMTLGHT.REQ.001	Electrical Specification	System Wattage (W) - 120 W +/-5%		
SMTLGHT.REQ.002	Electrical Specification	LED Wattage (W) - 105 W +/-2%		
SMTLGHT.REQ.003	Electrical Specification	AC Input Voltage Range (V) - 120-280 V		
SMTLGHT.REQ.004	Electrical Specification	Operating Frequency Range (Hz) - 47-53 Hz		
SMTLGHT.REQ.005	Electrical Specification	Total Harmonic Distortion (%) - <10%		
SMTLGHT.REQ.006	Electrical Specification	Low Intensity Mode Output - >10 lux at ground level		
SMTLGHT.REQ.007	Electrical Specification	Power Factor - >0.95		
SMTLGHT.REQ.008	Electrical Specification	Shall have below mentioned capabilities – <ul style="list-style-type: none"> <li>• Over Voltage Protection</li> <li>• Under Voltage Protection</li> <li>• Short Circuit Protection</li> <li>• Open Load Protection</li> <li>• On/off light scheduling</li> <li>• Independent control of each phase</li> <li>• Collecting data from electric meter</li> <li>• Identification of electrical faults</li> <li>• Non-volatile memory for data storage</li> </ul>		
SMTLGHT.REQ.009	Electrical Specification	Surge Protection (Both CM & DM) - 5KV Ext. 10 KV series		
SMTLGHT.REQ.010	Electrical Specification	Driver Details - Analog Dimmable driver		
SMTLGHT.REQ.011	Optical Specification	Luminous Flux(Lumen) - 10200 lumens		
SMTLGHT.REQ.012	Optical Specification	Luminous Efficacy (Lm/W) - 85 lm/w		
SMTLGHT.REQ.013	Optical Specification	Operation Mode - Continuous ON (full Intensity) and OFF and motion sensor operated (Low Intensity Mode) during No Motion Time		
SMTLGHT.REQ.014	Optical Specification	Minimum Motion Detection Distance - 15 meters from street light		
SMTLGHT.REQ.015	Optical Specification	Colour Temperature Range (K) - 5700 +/-300		

Smart Light				
Sr. No.	Category	Minimum Requirement Description	Compliance (Yes / No)	Deviations / Remarks
SMTLGHT.REQ.016	Optical Specification	CRI (Typ.) - >70		
SMTLGHT.REQ.017	Optical Specification	Secondary individual Lens to be provided		
SMTLGHT.REQ.018	Optical Specification	Built-in GSM/GPRS/EDGE modem		
SMTLGHT.REQ.019	Environmental Specification	Working Temp. Range - (-10 °C - +45 ° C)		
SMTLGHT.REQ.020	Environmental Specification	Working Humidity Range - 0 - 95%		
SMTLGHT.REQ.021	Environmental Specification	Max Recommended Junction Temperature - 85 ° C		
SMTLGHT.REQ.022	Environmental Specification	Temperature		
SMTLGHT.REQ.023	Environmental Specification	Max Allowable Junction Temperature - 120° C		
SMTLGHT.REQ.024	Environmental Specification	Life Time at Junction Temperature of 85 ° C based on LM-80 - 50000 Hours		
SMTLGHT.REQ.025	Mechanical Specification	Housing - Aluminium PDC		
SMTLGHT.REQ.026	Mechanical Specification	Housing dimension (mm) - 580x287x108		
SMTLGHT.REQ.027	Mechanical Specification	Lens - Batwing Profile,PC		
SMTLGHT.REQ.028	Mechanical Specification	Front Glass - Toughened Glass		
SMTLGHT.REQ.029	Mechanical Specification	Lamp IP Grade - IP 66 Power Supply IP - IP 67		
SMTLGHT.REQ.030	Mechanical Specification	Frame - Aluminium die-cast frame		

<b>Smart Traffic (Detectors &amp; Sensors and Controllers)</b>				
<b>Sr. No.</b>	<b>Category</b>	<b>Minimum Requirement Description</b>	<b>Compliance (Yes / No)</b>	<b>Deviations / Remarks</b>
<b>INTEGRATED PRESENCE DETECTION AND DATA COLLECTION SENSOR</b>				
SMTTRF.DET.REQ.001	General	Housing - Aluminium, with integrated rain/sun shield (optional: additional sunshield) Window in glass Screw Connectors: 3-pins for Broadband over Power Line (BPL)		
SMTTRF.DET.REQ.002	General	Mounting Bracket: Aluminium tube		
SMTTRF.DET.REQ.003	General	Mounting Piece: U-profile, glass fiber reinforced polyamide Attached to mounting bracket		
SMTTRF.DET.REQ.004	General	Height x Width x Depth (max. dimensions, housing + mounting bracket): Vertically mounted about 45 cm x 16 cm x 12 cm Horizontally mounted about 41 cm x 18 cm x 12 cm Diameter: about 12 cm Weight - < 900 gm		
SMTTRF.DET.REQ.005	Camera Type	Technology: Colour CMOS Sensor Size: 1/4 " Resolution: 640 x 480 pixels (VGA) Frame Rate: 25 FPS		
SMTTRF.DET.REQ.006	Lens Type	Wide Angle: Focal Distance 2,1mm Narrow Angle: Focal Distance 6,0mm ZOOM: Focal Distance: 5mm to 15mm, also supports motorized zoom via configuration tool		
SMTTRF.DET.REQ.007	Electrical Specifications	Broadband over Power Line (BPL) for power supply, communication of output status, configuration & monitoring (streaming video) via interface		
SMTTRF.DET.REQ.008	Electrical Specifications	RS485 Interface		
SMTTRF.DET.REQ.009	Electrical Specifications	Average Power Consumption $\leq$ 4W Operating Voltage - 12 to 26 V AC or DC Average Current Consumption 140mA @ 24VDC		

Smart Traffic (Detectors & Sensors and Controllers)				
Sr. No.	Category	Minimum Requirement Description	Compliance (Yes / No)	Deviations / Remarks
SMTTRF.DET.REQ.010	Video Compression	Type: H.264, MPEG-4 Frame Rate: up to 25FPS Resolution: VGA (640x480) Quality: up to 4Mbit/s Viewable via HTTP webpage IP-addressable		
SMTTRF.DET.REQ.011	Regulatory Compliance	Electromagnetic Compatibility: 2004/108/EG FCC: FCC Part 15 class A Shock & Vibration NEMA II specs Materials: all weatherproof (UV-resistant) Protection Grades: Housing - IP68, Connectors - IP67 Temperature Range: from -34°C to +80°C		
SMTTRF.DET.REQ.012	Sensor Firmware & Software	Shall provide presence detection for up to 4 zones Shall provide video images for the exact positioning of the detection zones. Shall be simple to program via both a portable PC. 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.		
SMTTRF.DET.REQ.013	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 integral pluggable screw terminal blocks for power input, power output (to sensor), RS485 (from sensor), Shall have a port PC connection.		
SMTTRF.DET.REQ.014	Sensor Cable	Shall be housed within a single overall jacket. Shall consist of two (2) 22AWG twisted pairs: one (1) 22AWG twisted pair for RS485 communications and one (1) 22AWG twisted pair for power (i.e. in total 4 wires + shielding)		
TRAFFIC SIGNAL CONTROLLER - SLAVE				
SMTTRF.MCON.REQ.001	Design	Modular & Scalable		

<b>Smart Traffic (Detectors &amp; Sensors and Controllers)</b>				
<b>Sr. No.</b>	<b>Category</b>	<b>Minimum Requirement Description</b>	<b>Compliance (Yes / No)</b>	<b>Deviations / Remarks</b>
SMTTRF.MCON.REQ.002	CPU	32 bit microcontroller		
SMTTRF.MCON.REQ.003	Memory	Internal Memory: Flash (512K), RAM (128K) External Memory: EEPROM (1MB)		
SMTTRF.MCON.REQ.004	Real Time Clock Selection	1. Calendar Clock (RTC) with 10 years Battery back-up. Clock accuracy better than +/- 1 minute per month 2. Inbuilt GPS Module for time synchronization with Accuracy +/- 1 sec. per year 3. ATCS Server Time		
SMTTRF.MCON.REQ.005	Protection	Auto Shut down on power fluctuation beyond limit & Auto Start up on restoration.		
SMTTRF.MCON.REQ.006	Output Switching	16 optically isolated solid state lamp driving output		
SMTTRF.MCON.REQ.007	Police Control Panel	Switches for Lamp OFF, Flash, Auto/Manual, Manual Advance & 4 Hurry Calls.		
SMTTRF.MCON.REQ.008	ATCS Interface	10/100Mbps RJ45 Ethernet port		
SMTTRF.MCON.REQ.009	Programming Facility	Built In Keyboard & LCD Display PC Software		
SMTTRF.MCON.REQ.010	Firmware Update	Through USB/RS232		
SMTTRF.MCON.REQ.011	Status Monitoring and Data Logging	RS 232/Ethernet		
SMTTRF.MCON.REQ.012	Auxiliary I/O Interface	8 Auxiliary I/O Interface		
SMTTRF.MCON.REQ.013	Output Protection	Open circuit, Short circuit, over load		
SMTTRF.MCON.REQ.014	Input/output Isolation	Optical Isolation.		
SMTTRF.MCON.REQ.015	Vehicle / Pedestrian Demand Actuation	16 optically isolated vehicle detector interface		
SMTTRF.MCON.REQ.016	Time Resolution	100 millisecond		
SMTTRF.MCON.REQ.017	ATC Compatibility	CoSiCoSt (Composite Signal Control Strategy)		
SMTTRF.MCON.REQ.018	Power Specification	Working Voltage - 12 V DC		

<b>Smart Traffic (Detectors &amp; Sensors and Controllers)</b>				
<b>Sr. No.</b>	<b>Category</b>	<b>Minimum Requirement Description</b>	<b>Compliance (Yes / No)</b>	<b>Deviations / Remarks</b>
SMTTRF.MCON.REQ.019	Power Specification	Power Consumption - 3.6 Watts		
SMTTRF.MCON.REQ.020	Certification	IEC - 60068 (ERTL)		
SMTTRF.MCON.REQ.021	Environmental	Support - Temperature - 0 °C - 55 °C, Humidity - 95%		
<b>TRAFFIC SIGNAL CONTROLLER - SLAVE</b>				
SMTTRF.SCON.REQ.001	Design	Modular & Scalable		
SMTTRF.SCON.REQ.002	CPU	32 bit microcontroller		
SMTTRF.SCON.REQ.005	Protection	Auto Shut down on power fluctuation beyond limit & Auto Start up on restoration.		
SMTTRF.SCON.REQ.006	Output Switching	16 optically isolated solid state lamp driving output		
SMTTRF.SCON.REQ.008	ATCS Interface	10/100Mbps RJ45 Ethernet port		
SMTTRF.SCON.REQ.010	Firmware Update	Through USB/RS232		
SMTTRF.SCON.REQ.011	Status Monitoring and Data Logging	RS 232/Ethernet		
SMTTRF.SCON.REQ.018	Power Specification	Working Voltage - 12 V DC		
SMTTRF.SCON.REQ.019	Power Specification	Power Consumption - 3 Watts		
SMTTRF.SCON.REQ.020	Certification	IEC - 60068 (ERTL)		
SMTTRF.SCON.REQ.021	Environmental	Support - Temperature - 0 °C - 55 °C, Humidity - 95%		



Environmental Sensors					
Sr. No.	Category	Minimum Requirement Description		Compliance (Yes / No)	Deviations / Remarks
ENV.REQ.001	Functional Requirement	The environment sensors should be have the following capabilities			
ENV.REQ.002	Functional Requirement	They should be ruggedized enough to be deployed in open air areas on streets and parks			
ENV.REQ.003	Functional Requirement	They should be able to read and report at least the following parameters			
		o Temperature			
		o Humidity			
		o Ambient Light			
		o Sound			
		o CO			
ENV.REQ.004	Functional Requirement	The sensor should be able to communicate its data using wireless technology			
ENV.REQ.005	Functional Requirement	The data should be collected in a software platform that allows third party software applications to read that data.			
ENV.REQ.006	Functional Requirement	The sensor management platform should allow the configuration of the sensor to the network and also location details etc.			
ENV.REQ.007	Air QualityParameters	NO2	upto 10ppm		
ENV.REQ.008	Air QualityParameters	CO	upto 1000 ppm		
ENV.REQ.009	Air QualityParameters	SO2	upto 20 ppm		
ENV.REQ.010	Air QualityParameters	O3	upto 1000 ppb		
ENV.REQ.011	Air QualityParameters	PM 2.5	0 to 230 micro gms / cu.m		

Environmental Sensors					
Sr. No.	Category	Minimum Requirement Description		Compliance (Yes / No)	Deviations / Remarks
ENV.REQ.012	Air QualityParameters	PM 10	0 to 450 micro gms / cu.m		
ENV.REQ.013	WeatherParameters	Temperature	0 to 100 Deg. C		
ENV.REQ.014	WeatherParameters	Relative Humidity	upto 100%		
ENV.REQ.015	WeatherParameters	Light	upto 10,000 Lux		
ENV.REQ.016	WeatherParameters	UV	upto 15 mW/ cm2		
ENV.REQ.017	WeatherParameters	CO2	upto 5000 ppm		
ENV.REQ.018	Noise Parameters	Noise	upto 120 dB (A)		
ENV.REQ.019	Interface & Power	GPS	Should have GPS capability		
ENV.REQ.020	Interface & Power	GSM	3G compatible		
ENV.REQ.021	Interface & Power	Wi-fi	802.11b/g/n		
ENV.REQ.022	Interface & Power	Power	12 V , 2 A DC supply for ESD		
ENV.REQ.023			12 V , 3 A DC or 230 V, 1 A for housing fan		
ENV.REQ.024	Other parameters	Dimensions	300mm ø dia x 200 mm (height) - disc*		
ENV.REQ.025	Other parameters	Mounting	To be located in a housing, on a pole		
ENV.REQ.026			500 mm x 250 mm x 250 mm *		
ENV.REQ.027			(*indicative - final size based on configuration)		

Environmental Sensors					
Sr. No.	Category	Minimum Requirement Description		Compliance (Yes / No)	Deviations / Remarks
ENV.REQ.028	Other parameters	Enclosure	Engineering Polymer or Metal construct		

Automated Vehicle Locator System - AVLS					
Sr. No.	Category	Minimum Requirement Description		Compliance (Yes / No)	Deviations / Remarks
AVLS.REQ.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.REQ.002	General Requirement	The AVLS shall be able to give ETA at next bus stops in real time based on speed and distance measurement. The system shall update ETA at each bus stop on all PIS accordingly.			
AVLS.REQ.003	General Requirement	The system shall be able to compare the actual location of the vehicle / bus, at any given time, with its scheduled location			
AVLS.REQ.004	General Requirement	The 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 en-route			
AVLS.REQ.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.REQ.006	General Requirement	Information elements that need to be captured and transmitted to City Operation Center at the minimum include longitude, latitude, and physical location en-route with date and time stamps, vehicle / bus number, route number, and Driver ID, etc.			
AVLS.REQ.007	General Requirement	Shall provide these data on real time basis at pre-determined and configurable intervals (10 seconds) over GPRS/GSM network			
AVLS.REQ.008	General Requirement	Tracking of vehicle / buses that deviate from the scheduled route based on definition of permitted geographic regions of operation			

<b>Automated Vehicle Locator System - AVLS</b>				
<b>Sr. No.</b>	<b>Category</b>	<b>Minimum Requirement Description</b>	<b>Compliance (Yes / No)</b>	<b>Deviations / Remarks</b>
AVLS.REQ.009	General Requirement	Vehicle Fleet Summary Dashboard – Quick view on vehicle fleet performance		
AVLS.REQ.010	General Requirement	Register a vehicle / bus on unscheduled route from backend on real time basis		
AVLS.REQ.011	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.REQ.012	General Requirement	Real-time Running Trip Line diagram of vehicle / buses on a particular route, for headway detection.		
AVLS.REQ.013	General Requirement	Auto headway detection and notification.		
AVLS.REQ.014	General Requirement	Applications Software shall have a facility to define the Masters.		
AVLS.REQ.015	General Requirement	New routes shall be created in the application.		
AVLS.REQ.016	General Requirement	Business rules engine for fare stages, fare structures, various routes etc. shall be configurable.		
AVLS.REQ.017	General Requirement	The 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.REQ.018	General Requirement	Officials shall be able to access the application as per the pre-defined roles and responsibilities		
AVLS.REQ.019	General Requirement	The application shall provide facility to query the data and generate the customized reports as per the requirements.		
AVLS.REQ.020	General Requirement	The system shall display the contact details of the bus driver / conductor so that the operation center staff can communicate with them directly.		
AVLS.REQ.021	General Requirement	The Operation Center 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.		

<b>Automated Vehicle Locator System - AVLS</b>				
<b>Sr. No.</b>	<b>Category</b>	<b>Minimum Requirement Description</b>	<b>Compliance (Yes / No)</b>	<b>Deviations / Remarks</b>
AVLS.REQ.022	General Requirement	The system be able to integrate with the City IOP/City Operations Platform platform with all the available data like Location , route information, Vehicle telemetry informations, Speed etc.		
AVLS.REQ.023	General Requirement	The system should allow programmability, allowing actions to be triggered based on events. e.g. speed metric can triggers API call to GIS Maps pulling speed limit on the road based on GPS or GTFS location.		
AVLS.REQ.024	General Requirement	The palatform should offer an Application builder for developping custom Applications as needed and also Should support an Interactive Development Environment that can facilitate in-house expertise to develop widgets and create API extensions		

Smart Parking System				
Sr. No.	Category	Minimum Requirement Description	Compliance (Yes / No)	Deviations / Remarks
SPIS.REQ.001	General Requirements	The system should be able count the number of vehicles entering and exiting a multi-level parking structure.		
SPIS.REQ.002	General Requirements	The system should do this using a wireless parking sensors network which captures free/occupied status		
SPIS.REQ.003	General Requirements	The system should communicate both the counts to a local and central software application over network.		
SPIS.REQ.004	General Requirements	The software application should be able to tally the entry and exit car counts and calculate the available parking in that parking structure.		
SPIS.REQ.005	General Requirements	System shall be able to make out configured in both the mode to detect parked vehicle in the authorized parking space and vehicle parked in the unauthorized parking space through wireless network		
SPIS.REQ.006	General Requirements	The software application should be able to communicate parking availability information at each parking lot on a LCD displays deployed at key points of interest in the city.		
SPIS.REQ.007	General Requirements	The software system should optimally make this data available to a smart phone application that citizens might use to get real time parking availability.		
SPIS.REQ.008	General Requirements	The system should retain Number Plate details of car entering /exiting the parking zone for at least 7 days for future forensics if required.		
SPIS.REQ.009	General Requirements	Smart Parking mobile app shall help users to locate free parking, block free parking and navigate to parking slot. Smart Parking app shall be available for iOS and Android Platform		
SPIS.REQ.010	General Requirements	A local system for parking operator for ticketing, revenue collection and reporting		
SPIS.REQ.011	General Requirements	Mobile users shall provide with QR code which gets verified at the local system at parking area, local system shall generate the parking ticket.		

Smart Parking System				
Sr. No.	Category	Minimum Requirement Description	Compliance (Yes / No)	Deviations / Remarks
SPIS.REQ.012	General Requirements	Normal users shall buy parking ticket at the parking area through local system.		
SPIS.REQ.013	General Requirements	The display board deployed at the parking area shall continuously connected with the local system and displays the real time data		
SPIS.REQ.014	General Requirements	Street side display shall be given feed regarding parking space availability from the central parking information system		

<b>Passenger Information System - PIS</b>				
<b>Sr. No.</b>	<b>Category</b>	<b>Minimum Requirement Description</b>	<b>Compliance (Yes / No)</b>	<b>Deviations / Remarks</b>
PIS.REQ.001	General Requirement	It shall manage the content on all the on Bus and Bus Stops LED display and shall show Bus number, route, schedule and ETA on LED screens. The ETA shall be calculated and refreshed at selectable refresh rate		
PIS.REQ.002	General Requirement	Display of PIS in a display unit at bus station shall be configurable based on bus station and platform. Single unit shall display services of more than one platform.		
PIS.REQ.003	General Requirement	It shall send the route files and schedule details from City Operation Center (COC) to on bus & bus stop LEDs with synchronized voice announcement		
PIS.REQ.004	General Requirement	PIS information shall be displayed in Marathi, Hindi and English alternatively (single or multiple language shall be configurable). Specifically, all display technologies and software shall support the Unicode ( <a href="http://www.unicode.org/">http://www.unicode.org/</a> ) character set.		
PIS.REQ.004	General Requirement	It shall have provision to show advertisement on bus stops & in-bus passenger facing display along with audio from speakers installed in bus.		
PIS.REQ.005	General Requirement	Bus stations display units shall be able to receive/display transmitted contents from the central system through a gateway or mention other suitable means		
PIS.REQ.006	General Requirement	The frequency and period of information display on PIS display shall be configurable from central location for advertisements and other transit information		
PIS.REQ.007	General Requirement	It shall manage the next stop announcements in on-bus passenger facing display along with audio from speakers based on GPS location received from AVLS system		
PIS.REQ.008	General Requirement	It shall have provision to integrate with Smart Transport Mobile Application which shall show bus route, schedule, real time bus location and ETA details		
PIS.REQ.009	General Requirement	Should be able to integrate with Integrated Operation Platform for complete dashboard view		



<b>Fleet Management System - FMS</b>				
<b>Sr. No.</b>	<b>Category</b>	<b>Minimum Requirement Description</b>	<b>Compliance (Yes / No)</b>	<b>Deviations / Remarks</b>
FMS.REQ.001	General Requirement	System shall have list of all the buses, routes, drivers & conductors available for duty allocation		
FMS.REQ.002	General Requirement	Provision to enter duty for driver, conductor and buses and shall be able to assign to all buses.		
FMS.REQ.003	General Requirement	It shall have provision to send SMS to respective driver and conductor about their duty.		
FMS.REQ.004	General Requirement	It shall have provision to create report for the vehicles available for duty, under maintenance and on casual duty to manage the fleet effectively		
FMS.REQ.005	General Requirement	It shall keep records of KM run of bus to monitor and plan the maintenance of the bus after certain run. The system shall have provision to set the KM manually in the system if required.		
FMS.REQ.006	General Requirement	Provision to alter driver and conductor duty in system and in such scenario immediate SMS shall go to driver and conductor about the change in their duty		
FMS.REQ.007	General Requirement	Should be able to integrate with Integrated Operation Platform for complete dashboard view		

<b>Mobile Application - Transport</b>				
<b>Sr. No.</b>	<b>Category</b>	<b>Minimum Requirement Description</b>	<b>Compliance (Yes / No)</b>	<b>Deviations / Remarks</b>
MT.REQ.001	General Requirement	Mobile application shall give access to real-time bus schedules, bus routes, frequency etc.		
MT.REQ.002	General Requirement	Query based GUI		
MT.REQ.003	General Requirement	It shall give following information: <ul style="list-style-type: none"> <li>• Scheduled and expected time of arrival at each stop along with bus route no. and route name</li> <li>• Stops names for each route name and route no.</li> <li>• Running information of bus (ETA) and ticket price</li> <li>• Navigation system to reach out to the nearest/intended bus stop</li> </ul>		
MT.REQ.004	General Requirement	Support all popular & latest versions of android platform and shall be downloadable to any Android Mobile Phone or a Tablet for public		
MT.REQ.005	General Requirement	Provide direct update feature which shall ensure application can be updated as soon as new build is published on server to avoid running of multiple versions of same apps		
MT.REQ.006	General Requirement	Offer advanced capabilities to ensure security of application data, application authenticity, application communication with back-end servers as well as additional security like user security and device authentication		
MT.REQ.006	General Requirement	Should be able to integrate with Integrated Operation Platform for complete dashboard view		

<b>Smart Lighting System - SLS</b>				
<b>Sr. No.</b>	<b>Category</b>	<b>Minimum Requirement Description</b>	<b>Compliance (Yes / No)</b>	<b>Deviations / Remarks</b>
SLS.REQ.001	General Requirement	Each LED fixture is equipped with controllable driver communicating with the controller node		
SLS.REQ.002	General Requirement	Smart street lighting sensors shall detect moving objects, vehicles and people, sends the data to the controller node and then the light levels are adjusted accordingly		
SLS.REQ.003	General Requirement	Shall be able to operate at any weather condition and shall be communicating using wireless technology (preferably leveraging the City WiFi)		
SLS.REQ.004	General Requirement	Shall have the capability to receive the instruction from the Lighting Operations Management software and act accordingly		
SLS.REQ.005	General Requirement	Allows programming, dimming, monitoring and metering of street lights		
SLS.REQ.006	General Requirement	Ability to control individual or group of LED lights on the street for turning on, off and dimming as per the command received from the Lighting Operations Management software		
SLS.REQ.007	General Requirement	Ability to operate in real time based on Motion sensing & Ambient light sensing capabilities		
SLS.REQ.008	General Requirement	Ability to create policies for City lighting based on time of the day, ambient lighting conditions and other scenarios and events on the street. For example, the solution can be configured to dim the lights in the middle of the night when the streets are empty and when there is movement of people or vehicles, the intensity can be increased to provide enhanced lighting, traffic based luminosity control, switching alternate lights ON/OFF etc.		
SLS.REQ.009	General Requirement	The rule engine set up on the Lighting Management system shall run on the real time data and apply the policies automatically. At any time, these policies can be overridden by human intervention with the system		
SLS.REQ.010	General Requirement	Monitor voltage, current, voltage fluctuation, power consumption for each individual light as well as a group of lights and city areas.		
SLS.REQ.011	General Requirement	The solution can also detect failures of LED bulbs and other circuitry and generate alarms for maintenance automatically.		
SLS.REQ.012	General Requirement	Solution also allows to operate the Smart Lighting System manually too		

Smart Lighting System - SLS				
Sr. No.	Category	Minimum Requirement Description	Compliance (Yes / No)	Deviations / Remarks
SLS.REQ.013	General Requirement	<ul style="list-style-type: none"> <li>- Should be able to operate the lights switch on/off, increase/decrease luminosity as per the command received from the Lighting Operations Management software</li> <li>- Should be able to see the real time status of the Smart Lighting System on a city map view of the City Infrastructure Management Dashboard should be able to see the real time status of the Smart Lighting System on a city map view of the City Infrastructure Management Dashboard</li> <li>- Should enable Over the Air (OTA) firmware update</li> <li>- Rule engine set up on the Lighting Operations Management software should run on the real time data and apply the policies automatically</li> <li>- Data transmitted by and received from the sensors should be encrypted and tamper proof end to end (from sensor to application)</li> </ul>		
SLS.REQ.014	General Requirement	<p>MIS -</p> <ul style="list-style-type: none"> <li>• Real time status of individual Street lights at any point of time on a city map view of the Management Dashboard.</li> <li>• Real time energy consumption reports of each light, group of lights and city areas</li> <li>• At any point in time, the map view shall give the details of the status, luminosity of the lights in city map view</li> <li>• Various other customized reports as per the requirement</li> </ul>		
SLS.REQ.015	General Requirement	Should provide an external infrared interface for security keys transfer and local configuration		
SLS.REQ.016	General Requirement	Should be able to integrate with Integrated Operation Platform for complete dashboard view		

Area Based Traffic Management System				
Sr. No.	Category	Minimum Requirement Description	Compliance (Yes / No)	Deviations / Remarks
ATMS.REQ.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.REQ.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 center by each controller.		
ATMS.REQ.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 Center based on the data and information gathered by vehicle detectors at strategic locations at the intersections controlled by the system		
ATMS.REQ.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.REQ.005	General Requirement	Pedestrian Priority <ul style="list-style-type: none"> <li>• 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.</li> <li>• 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.</li> <li>• Shall allow the pedestrian green and/or flashing red intervals to overlap between one or more stages with non-conflicting phases if so required.</li> </ul>		

Area Based Traffic Management System				
Sr. No.	Category	Minimum Requirement Description	Compliance (Yes / No)	Deviations / Remarks
ATMS.REQ.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.REQ.007	General Requirement	Should be able to integrate with Integrated Operation Platform for complete dashboard view		

**Note: For Variable Message System (VaMS) and Public Address System specifications kindly refer to City Surveillance specification section**

## 1.6 Common Infrastructure & Solutions

<b>Enterprise Management System (EMS)</b>				
<b>Sr. No.</b>	<b>Item</b>	<b>Minimum Requirement Description</b>	<b>Requirement available (Yes/ No)</b>	<b>Standard/ Customized/ Bespoke</b>
EMS.REQ.001	Enterprise Management System	Bidder should quote tool for monitoring services, & SLA along with Helpdesk tool for NMC along with all the necessary Hardware, DB, OS, etc.		
EMS.REQ.002	Enterprise Management System	Solution should be scalable and open to third party integration.		
EMS.REQ.003	Enterprise Management System	Should support Web / Administration Interface.		
EMS.REQ.004	Enterprise Management System	Should provide compatibility to standard RDBMS.		
EMS.REQ.005	Enterprise Management System	The Service Management solution namely Service desk (incident and problem mgmt.), Change, and SLA management should have shared configuration database with a unified architecture.		
EMS.REQ.006	Enterprise Management System	Offered solution should provide for future scalability of the whole system without major architectural changes.		
EMS.REQ.007	Enterprise Management System	Enterprise Management System should provide for end to end performance, availability, fault and event and impact management for all enterprise resources that encompasses the heterogeneous networks, systems, applications, databases and client infrastructure present in the enterprise.		
EMS.REQ.008	Enterprise Management System	The agent and agentless monitor should be able to collect & manage event/fault, performance and capacity data and should not require separate collectors.		
EMS.REQ.009	Enterprise Management System	The solution should reduce manual customization efforts and should speed-up problem identification and resolution of the IT performance anomalies with intelligent events.		
EMS.REQ.010	Enterprise Management System	The solution should accelerate problem isolation through accurate analysis of probable cause through end-to-end correlation.		
EMS.REQ.011	Enterprise Management System	The solution should have the capability to identify probable root cause using a variety of filtering and statistical correlation		

<b>Enterprise Management System (EMS)</b>				
<b>Sr. No.</b>	<b>Item</b>	<b>Minimum Requirement Description</b>	<b>Requirement available (Yes/ No)</b>	<b>Standard/ Customized/ Bespoke</b>
		methods to determine their relevance to the issue being researched.		
EMS.REQ.012	Enterprise Management System	The solution should possess capabilities that deliver self-learning capabilities to virtually eliminate the effort of manual threshold, rule, and script maintenance.		
EMS.REQ.013	Enterprise Management System	The agent and agentless monitor should be able to collect & manage event/fault, performance and capacity data and should not require separate collectors.		
EMS.REQ.014	Enterprise Management System	The solution should have predictive analytics and intelligence in-built into it so as to detect any anomaly before it could potentially hit the threshold thereby giving enough lead time to users to resolve the issues before the threshold is breached.		
EMS.REQ.015	Enterprise Management System	The solution should carry out automated probable cause analysis by picking up feeds from every infrastructure component being monitored and automating the correlation of these alarms/events to point out the probable cause of an infrastructure error.		
EMS.REQ.016	Enterprise Management System	Solution should carry out probable cause analysis thereby helping operators to identify the root cause without having to write complex rules for correlation.		
EMS.REQ.017	Enterprise Management System	Solution should be able to score the events and display the highest impacting events in descending order or any other order as customized by the administrator.		
EMS.REQ.018	Enterprise Management System	The Solution should offer the ability to monitor any		
EMS.REQ.019	Enterprise Management System	Custom/home-grown applications for which the monitoring areas have been defined.		
EMS.REQ.020	Enterprise Management System	The solution should be extensible enough to support capacity planning and optimization with data collected through the deployed performance management agent or from agentless data collectors.		
EMS.REQ.021	Enterprise Management System	Should be able to monitor/ manage large heterogeneous systems environment continuously.		



<b>Enterprise Management System (EMS)</b>				
<b>Sr. No.</b>	<b>Item</b>	<b>Minimum Requirement Description</b>	<b>Requirement available (Yes/ No)</b>	<b>Standard/ Customized/ Bespoke</b>
EMS.REQ.022	Enterprise Management System	Servers: Should be able to monitor the server instances, database and instance status, initialization parameters, CPU usage, parallel processing, and SQL tracing.		
EMS.REQ.023	Enterprise Management System	Should be able to monitor performance statistics reported as timings and throughput values for such operations as reads, writes, and recursive calls.		
EMS.REQ.024	Enterprise Management System	Should be able to monitor statistics reports as averages and percentages for such items as data caches hits, queue waits, disk sorts, and rollbacks.		
EMS.REQ.025	Enterprise Management System	The Network Management should monitor performance across heterogeneous networks having multiple categories of devices like firewall, switches etc. across Department including the DC, DR site.		
EMS.REQ.026	Enterprise Management System	It should proactively analyze problems to improve network performance.		
EMS.REQ.027	Enterprise Management System	The Network Management function should create a graphical display of all discovered resources.		
EMS.REQ.028	Enterprise Management System	Should monitor various operating system parameters such as processors, memory, files, processes, file systems etc. where applicable using agent /agentless on the servers to be monitored.		
EMS.REQ.029	Enterprise Management System	Provide performance threshold configuration for all the agents to be done from a central GUI based console that provide a common look and feel across various platforms in the enterprise. These agents could then dynamically reconfigure the performance monitors to use these threshold profiles they receive.		
		<b>IT Service Management</b>		
EMS.REQ.030	Enterprise Management System	Centralized IT helpdesk for technical and functional support should be maintained to respond to queries and solve issues of the users.		
EMS.REQ.031	Enterprise Management System	The Helpdesk should be accessible through various communication channels viz. Telephone, web based facility and		

<b>Enterprise Management System (EMS)</b>				
<b>Sr. No.</b>	<b>Item</b>	<b>Minimum Requirement Description</b>	<b>Requirement available (Yes/ No)</b>	<b>Standard/ Customized/ Bespoke</b>
		email. The helpdesk should be able to respond to the queries/problems in the time limits as specified in Service Level Agreement.		
EMS.REQ.032	Enterprise Management System	Online Helpdesk system should be deployed and would be used for management and support activity. Service desk is envisaged as a tool that will facilitate the end-to-end service support for users. The proposed system should include required hardware and software and should have sufficient analyst licenses to meet the requirement of Project.		
EMS.REQ.033	Enterprise Management System	The Solution should have the complete ITIL process flow for Incident, problem, Change and release Management.		
EMS.REQ.034	Enterprise Management System	The solution should have Service Management Process Model in built based on ITIL v3 best practices.		
EMS.REQ.035	Enterprise Management System	At each stage in the cycle of the incident, the system should prompt users on the status and the missing information that is required to complete the flow.		
EMS.REQ.036	Enterprise Management System	In case any process step is missed, the system prompts users to complete that step before they move to the next step.		
EMS.REQ.037	Enterprise Management System	Solution should support reporting on the process flow to allow management to understand how organization is performing in terms of process adherence.		
EMS.REQ.038	Enterprise Management System	Solution should support multi-tenancy with complete data isolation as well as with ability for analysts based on access rights to view data for one, two or more organizational units.		
EMS.REQ.039	Enterprise Management System	Solution should automatically provide solutions from the knowledge base.		
EMS.REQ.040	Enterprise Management System	Workflow should be able to perform notification via email, SMS and the have provision to interface with other communication modes. The solution should provision the administrator to create new or modify existing workflow by using actions like set fields, push fields, SQL query etc.		
EMS.REQ.041	Enterprise Management System	The solution should provide the functionality of executing searches to the entire database.		

<b>Enterprise Management System (EMS)</b>				
<b>Sr. No.</b>	<b>Item</b>	<b>Minimum Requirement Description</b>	<b>Requirement available (Yes/ No)</b>	<b>Standard/ Customized/ Bespoke</b>
		<b>Incident/Problem Management</b>		
EMS.REQ.042	Enterprise Management System	Flexibility of logging incidents via various means - web interface, email, phone. Service Desk solution should allow detailed multiple levels/tiers of categorization on the type of incident being logged.		
EMS.REQ.043	Enterprise Management System	Service Desk solution should provide classification to differentiate the criticality of the security incident via the priority levels, severity levels and impact levels.		
EMS.REQ.044	Enterprise Management System	It should allow SLA to be associated with a ticket based on priority, severity, incident type, requestor, asset, location or group individually as well as collectively.		
EMS.REQ.045	Enterprise Management System	Solution should support fast service restoration leveraging previous incident data.		
EMS.REQ.046	Enterprise Management System	It should be possible for agent to view the 'Health of a selected asset' from within the ticket.		
EMS.REQ.047	Enterprise Management System	The health view should be consistent across platform (Windows & flavors of UNIX / Linux).		
EMS.REQ.048	Enterprise Management System	Should support automatic assignment of ticket to the right skilled resource based on business priority Ex - Database crash issue need not be assigned to a DBA unless the business service is completely down.		
EMS.REQ.049	Enterprise Management System	Asset causing the business failure and business service that has failed should be automatically related to the ticket.		
EMS.REQ.050	Enterprise Management System	It should be possible to architect a decentralized service operations (across OS, database and application versions).		
EMS.REQ.051	Enterprise Management System	For integrations with other EMS/NMS tools, various options for integration should be provided - APIs, web services, SDKs.		
EMS.REQ.052	Enterprise Management System	It should have an updateable knowledge base for technical analysis and further help end-users to search solutions for previously solved issues. Should support full text search capabilities.		

<b>Enterprise Management System (EMS)</b>				
<b>Sr. No.</b>	<b>Item</b>	<b>Minimum Requirement Description</b>	<b>Requirement available (Yes/ No)</b>	<b>Standard/ Customized/ Bespoke</b>
EMS.REQ.053	Enterprise Management System	<b>Change Management</b>		
EMS.REQ.054	Enterprise Management System	Should support Change Impact and change collision detection based on affected CIs from CMDB.		
EMS.REQ.055	Enterprise Management System	Solution should provide for Change Calendar with periodical views.		
EMS.REQ.056	Enterprise Management System	Should support self-service change request and fulfilment with standard change requests via service catalogue.		
EMS.REQ.057	Enterprise Management System	Should support Incident & problem driven change-release-deployment activities. End to End Release Management workflows should be supported with in-built rollback capabilities.		
EMS.REQ.058	Enterprise Management System	Should support unified change and release tools (planning, risk assessment, scheduling, and execution tools) for complete enterprise across virtual & physical environments, applications, etc.		
	Enterprise Management System	<b>Configuration Management</b>		
EMS.REQ.059	Enterprise Management System	The Configuration Management Database should support multiple datasets with federation and reconciliation facilities so as to get data from various discovery tools and also through manual import process.		
EMS.REQ.060	Enterprise Management System	The Configuration Management should support Definitive Software and Media Library with content updates on a periodic basis.		
EMS.REQ.061	Enterprise Management System	Normalization of data should be possible along complete definitive media library – software, hardware with standardization on attributes.		
EMS.REQ.062	Enterprise Management System	Reconciliation of data should be possible with multiple data providers based on common attributes and ability to define precedence rules on attributes.		
EMS.REQ.063	Enterprise Management System	Federation of external data sources should be possible with ability to store common attributes inside CMDB and getting other attributes from external data sources in real time.		

<b>Enterprise Management System (EMS)</b>				
<b>Sr. No.</b>	<b>Item</b>	<b>Minimum Requirement Description</b>	<b>Requirement available (Yes/ No)</b>	<b>Standard/ Customized/ Bespoke</b>
EMS.REQ.064	Enterprise Management System	Should provide best in class integration capabilities with CMDB compliant APIs.		
EMS.REQ.065	Enterprise Management System	Should Provide a single shared view of services supporting Service Design, Transition and Operations stages of the lifecycle.		
EMS.REQ.066	Enterprise Management System	Should Provide a Service catalogue so as to establish a framework for Service definitions based on IT and business alignment.		
EMS.REQ.067	Enterprise Management System	Should Provide Service blueprints to describe functional and deployment models for the Service definitions.		
EMS.REQ.068	Enterprise Management System	Should automatically create Service models to describe how IT infrastructure supports business services.		
EMS.REQ.069	Enterprise Management System	Manage services consistently across heterogeneous Primary site & DR site and cloud environments.		
		<b>Service Level Management / Monitoring</b>		
EMS.REQ.070	Enterprise Management System	The SLA Monitoring function of the EMS is by far the most important requirement of the Integrated Project. This is on account of the fact that commitment of the projects to the citizens is dependent on an effective and continuous monitoring of the timelines within which citizens are served at the Portal or GSKs. In this context, the SLA Monitoring will have to possess the following capabilities:		
EMS.REQ.071	Enterprise Management System	Response times of Portal;		
EMS.REQ.072	Enterprise Management System	Transaction handling capacity of application server in terms of number of concurrent connects;		
EMS.REQ.073	Enterprise Management System	Should compile the performance statistics from all the IT systems involved and compute the average of the parameters over a month, and compare it with the SLA metrics laid down in the RFP;		
EMS.REQ.074	Enterprise Management System	Have a consolidated, automated graphical report for SLA compliance with ability to drill down to reason for non-compliance.		

<b>Enterprise Management System (EMS)</b>				
<b>Sr. No.</b>	<b>Item</b>	<b>Minimum Requirement Description</b>	<b>Requirement available (Yes/ No)</b>	<b>Standard/ Customized/ Bespoke</b>
EMS.REQ.075	Enterprise Management System	Manage service levels for delivery and support of business services.		
EMS.REQ.076	Enterprise Management System	Fast, repeatable process for defining and capturing service level measurements.		
EMS.REQ.077	Enterprise Management System	Real-time visualization of service level targets, agreement compliance data, penalties and rewards.		
EMS.REQ.078	Enterprise Management System	Deliver service level information and alerts directly to IT Operations and Service Support consoles.		
EMS.REQ.079	Enterprise Management System	Should support compliance and cost trending to assist in identifying areas for process and operational improvements.		
		<b>Service Request Management</b>		
EMS.REQ.080	Enterprise Management System	Should support single service catalogue for requestable services		
EMS.REQ.081	Enterprise Management System	Should provide for Service Requests Workflows and Fulfilment definitions for commonly used IT/non-IT services.		
EMS.REQ.082	Enterprise Management System	Catalog based on User profile		
EMS.REQ.083	Enterprise Management System	Ability to position both Custom-made and Standard Requests		
EMS.REQ.084	Enterprise Management System	Should send notifications to Customers based on the status		
EMS.REQ.085	Enterprise Management System	Should have the ability to extend and create new service request		
EMS.REQ.086	Enterprise Management System	Should have predefined catalogues that cover specific use cases		
EMS.REQ.087	Enterprise Management System	Should be completely web based and should be accessible from an portal		
EMS.REQ.088	Enterprise Management System	The services should be integrated to SLAs and should be auto measured for adherence.		
		<b>Reporting</b>		
EMS.REQ.089	Enterprise Management System	Should provide for Reports for Service Support and Service Delivery processes through a unified portal.		

<b>Enterprise Management System (EMS)</b>				
<b>Sr. No.</b>	<b>Item</b>	<b>Minimum Requirement Description</b>	<b>Requirement available (Yes/ No)</b>	<b>Standard/ Customized/ Bespoke</b>
EMS.REQ.090	Enterprise Management System	Should have ability to have a consolidated view of data collected from different types of operations (Eg - SLA compliance for a selected service, it's dependent SLAs, OLA and UPCs, it's changes by priority, open incidents by priority and status, it's assets and individual asset compliance, patches installed and compliance to patches etc.) and displayed in a universal portal		
EMS.REQ.091	Enterprise Management System	Provide users (based on role) to drill down to specific report/data on a need basis		
EMS.REQ.092	Enterprise Management System	Provide detailed reports on a specific area as per the need of the user		
EMS.REQ.093	Enterprise Management System	Should support multiple views with flexible structure along with role based access.		
EMS.REQ.094	Enterprise Management System	The Service Desk / Helpdesk & SLA Monitoring tool shall have software application which is ITIL compliant		

<b>Integrated Operation Platform (IOP)</b>				
<b>Sr. No.</b>	<b>Item</b>	<b>Minimum Requirement Description</b>	<b>Compliance (Yes / No)</b>	<b>Deviations / Remarks</b>
IOP.REQ.001	General Requirements	IOP shall be open architecture based, highly scalable and able to integrate multiple disparate systems seamlessly on a common platform		
IOP.REQ.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.REQ.003	General Requirements	Some of the incidents that the IOP responds to include but are not limited to the following: <ul style="list-style-type: none"> <li>• Hazards / Calamities: Natural, Man-made, Environmental</li> <li>• Epidemics (Health)</li> <li>• Transportation (Road, Rail etc)</li> <li>• Public Utility (Water, Electricity, Street Lighting, Solid Waste Management)</li> <li>• Public Safety (Crime, Law &amp; Order)</li> </ul>		
IOP.REQ.004	General Requirements	The system shall integrate with various emergency response services such as Ambulance, Fire, Disaster Management Systems, etc.,		
IOP.REQ.005	General Requirements	The system shall integrate with various social media applications such as Facebook, Twitter etc., and also provide intelligent dashboard functions as required		
IOP.REQ.006	General Requirements	The system shall support various sensors like Cameras, GPS, Voice devices (Analog & Digital), Storage devices, Sensor inputs from other Utility applications/ systems		
IOP.REQ.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.REQ.008	General Requirements	The IOP platform shall provide a dashboard functionality to manage workflows by integrating information from different agencies and systems to facilitate responsive decision making		
IOP.REQ.009	General Requirements	The IOP platform should provide a cross-agency collaboration tool to support instant communication between various user groups and authorities		
IOP.REQ.010	General Requirements	The IOP platform should facilitate training mechanism		
IOP.REQ.011	Location Requirements	The platform shall have a GIS based map to provide the location detail		
IOP.REQ.012	Location Requirements	Multiple layer maps to be supported as required for various applications		



<b>Integrated Operation Platform (IOP)</b>				
<b>Sr. No.</b>	<b>Item</b>	<b>Minimum Requirement Description</b>	<b>Compliance (Yes / No)</b>	<b>Deviations / Remarks</b>
IOP.REQ.013	Location Requirements	GIS maps to comply OGC standards		
IOP.REQ.014	Location Requirements	Maps to support Drag & Drop functionality of various sensors at any given point of time		
IOP.REQ.015	Location Requirements	Map functionality to provide search options on basis of events, sensors, time etc.,		
IOP.REQ.016	Location Requirements	GIS to support addition/removal of sensors/ systems on need based		
IOP.REQ.017	Location Requirements	Map to support event based response actions for decision making in case of any emergency / critical situation		
IOP.REQ.018	Location Requirements	GIS based application to support Role based authentication for effective management of the system		
IOP.REQ.019	Realtime Requirements	CCTV feeds to be viewed on the Map in case of any event triggers		
IOP.REQ.020	Realtime Requirements	System to provide instant threat/event management based on the triggers generated		
IOP.REQ.021	Realtime Requirements	The system shall provide view and availability of various systems/ sensors on the map at any given time		
IOP.REQ.022	Realtime Requirements	The system shall facilitate communication between various agencies and personnel to address the situations		
IOP.REQ.023	Realtime Requirements	The System shall support tracking of realtime devices integrated		
IOP.REQ.024	Realtime Requirements	The system shall trigger alerts for any of the sensors/ applications		
IOP.REQ.025	Incident Response	The system shall facilitate setting the priority of the event and enable triggering the incidents automatically		
IOP.REQ.026	Incident Response	The system shall allow setting up multiple triggering rules per incident type		
IOP.REQ.027	Incident Response	The system shall enable associating response procedures to incident types. The associated procedures should be available for selection to operators upon manual incident creation.		

<b>Integrated Operation Platform (IOP)</b>				
<b>Sr. No.</b>	<b>Item</b>	<b>Minimum Requirement Description</b>	<b>Compliance (Yes / No)</b>	<b>Deviations / Remarks</b>
IOP.REQ.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.REQ.029	Post Incident Requirement	Shall have an event reconstruction functionality to give a complete overview of the synchronous events in the timeframe		
IOP.REQ.030	Post Incident Requirement	Shall provide a facility to export all the event scenario as a playable media file		
IOP.REQ.031	Post Incident Requirement	System shall support sorting and filtering the list of incidents		
IOP.REQ.032	Assets Management	The system should present the operator with a logical tree that contains devices from different types		
IOP.REQ.033	Assets Management	The system shall allow searching the device tree by device name or device type		
IOP.REQ.034	Assets Management	The system shall indicate the device type by an icon		
IOP.REQ.035	Assets Management	The system should display a pop-up for a device with its details		
IOP.REQ.036	Health Management	The 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.REQ.037	Web Intelligence	The system should have a tool for monitoring websites and social networks for topics of interest over time such that it should monitor new information on a variety of requirements from multiple sources in one platform.		
IOP.REQ.038	Web Intelligence	The system should allow defining the customized requirements such that it should set the data sources to follow, assert the Intelligence as customized queries, and build an ontology which is a knowledge representation of the subject-matter under investigation.		
IOP.REQ.039	Web Intelligence	The system should visit the sites on pre-defined schedule and should be able to log-in to the sites if needed, given proper credentials.		
IOP.REQ.040	Web Intelligence	The system should allow Incoming data to be processed, analyzed, filtered and matched against the defined requirements		

<b>Integrated Operation Platform (IOP)</b>				
<b>Sr. No.</b>	<b>Item</b>	<b>Minimum Requirement Description</b>	<b>Compliance (Yes / No)</b>	<b>Deviations / Remarks</b>
IOP.REQ.041	Web Intelligence	The system should have an external module gleaning data off the web, and should be able to send it through a unidirectional data-diode to internal system for processing. The system should separates the user system from the external network by securing the user from the risks associated with open networks		
IOP.REQ.042	Web Intelligence	It should allow all the data in the system to be accessible by role based mechanism		
IOP.REQ.043	Web Intelligence	The system should have Semantic support mechanism such that the system should build around Semantic-Technologies, harnessing the power of the semantic web for making sense of big data, transforming data to intelligence		
IOP.REQ.044	Web Intelligence	The system should be used to integrate data from existing databases, and also data gathered from the web about entities like people, organizations, groups, concepts etc. as well as the relationships between them.		
IOP.REQ.045	Web Intelligence	It should also provide entity recognition and disambiguation based on the ontology.		
IOP.REQ.046	Web Intelligence	The 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.REQ.047	Web Intelligence	The system should be able to correlate the external data (structured and unstructured) with internal data from multiple internal databases into a coherent ontology acting as a graph database		
IOP.REQ.048	Web Intelligence	The system should be able to search across data from different silos, across many data types (new items, blog postings, people, tweets, and more)		
<b>Indicative MIS Reports – “Smart Strip” – Smart Transport &amp; ICT enabled Solid Waste Management</b>				
MIS.REQ.001	General Requirement	Stops skipped.		
MIS.REQ.002	General Requirement	Speed violation, Harsh braking, Harsh Acceleration.		
MIS.REQ.003	General Requirement	Driver duty performance daily/weekly/monthly.		
MIS.REQ.004	General Requirement	Driver wise improper stopping.		

<b>Integrated Operation Platform (IOP)</b>				
<b>Sr. No.</b>	<b>Item</b>	<b>Minimum Requirement Description</b>	<b>Compliance (Yes / No)</b>	<b>Deviations / Remarks</b>
MIS.REQ.005	General Requirement	Details of Missed trips.		
MIS.REQ.006	General Requirement	On-going dynamic analysis from archived data for operating and strategic decisions through summarized reports and graphic representation.		
MIS.REQ.007	General Requirement	Position of the particular vehicle at any given point of time mapped to the land mark location, area, bus stop, etc.		
MIS.REQ.008	General Requirement	Tracking the complete route taken by particular vehicle on time scale		
MIS.REQ.009	General Requirement	Route specific distance travelled by a bus on a given date & time		
MIS.REQ.010	General Requirement	Monitor start time of the trip, completion of the trip, number of trip(s) completed, etc		
MIS.REQ.011	General Requirement	Monitor in-shedding /out-shedding of buses from depot automatically without human intervention.		
MIS.REQ.012	General Requirement	Time taken to complete a trip by specific bus, route based, within specified time slots in a day		
MIS.REQ.013	General Requirement	Deviations taken by the specific bus during the duty / trip related to routes, stoppages at bus stops, over speeding, distance travelled between stops within specific time, etc		
MIS.REQ.014	General Requirement	Bus operations specific (Inter state, inter city operations) reports		
MIS.REQ.015	General Requirement	Position of the vehicle at any point of time and the complete route taken by the vehicle along with the time scale.		
MIS.REQ.016	General Requirement	Route wise, time period wise, bus wise, driver wise, conductor wise, trip wise, exception reports (e.g. speed over limit incidents, route diversion incidents).		
MIS.REQ.017	General Requirement	Category of bus wise, route wise, time period of the day wise, bus wise, trip wise, duty wise scheduled / actual distance travelled on the time scale, summary as well as detailed reports along-with exceptions (e.g. actual distance travelled due to route diversion because of traffic jams, etc). Category of bus wise, depot wise, route wise, time period of the day wise, trip wise, duty wise actual fuel and oil consumption, summary as well as detailed reports if this information is available on the bus.		

<b>Integrated Operation Platform (IOP)</b>				
<b>Sr. No.</b>	<b>Item</b>	<b>Minimum Requirement Description</b>	<b>Compliance (Yes / No)</b>	<b>Deviations / Remarks</b>
MIS.REQ.018	General Requirement	Category of bus wise, depot wise, route wise, time period of the day wise, trip wise, duty wise, bus stop wise/ location wise actual passenger flow pattern, summary as well as detailed reports.		
MIS.REQ.019	General Requirement	Category of bus wise, depot wise, route wise, time period of the day wise, bus stop wise/ location wise scheduled / actual number of buses, summary reports along-with exceptions like cancellation of buses, route diversions due to road works, etc.		
MIS.REQ.020	General Requirement	Query based reports, as per the user requirements		
MIS.REQ.021	General Requirement	VTS wise data transfer logs on time scale and with date & time stamps		
MIS.REQ.022	General Requirement	Data logs for PIS unit wise information distributed to various locations.		
<b>Indicative Analytics &amp; Decision Support System – “Smart Strip” – Smart Transport &amp; ICT enabled Solid Waste Management</b>				
ADSS.REQ.001	General Requirement	Average peak and lean demand in passenger load during various times of a typical day (non-seasonal).		
ADSS.REQ.002	General Requirement	Average peak and lean demand in passenger load during various times of a Special day (seasonal).		
ADSS.REQ.003	General Requirement	Peak and lean revenue collections during various times of a typical day (non-seasonal).		
ADSS.REQ.004	General Requirement	Peak and lean revenue collections during various times of a special day (Seasonal).		
ADSS.REQ.005	General Requirement	Average peak and lean time from start to destination of a route during various times of the day.		
ADSS.REQ.006	General Requirement	Peak and lean bus-stop utilization rate – no. of passengers boarding at different bus stops enroute		
ADSS.REQ.007	General Requirement	Route planner / optimizer system shall incorporate: <ul style="list-style-type: none"> <li>• Route planning, scheduling and analysis</li> <li>• Real time scheduling and routing of buses</li> <li>• Demographic analysis and route restructuring</li> <li>• Transportation planning &amp; modelling</li> </ul>		

<b>Integrated Operation Platform (IOP)</b>				
<b>Sr. No.</b>	<b>Item</b>	<b>Minimum Requirement Description</b>	<b>Compliance (Yes / No)</b>	<b>Deviations / Remarks</b>
ADSS.REQ.008	Map Based Analysis	Creating buffers along the emergency site, working site etc.		
ADSS.REQ.009	Map Based Analysis	Creating Geo-fence Dynamically and sending alerts in case of vehicle moves out of the geo fence.		
ADSS.REQ.010	Map Based Analysis	Halt time within the geo-fences.		
ADSS.REQ.011	Map Based Analysis	Geofences to be created at every bus stop location.		
ADSS.REQ.012	Map Based Analysis	Geo routing the assigned routes and sending alerts in case of route deviation.		
ADSS.REQ.013	Map Based Analysis	The Map shall have facility to flash or show messages sent by the vehicle communication unit.		

<b>42U Rack</b>				
<b>Sr. No.</b>	<b>Item</b>	<b>Minimum Requirement Description</b>	<b>Compliance (Yes / No)</b>	<b>Deviations / Remarks</b>
RACK.REQ.001	Form Factor / Dimension	42U (600x1000)		
RACK.REQ.002	Material	Aluminium		
RACK.REQ.003	Cooling	Provision for heat dissipation for side-to-side and Front-to-Back units		
RACK.REQ.004	Cable Entry	Top and Bottom gland cable Entry trays with brush		
RACK.REQ.005	Side Panels	Full Side Panels for both sides		
RACK.REQ.006	Front Door	Front door with latch and ventilation holes.		
RACK.REQ.007	Back Door	Back door with latch and ventilation holes.		
RACK.REQ.008	PDU	2* Dual 32 A PDU		
RACK.REQ.009	Power Outlets	2* 16 receptacle Power Connectors each connected to separate PDUs		
RACK.REQ.010	Extra Units	Keyboard Drawer, 2x fixed tray		
RACK.REQ.011	Mounting Accessories	Nuts and washers for mounting equipment and slides.		
RACK.REQ.012	Cable Managers	Adequate cable managers for units.		
RACK.REQ.013	Depth Support	4 * Depth Support channels		
RACK.REQ.014	Support	The rack should not be an end of life / end of service product.		

RFP for Selection of System Integrator for Implementation of Nagpur Smart City Solutions

UPS				
Sr. No.	Item	Minimum Requirement Description	Compliance (Yes / No)	Deviations / Remarks
UPS.REQ.001	Capacity	5KVA, 10 KVA, and 20 KVA		
UPS.REQ.002	Technology	True ONLINE (Double Conversion) PWM technology using IGBTs for switching at high frequency (>15 KHz)		
UPS.REQ.003	Connector	SNMP Connectivity		
UPS.REQ.004	Electrical Input	Single Phase, 230 V AC with an option to select three phase		
UPS.REQ.005	Electrical Input	Voltage Range 155 – 280 V on Full Load Voltage Range 110 – 280 V on less than 70% Load		
UPS.REQ.006	Electrical Input	Frequency Range 45 – 55 Hz		
UPS.REQ.007	Electrical Input	Efficiency AC to AC: > 85% (AC to AC)		
UPS.REQ.008	Electrical Output	230V AC		
UPS.REQ.009	Electrical Output	Frequency: 50 Hz + 0.25Hz (free running); + 2Hz (sync mode)		
UPS.REQ.010	Electrical Output	Voltage Regulation: +1% on mains/batteries		
UPS.REQ.011	Electrical Output	Overload Capacity: 125% for 5 min., 110% for 10 mins.		
UPS.REQ.012	Electrical Output	Waveform; Pure Sine wave		
UPS.REQ.013	Protection	Electronic Overload Sensing, and circuit breaker protection.		
UPS.REQ.014	Protection	Overheating, Output short circuit, low battery, input over/under voltage etc.		
UPS.REQ.015	Battery Type	Sealed Maintenance Free Battery, Mains & Battery with necessary indicators, alarms and protection with proper battery storage stand		
UPS.REQ.016	Backup Time	Minimum 2 hour backup on rated load		
UPS.REQ.017	DC Voltage	MIN. : 240 V		



UPS				
Sr. No.	Item	Minimum Requirement Description	Compliance (Yes / No)	Deviations / Remarks
UPS.REQ.018	Charging Features	Adjusted to about 10% of battery capacity for fast charging. 1. Boost/trickle charging facility 2. Uncontrolled rectifier with high efficiency and reliability. 3. Low battery protection to avoid deep discharging of batteries. 4. Self-test diagnostic feature		
UPS.REQ.019	Other Features	UPS Bypass Automatic on Overload or UPS Failure		
UPS.REQ.020	Other Features	Monitoring panel with LCD display to provide following information:- 1. Input/output voltage 2. Input/output frequency 3. Load current 4. Charging current LED display for: - UPS on, battery operation, bypass, alarm battery charge level, etc. Alarms for :- Mains failure, low battery, overload etc.		
UPS.REQ.021	Other Features	RS 232 Standard Interface port in conjunction with UPS monitoring software provides information about UPS health, status, battery backup etc.		
UPS.REQ.022	Environmental	Temperature 0-40°C operating, 0 to + 60° C		
UPS.REQ.023	Environmental	Humidity 0 – 95% RH non-condensing		
UPS.REQ.024	Environmental	Audible noise < 50 dB (A)		
UPS.REQ.025	Mandatory Compliance	Safety certified to IEC standards or as per applicable in Indian law		
UPS.REQ.026	Mandatory Compliance	EMC certified to IEC standards.		
UPS.REQ.027	Mandatory Compliance	ISO 9001:2000 and ISO 14001 certified ETDC/ERTL test reports for above specifications.		

RFP for Selection of System Integrator for Implementation of Nagpur Smart City Solutions

UPS				
Sr. No.	Item	Minimum Requirement Description	Compliance (Yes / No)	Deviations / Remarks
UPS.REQ.028	Mandatory Compliance	Dimension Light Weight/Smaller Footprint		

Field UPS				
Sr. No.	Item	Minimum Requirement Description	Compliance (Yes / No)	Deviations / Remarks
UPS1.REQ.001	Capacity	1 KVA		
UPS1.REQ.002	Input Range	Voltage Range 155-280 V on Full Load Voltage Range 110-280 V on Less than 70% Load Frequency 50 HZ $\pm$ 3 HZ		
UPS1.REQ.003	Output Voltage & Waveform	220V AC/ 230V AC/ 240V AC (Selectable)		
UPS1.REQ.004	I/P & O/P Power Factor	0.9 or higher power factor		
UPS1.REQ.005	Mains & Battery	Sealed Lead Maintenance Free VRLA type (Lead Calcium SMF batteries NOT acceptable), Mains & Battery with necessary indicators, alarms and protection with proper battery storage stand		
UPS1.REQ.006	Frequency	50 Hz $\pm$ 0.5% (free running), Pure Sine wave		
UPS1.REQ.007	Crest Factor	min. 3:1		
UPS1.REQ.008	Third Harmonic Distribution	< 3%		
UPS1.REQ.009	Input Harmonic Level	< 10%		
UPS1.REQ.010	Overall Efficiency	Min. 90% on Full Load;		
UPS1.REQ.011	Noise Level	< 55 db @ 1 Meter		
UPS1.REQ.012	Backup	at least 240 minutes (4 hours / VAH)		
UPS1.REQ.013	Warranty	3 years with UPS & battery		
UPS1.REQ.014	Certification	ISO 9001:2008 & ISO 14001 certified		
UPS1.REQ.015	Protection	To be provided for overload/ short circuit; over heating; input over/ under voltage; output over/ under voltage.		
UPS1.REQ.016	Alarms & Indications	All necessary alarms & indications essential for performance monitoring of UPS like mains fail, low battery & fault detection		
UPS1.REQ.017	Interface	SNMP interface support (for remote monitoring)		

<b>Field UPS</b>				
<b>Sr. No.</b>	<b>Item</b>	<b>Minimum Requirement Description</b>	<b>Compliance (Yes / No)</b>	<b>Deviations / Remarks</b>
UPS1.REQ.018	Galvanic Isolation	To be provided through Inbuilt transformer		
UPS1.REQ.019	Compatibility	UPS to be compatible with DG Set supply and mains supply		
UPS1.REQ.020	Bypass	Automatic Bypass Switch		
UPS1.REQ.021	Technology	True ON-LINE (Double Conversion) with IGBT based inverter and PWM Technology		
UPS1.REQ.022	Support	The system should not be an end of life / end of service product.		
UPS1.REQ.023	Operating Temperature	0 to 55 Degrees Centigrade		

<b>SAN Switch</b>				
<b>Sr. No.</b>	<b>Item</b>	<b>Minimum Requirement Description</b>	<b>Compliance (Yes / No)</b>	<b>Deviations / Remarks</b>
SANS.REQ.001	Power Specification	200-240V, 50-60 Hz		
SANS.REQ.002	Operating temperature range	0° to 40° C		
SANS.REQ.003	Operating Relative Humidity range (non-condensing)	10 to 90% relative humidity		
SANS.REQ.004	Total no. of ports on the proposed switch	24		
SANS.REQ.005	Throughput of each FC port	8/16Gbps		
SANS.REQ.006	Support for 4/8/16 Gb/s HBAs	YES		
<b>Protocol Supported</b>				
SANS.REQ.007	FC	Yes		
SANS.REQ.008	FCP	Yes		
SANS.REQ.009	FC-AL	Yes		
SANS.REQ.010	Designed for high availability with no Single Point of Failure	YES		
<b>Power Supply</b>				
SANS.REQ.011	Hot Swappable Power supply proposed	YES		
SANS.REQ.012	(N+1) redundant power supply proposed	YES		

<b>SAN Switch</b>				
<b>Sr. No.</b>	<b>Item</b>	<b>Minimum Requirement Description</b>	<b>Compliance (Yes / No)</b>	<b>Deviations / Remarks</b>
<b>Cooling Fans</b>				
SANS.REQ.013	Hot Swappable Cooling Fans proposed	YES		
SANS.REQ.014	(N+1) redundant Cooling Fans proposed	YES		
SANS.REQ.015	Capability for streaming the data in multiple paths with Optimization algorithms for streaming data through shortest available path.	YES		
SANS.REQ.016	Capabilities for cascading of switches	YES		
SANS.REQ.017	Non-disruptive firmware update	YES		
SANS.REQ.018	End to end performance monitoring	YES		
SANS.REQ.019	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.	YES		
<b>Zoning and security</b>				
SANS.REQ.020	Support for hardware -enforced zoning	YES		
SANS.REQ.021	Policy based security and centralised fabric management	YES		
SANS.REQ.022	Support for Encrypted password	YES		
SANS.REQ.023	Support for PKI Digital certificates	YES		
SANS.REQ.024	Support for FCAP authentication	YES		
SANS.REQ.025	Support for RADIUS, SSL / HTTPS, SSH, SNMP V3	YES		
SANS.REQ.026	Support for LUN masking	YES		
<b>Support for Hardware based trunking</b>				
SANS.REQ.027	Compatability with proposed network devices	Yes		
SANS.REQ.028	Compatability with proposed servers	Yes		
SANS.REQ.029	The system should not be an end of life / end of service product.	Yes		



<b>Desktop</b>				
<b>Sr. No.</b>	<b>Item</b>	<b>Minimum Requirement Description</b>	<b>Compliance (Yes / No)</b>	<b>Deviations / Remarks</b>
DSK.REQ.001	Processor	Intel Core i5 , 64bit x86 Processor @ 3.2 GHz or more,4MB L3 cache, Memory support DDR3 or better specifications		
DSK.REQ.002	Motherboard & Chipset	OEM Motherboard		
DSK.REQ.003	Video	Integrated Graphic controller		
DSK.REQ.004	Network	Integrated 10/100/1000 Gigabit Ethernet controller		
DSK.REQ.005	Ports	1 HDMI port (Preferable), 2x USB 2.0 and 2 x USB 3.0 (Preferable) , 10 USB ports external - with minimum 4 ports USB 3.0 Front I/O includes (2 or more ) USB 2.0 ports Rear I/O includes (2 or more ) USB 3.0 ports, (2 or more) USB 2.0 ports, serial port, Parallel port, PS/2 mouse and keyboard ports, RJ-45 network interface, DisplayPort 1 VGA and 3.5mm audio in/out jacks; 4 in 1 Media Card Reader (Preferable)		
DSK.REQ.006	HDD Controller	Integrated dual port SATA-II controller		
DSK.REQ.007	Memory	16GB DDR III 1333MHz or higher		
DSK.REQ.008	Storage	1TB @ HDD 7200 RPM		
DSK.REQ.009	Optical Drive	22X DVD writer or higher and the corresponding software		
DSK.REQ.010	Monitor	21" TFT LCD monitor minimum 1920 x 1080 resolution with 5 ms response time or better specifications, TCO 03 or higher certified		
DSK.REQ.011	Keyboard	107 or more Keys Keyboard		
DSK.REQ.012	Mouse	2 / 3 button USB Optical Scroll Mouse with anti-static mouse pad resolution of Optical 1000 cpi, Complying to CE and FCC norms		
DSK.REQ.013	Power Management and DMI	System with Power management features & Desktop Management Interface implementation		
DSK.REQ.014	Operating System	Windows desktop latest version		
DSK.REQ.015	Power input	100 -240V AC		



<b>Ruggedized Laptop</b>				
<b>Sr. No.</b>	<b>Item</b>	<b>Minimum Requirement Description</b>	<b>Compliance (Yes / No)</b>	<b>Deviations / Remarks</b>
RUL.REQ.001	Processor	Intel i5 processor or better		
RUL.REQ.002	Motherboard	OEM Motherbord and chipset		
RUL.REQ.003	Memory	4GB DDR3 SDRAM		
RUL.REQ.004	HDD	500 GB		
RUL.REQ.005	Display	14" or better display. The display should be visible in sunlight		
RUL.REQ.006	Interfaces	<ul style="list-style-type: none"> <li>• Serial RS232C</li> <li>• VGA port</li> <li>• Audio In/out</li> <li>• USB 2.0</li> <li>• LAN</li> <li>• Firewire IEEE1394a</li> </ul>		
RUL.REQ.007	Connectivity	<ul style="list-style-type: none"> <li>• Bluetooth 4.0</li> <li>• Wireless LAN 802.11 a/b/g/n compliant</li> <li>• LAN - 1000BaseT/ 100BaseT-Tx/ 10BaseT</li> <li>• 3G connectivity</li> </ul>		
RUL.REQ.008	Power	AC Adaptor, 10 hours battery Backup		
RUL.REQ.009	Operating System	Windows latest version		
RUL.REQ.010	Ruggedness	<ul style="list-style-type: none"> <li>• Water resistance test: IEC529 (JIS C0920) IPX54,</li> <li>• MIL-STD 810G 506.5 4</li> <li>• Dust resistance test: IEC529 (JIS C0920) IP6X4,</li> <li>• MIL-STD 810G 510.5 4</li> <li>• Gravity drop resistance test: MIL-STD 810G 516.6 4</li> <li>• Vibration resistance test: MIL-STD 810G 514.6 4</li> </ul>		
RUL.REQ.011	Security features	TPM (TCG V1.2 compliant), Integrated hardware security lock slot, Password security (supervisor password, user password)		



<b>Laser Jet Printer</b>				
<b>Sr. No.</b>	<b>Item</b>	<b>Minimum Requirement Description</b>	<b>Compliance (Yes / No)</b>	<b>Deviations / Remarks</b>
LJN.REQ.001	Print speed, black	30 ppm or more		
LJN.REQ.002	Print resolution, black	1200 x 600 x 2 dpi or more		
LJN.REQ.003	Print technology	Laser		
LJN.REQ.004	Monthly duty cycle	8000 pages or more		
LJN.REQ.005	Memory, standard	32 MB or higher		
LJN.REQ.006	Print languages, standard	Host-based printing, PCL 5e		
LJN.REQ.007	Duplex printing (printing on both sides of paper)	Automatic (standard)		
LJN.REQ.008	Media sizes, standard	A4 , letter		
LJN.REQ.009	Media sizes, custom	250-sheet input tray: 5.8 x 8.27 to 8.5 x 14 in; priority feed slot: 3 x 5 to 8.5 x 14 in preferable		
LJN.REQ.010	Network ready	Standard (built-in Ethernet)		
LJN.REQ.011	ENERGY STAR® Qualified	Yes		
LJN.REQ.012	<b>Warranty Coverage</b>	Comprehensive warranty for 5 years.		

RFP for Selection of System Integrator for Implementation of Nagpur Smart City Solutions

<b>Multifunction Device</b>				
<b>Sr. No.</b>	<b>Item</b>	<b>Minimum Requirement Description</b>	<b>Compliance (Yes / No)</b>	<b>Deviations / Remarks</b>
<b>Printer Specifications</b>				
LJM.REQ.001	Print speed, Color	18 ppm or more		
LJM.REQ.002	Print resolution, Color	Up to 600 x 600 dpi		
LJM.REQ.003	Print technology	Laser		
LJM.REQ.004	Monthly duty cycle	8000 pages or more		
LJM.REQ.005	Memory, standard	32 MB or more		
LJM.REQ.006	Print languages, standard	Host-based printing, PCL 5e		
LJM.REQ.007	Duplex printing (printing on both sides of paper)	Manual (driver support)		
LJM.REQ.008	Media sizes, standard	A4, Letter		
LJM.REQ.009	Media sizes, custom	250-sheet input tray: 5.8 x 8.27 to 8.5 x 14 in; priority feed slot: 3 x 5 to 8.5 x 14 in		
<b>Scanner Specifications</b>				
LJM.REQ.010	Scanner type	Flatbed, ADF		
LJM.REQ.011	Scan resolution, optical	1200 dpi or more		
LJM.REQ.012	Scan size	8.5 x 11.7 in		
LJM.REQ.013	Scan speed	6ppm or above		
LJM.REQ.014	Supported file formats	PDF; TIF; BMP; GIF; JPG		
<b>Copier Specifications</b>				
LJM.REQ.015	Copy resolution	600x 400 dpi or more		
<b>Fax Specifications</b>				
LJM.REQ.016	Auto redial	Yes		
LJM.REQ.017	Fax delayed sending	Yes		
<b>Other Specifications</b>				
LJM.REQ.018	Network ready	Standard (built-in Ethernet)		
LJM.REQ.019	ENERGY STAR® Qualified	Yes		
LJM.REQ.020	Warranty Coverage	Comprehensive warranty for 3 years.		

<b>Hekpdesk</b>				
<b>Sr. No.</b>	<b>Category</b>	<b>Minimum Requirement Description</b>	<b>Compliance (Yes / No)</b>	<b>Deviations / Remarks</b>
<b>Automatic Call Distribution (ACD)</b>				
REQ.001	General Requirement	Routing of the calls to available agent would be done by ACD.		
REQ.002	General Requirement	ACD would employ a rule based routing strategy		
REQ.003	General Requirement	ACD should be able to identify available agents and transfer the call accordingly		
REQ.004	General Requirement	Call routing to the agents based on the “longest idle basis”		
REQ.005	General Requirement	ACD shall seamlessly integrate with IP PBX system		
REQ.006	General Requirement	When a call is transferred to the IP phone then the call details should also be simultaneously transferred to CAD software in a pre-defined format.		
<b>Call Telephony Integration (CTI)</b>				
REQ.007	General Requirement	Allow interaction between telephone and a computer to be integrated or coordinated.		
REQ.008	General Requirement	Shall act as a common interface for integration of all the software applications deployed.		
REQ.009	General Requirement	Shall support relevant screen pop-ups on the agents’ screen on the basis of call location detection		
REQ.010	General Requirement	Shall pass events & information of agents’ status & changes in agent status as well as incoming calls to the computer applications		
<b>Interactive Voice Recording System (IVRS)</b>				
REQ.0011	General Requirement	Shall help caller in interaction with voice and DTMF (Dual tone multi-frequency signalling) via keypad. Through the IVRS system, caller would easily be able to direct the concern to appropriate agent at the helpdesk		

<b>Hekpdesk</b>				
<b>Sr. No.</b>	<b>Category</b>	<b>Minimum Requirement Description</b>	<b>Compliance (Yes / No)</b>	<b>Deviation s / Remarks</b>
REQ.0012	General Requirement	IVRS shall be able to queue the calls and provide position number in queue and approximate time to reach agent		
REQ.0013	General Requirement	Shall support English, Hindi and Marathi languages		
<b>IP PBX</b>				
REQ.014	General Requirement	IP PBX software allows transferring calls received on PRI lines to the IP network.		
REQ.015	General Requirement	IP PBX shall ring the IP phone of the identified agent		
REQ.016	General Requirement	Provision to broadcast "Greeting Message" whenever a call is received on the system		

<b>IP Phone</b>				
<b>Sr. No.</b>	<b>Item</b>	<b>Minimum Requirement Description</b>	<b>Compliance (Yes / No)</b>	<b>Deviations / Remarks</b>
IPP.REQ.006	General Requirement	The IP Phone shall have LED/LCD Indicator for Call Waiting and Message Waiting.		
IPP.REQ.007	General Requirement	The IP Phone shall support Dynamic Host Configuration Protocol (DHCP) based as well as statically configured IP address assignment.		
IPP.REQ.008	General Requirement	The IP Phone shall have minimum 2.5"X2.0", high resolution graphical grayscale LCD display.		
IPP.REQ.009	General Requirement	It shall be possible to create Local Phone book with at least 50 contacts as well as pull information from the directory (Integration with directory like Active directory Contact details etc.).		
IPP.REQ.010	General Requirement	The IP phones shall support industry standard audio codec viz. G.711 (A-law and Mu-law), G.729 (including G.729 A and G.729 B), G.722 audio codec.		
IPP.REQ.011	General Requirement	The IP Phone shall support Voice Activity Detection, Silence Suppression and Echo Cancellation.		
IPP.REQ.012	General Requirement	The display shall provide features such as Date and Time, Calling Party Number and Digits Dialed.		
IPP.REQ.013	General Requirement	IP phones shall be able to work on SIP/H.323 protocols.		
IPP.REQ.014	General Requirement	There shall be provision to provide electrical power to the IP phones either through power adapter or via PoE (IEEE 802.3af) enabled Ethernet port.		
IPP.REQ.015	General Requirement	The IP phones shall support for POE Class 1 or POE Class 2		
IPP.REQ.016	General Requirement	The Phones shall have configurable Abbreviated Dial & Speed Dial.		
IPP.REQ.017	General Requirement	The firmware of IP phones shall be upgradable using HTTPS or FTP or TFTP or SFTP.		

IP Phone				
Sr. No.	Item	Minimum Requirement Description	Compliance (Yes / No)	Deviations / Remarks
IPP.REQ.018	General Requirement	It shall be possible to view call history for at least last 10 missed calls, 10 dialled calls and 10 received calls for each call taker desk.		
IPP.REQ.019	General Requirement	It shall be possible to set preferences such as Display Contrast and Ring Types.		
IPP.REQ.020	General Requirement	The IP Phones shall be SNMP manageable (SNMP v1, SNMP v2c and/or SNMPv3 protocols) directly or through the PBX server. IP Phones or PBX server shall be able to send IP phone related SNMP traps to the configured Network Management System (NMS). Bidder shall provide generic as well as vendor/OEM specific SNMP MIBs of the equipment for monitoring/management through standard NMS systems along with the equipment.		
IPP.REQ.021	Features	Mobile-Phone style menu with access to most often used features like call forwarding, Park, Settings etc. On screen status indication for activated features like call forwarding		
IPP.REQ.022	Message Indicator	Waiting	Used as ringing call alert indicator	
IPP.REQ.023	Mounting		Desk or wall mountable with optional wall mount adapter.	

## 5. ANNEXURES:

### ANNEXURE I: Indicative list of City WiFi locations

#	INDICATIVE LIST OF CITY WIFI LOCATION
1	Aath Rasta Square
2	Abhyankar Nagar Bus Stop
3	Additional
4	Agayaramdevi Sq.
5	Ajani Railway Station
6	Ajni Square
7	Alankar Talkies Square
8	Ambazari Overflow point
9	Anand Theatre
10	Awasti Nagar
11	Bajaj Nagar Square statue
12	Bal Jagat
13	Balbhawan
14	Bande Plot Chowk
15	Bharat Nagar Square
16	Bharatwada Hotspot
17	Bhauji Page Udyan
18	Bhole Petrol Pump Chowk
19	Borgaon square
20	Cotton Market Square
21	Dattatray Nagar Garden
22	Deputy Signal Bazar Chowk
23	Dhantoli Garden
24	Diagonally oopt to statue
25	Friends colony
26	G. T. Padole Hospital
27	Gaddigodam Bus Stop
28	Gangabai Ghat Sq

#	INDICATIVE LIST OF CITY WIFI LOCATION
29	Gittikhadan square
30	Gorewada square
31	HB Town area
32	Hingana TPoint
33	Hislop College Square
34	Hotel Ashoka Square
35	Inox Centre
36	INOX Centre
37	Jafar Nagar
38	Jagnade square
39	Jaitala Road
40	Jaripatka
41	Jhansi Rani Square
42	Kadbi Square
43	LAD Square Bus Stop
44	Law College Square
45	Laxmi Bhavan Chowk
46	Laxmi Nagar Square
47	LIC Square Lic building
48	Lokmat Sq.
49	Mahalgi Square
50	Maharaja Bagh
51	Manewada Square
52	Mangalwari zone
53	Mankapur square
54	Mate Square
55	Morris College T Point
56	Nagpur University
57	Nandanvan BoB
58	Narendra nagar railway bridge
59	Nasare Sabhaghru



#	INDICATIVE LIST OF CITY WIFI LOCATION
60	Near Chamat flour Mill
61	Near NIT chairman's bungalow
62	Omkar Nagar Square
63	Phutala Lake
64	Prashant Nagar
65	Pratap Nagar Chowk
66	Raj Nagar
67	Rajiv Gandhi Udyan
68	Ravi Nagar Chowk
69	Sadar Gandhi Square
70	Sai Mandir
71	Sakardhara Chowk
72	Santh Eknath Dwar Chowk Sunil hotel
73	Santra Orange Market
74	Satabdi Square
75	Shankar Nagar Square
76	Sharda Square
77	Shri Guru Ramdasji Gurudwara
78	Somalwada Square
79	ST Bus Stop
80	Swami Narayan Mandir
81	Towards laxmi bhavan square
82	Variety Sq.
83	Vayusena nagar KV
84	Yashwantrao Chavan Stadium
85	All NMC Offices
86	Key Government Offices (Nagpur) including Collector Office, Zila Parishad office and others in Civil Lines area

**ANNEXURE II: Indicative List of City Surveillance Locations**

Sl.No.	Name of Police Station	LOCATION	CCTV CAMER A PTZ	CCTV CAMER A Fixed
<b>List of Critical Locations</b>				
1.	Sitabuldi	Senetorium Hall	1	2
2.		Building near Matruseva Sangh	2	3
3.		Open place near M.P.Bus Stand	1	2
4.		Morbhavan bas stand	1	2
5.		Opposite to old Mores college	1	2
6.		Canal Road	1	2
7.	Ambazari	Futala lake open place	1	2
8.		Forest area opposite site to Vayusena nagar	2	3
9.		Ambazari Talav area	2	3
10.		Campus	2	3
11.		Telankhadi Garden openplace	1	2
12.	MIDC	Esasni Area	2	3
13.		Waghdhara Area,	2	3
14.		Building near to Masukshaha Dargah	1	2
15.	Wadi	Quarters on Nipani-Sonegaon Road	2	3
16.		Defence Area	2	3
17.		Khadgaon Road	1	2
18.	Sonegaon	In MihanArea – Khapri, Telhara, Kalkuti, Dahegaon, Panjri, Persodi,	2	3
19.		Outer ring road area, Shivangaon area, Sonegaon Talav and open place near to Talav.	3	5
20.	RP Nagar	Hingna Tea point area	1	3
21.		Jaytala area	2	3
22.	Sadar	Opposite to C.P. Club	1	2

Sl.No.	Name of Police Station	LOCATION	CCTV CAMER A PTZ	CCTV CAMER A Fixed
23.		Opposite to St. John School	1	2
24.		Aakar Building Area	1	2
25.	Panchapoli	Kolkata railway line east area,	1	2
26.		Thakkargram to Naik lake	1	2
27.	Jaripatka	Khasada vasti,	2	3
28.		Samta nagar area	2	3
29.		Near Paramid city	1	2
30.		Railway line on D.I. road	1	2
31.	Koradi	Bokhara to chakki Khapa road	1	2
32.		Lonara road	1	2
33.		Backside of koradi devi Mandir , Gaymukh building area	1	2
34.		Mankapur railway line area	1	2
35.	Gittikhadan	Dabha Area,	1	2
36.		Seminary Hill forest Area	2	3
37.		C.P.W. colony	2	3
38.		Opposite site of Telankhadi area- open place	1	2
39.		Hazaripahad area	2	3
40.		Gorawada area	2	3
41.	Tahasil	Railway colony guard line,Railway Banglow no. C-26, D-53,F-53 qrt. no.M-89, NMC school, Timki Primary Bengali school,Panja NMC school, Jagannath Budhawari,	3	5
42.	Lakadganj	Old Building near Ponam Mall, Old Hospital building in Queta colony.	2	3
43.	Ganeshpeeth	Maskasath NMC school.	1	2
44.		Empress Mill T-point	1	3

Sl.No.	Name of Police Station	LOCATION	CCTV CAMER A PTZ	CCTV CAMER A Fixed
45.		Backside of ST stand,	1	2
46.		Mokshdham Ghat,	1	4
47.		Underbridge near Vijay Talkies.	1	2
48.	Kotwali	Mhada Qrt.,Chikhali,Open palce Near Mittal Enclave,Near Cilypat company Kapsi Bujurg road, Nageshwar nagar area, Bharatwadi area, Wanjara vasti.	3	7
49.	Yashodhara	Behind Akash Relay Kendra Old building,Backside of Bhilgaon, Bhilgaon to Ranala road,	3	7
50.		Ajani railway qtr.,	1	3
51.	Ajani	Chintamani Nagar,	2	3
52.		Abhay nagar, Backside of medical college.	2	3
53.	Dhantoli	Gajanan railway line, Behind Central Jail.	2	3
54.	Sakkardara	Shyambagh area, Sindhiban, Bada Tajbagh, Chhota Tajbagh,	2	3
55.		Somwari Qrt., Old Qrt.of Vima Hospital.	1	4
56.	Imamwada	T.B. Ward Area	1	2
57.	Nandanvan	Bhande plot, BRO office,	1	2
58.		Darshan colony old building, Shrikrishna nagar old building,	1	2
59.		Sangharshnagar, Deshpande layout,	1	2
60.		Bhutbangala, empty building	1	2
61.		Hudkeshwar (Khurd),	2	3
62.		Kiranapur,Adyali village ,	2	3
63.	Hudkeshwar	Narsala,Kannad,	1	2
64.		Vihirgaon,Bhogali,Gotal,	2	3
65.		Panzari,Shankarpur,	1	2

Sl.N o.	Name of Police Station	LOCATION	CCTV CAMER A PTZ	CCTV CAMER A Fixed
66.		Besa,Beltarodi road.	1	2
	<b>ZONE 1</b>			
67.	Sitabuldi	Zasirani chowk	1	4
68.		Variety chowk	1	4
69.		RBI chowk	1	4
70.		Munje chowk	1	4
71.		Rahate chowk	1	4
72.		Jai Stambh chowk	1	4
73.		Manas chowk	1	4
74.		Akash Wani chowk	1	4
75.		Maharaj Bag chowk	1	4
76.		Board office square	1	4
77.		Panchshil square	1	4
78.		Canal Road Shri Ram bhavan square	1	4
79.		Mories college T Point	1	3
80.		Jaystambh square Railway station	1	4
81.		R.B.I square	1	4
82.		Akashwani square	1	4
83.		GPO square	1	4
84.		Moris T point	1	3
85.		Board office square	1	4
86.		RajaRani square	1	4
87.	MLA Hostel square	1	4	
88.	RBI Quarter square	1	4	
89.	Variety square	1	4	

Sl.N o.	Name of Police Station	LOCATION	CCTV CAMER A PTZ	CCTV CAMER A Fixed
90.		Maharaja Bagh square	1	4
91.		Bhole petrol square	1	4
92.		LAW College square	1	4
93.		Zashi Rani square	1	4
94.		University Library square	1	4
95.		Alankar talkies square	1	4
96.		Shankar Nagar square	1	4
97.		Y Point Children park	2	3
98.		Laximi Bhavan square	1	4
99.		Panchshil square	1	4
100.		Gyara Majali Building	1	2
101.		Lendra park T point	1	3
102.		Kachipura square	1	4
103.		Bajaj Nagar square	1	4
104.		Munje square	1	4
105.		Manas square	1	4
106.		Bardi Main market	2	3
107.	Ambazari	Ambazari T point	1	3
108.		juna amravati naka	1	4
109.		Ravi nagar square	1	4
110.		Futala lake y point	1	3
111.		Futala lake vadache jhad point	1	2
112.		Ram nagar square	1	4
113.		Shankar nagar square	1	4
114.		Bajaj nagar square	1	4

Sl.No.	Name of Police Station	LOCATION	CCTV CAMER A PTZ	CCTV CAMER A Fixed
115.		Laxmi bhawan square	1	4
116.		1 shradhanandpeth square	1	4
117.		LAD Squire	1	4
118.		Ledige club squire	1	4
119.		Law college	2	3
120.		coffe house squire	1	4
121.		laxmi bhavan squire	1	4
122.		Shankar nagar squire	1	4
123.		Bajaj nagar	2	3
124.		opp wockhart hospital	1	2
125.		Ambazari T point	1	3
126.		Ram Nagar squire	1	4
127.		Ravi nagar squire	1	4
128.		Bharat nagar T Point	1	3
129.		Campus squire	1	4
130.		Futala Talav	2	3
131.		Near Madrasi Mandir	1	2
132.		Pandharbodi	2	3
133.		Gokulpeth market	2	3
134.		Abhyankar Nagar Road	1	2
135.		Telankhedi Area	2	3
136.		Ambazari Bay Bas Road	1	2
137.		yashawant Nagar ground	2	3
138.		Shivaji Nagar Gardan	2	3
139.		Shivaji Nagar Basket ball ground	2	3

Sl.No.	Name of Police Station	LOCATION	CCTV CAMER A PTZ	CCTV CAMER A Fixed
140.		shubhas Nagar T Point	1	3
141.		Near carzy casal	1	2
142.	MIDC	Hingna Naka	1	4
143.		SRPF Gate No. 2	1	2
144.		Takli sim bodhvihar hingna road	1	4
145.		Mansi girls hostel hingna road	1	2
146.		Yashodhara nagar t point hingna road	1	3
147.		Gadge nagar t point hingna road	1	3
148.		SRPF Geat petrol pump bansi nagar hingna road	1	2
149.		Deshmukh treding company t point hingna road	1	3
150.		Sent zeviys school t point hingana road	1	3
151.		Balaji nagar bus stop t point hingana road	1	3
152.		Tractor company chowk hingana road	1	4
153.		SRPF geat no. 2 chowk hingana road	1	4
154.		Kalmegh nagar road t point hingana road	1	3
155.		CRPF gate t point hingana road	1	3
156.		Manglwari bazar parisar hingana road	2	3
157.		IC Chowk t point hingana road	1	3
158.		Takiywale baba dargaha hingana road	1	2
159.		Zone chowk hingana road	1	4
160.		Rajiv nagar road hingana road	1	2
161.		Karve girls hostel hingana road	1	2
162.	Ycce college main geat hingana road	1	2	
163.	Wanadongri t point	1	3	
164.	Wadi	Wadi T Point	1	3



Sl.No.	Name of Police Station	LOCATION	CCTV CAMER A PTZ	CCTV CAMER A Fixed
165.		Wadi Naka no 1NO	1	4
166.		Narayan nagar NHNO6	2	3
167.		Wadi Naka no 10	1	4
168.		Control Wadi	1	4
169.		Ramabai Square Control wadi	1	4
170.		MIDC Tarnign	1	2
171.		Katol Road BayPass	2	3
172.		KhadGaon Road tarnign	1	2
173.		Dattawadi Square	1	4
174.		Dattawadi Sarafa Bazar	2	3
175.		GuruDatta Socity	2	3
176.		PS Main Gate	1	2
177.		8 th Mail	1	2
178.		Ambedakar Nagar Square	1	4
179.		Davalamethi Road	1	2
180.		8 th Mial Market Road	1	2
181.		Lawa Gaon Square	1	4
182.		Ganesh Nagar Drugdhamna	1	2
183.		WadaDhamnaSquare	1	4
184.		Surabaldi Gaon Tranign	1	2
185.		WadaDhamna Godaun Aria	1	2
186.		HighLand Park Tarnig	1	2
187.		Narayan nagar NH06	2	3
188.		Khadgaon Road Tekadiwadi	1	2
189.		Dhammakirtinagar	2	3

Sl.N o.	Name of Police Station	LOCATION	CCTV CAMER A PTZ	CCTV CAMER A Fixed
190.	Sonegaon	Sawarkar Nagar chowk	1	4
191.		Khapri Naka	1	4
192.		Somalwada chowk	1	4
193.		Manish Nagar Railway	1	2
194.		Reliance Fresh	1	2
195.		Purshottam Bazar, Beltrodi	2	3
196.		Padmavati T – Point	1	3
197.		Chinch bhvan bus stop	1	2
198.		Sahkar Nagar	2	3
199.		Wardha road Rajiv Nagar Square	1	4
200.		Infront of Hotel Pride	1	2
201.		Somlwada Square	1	4
202.		Bhende layout Square	1	4
203.		RP Nagar	Trimurti chowk	1
204.	Sambhaji chowk		1	4
205.	Padole chowk		1	4
206.	Pratap Nagar chowk		1	4
207.	Coca Cola chowk		1	4
208.	Khamla maton market chowk		1	4
209.	Outer ring road		2	3
210.	Mokhare college		1	2
211.	Jaytala bazaar chowk		1	4
212.	Hingna T point		1	3
213.	Mangalmurti chowk		1	4
214.	Shubhash nagar T point		1	3

Sl.N o.	Name of Police Station	LOCATION	CCTV CAMER A PTZ	CCTV CAMER A Fixed
215.		Mate chowk	1	4
216.		Laxminagar chowk	1	4
217.		Athat Rasta chowk	2	8
218.		Jerlly lawn	2	3
219.		Savarkar nagar chowk	1	4
220.		Chatrapati nagar chowk	1	4
221.		Sneh nagar petrol pump	1	2
222.		Sneh nagar garden	2	3
223.		Pande layout pani tanki	1	2
224.		Gulmohar lawn	2	3
225.		Rammandir swavalambi nagar	1	2
226.		Survey nagar	2	3
227.		Nelco society	2	3
228.		Rpts road	1	2
229.		Jain mandir laxminagar	1	2
230.		Radhey mangalam gali	1	2
231.		Ganesh mandir taty tope nagar	1	2
232.		Pratap nagar durga mandir	1	2
233.		Aaji aajoba park	2	3
234.		Nit garden trimurti nagar	1	2
235.		Pratapnagr chowk	1	4
236.		Khamla market	2	3
<b>ZONE 2</b>				
237.	Sadar	L.I.C. Chowk	1	4
238.		Gaddigodanm square	1	4

Sl.N o.	Name of Police Station	LOCATION	CCTV CAMER A PTZ	CCTV CAMER A Fixed
239.		Meshram putla square	1	4
240.		Chhovani square	1	4
241.		Sadar café house square	1	4
242.		V.C.A. chowk	1	4
243.		Punam chamber ahead	1	2
244.		Pagalkhana square	1	4
245.		Vanita vikas square	1	4
246.		Hotel Ashoka Chowk	1	4
247.		Katol Chowk Naka	1	4
248.		Durga Mata Mandir Chowk	1	4
249.		Police Talao Chowk	1	4
250.		Gondwana Chowk	1	4
251.		Punam Chamber	1	4
252.		Gaddigodam Chowk	1	4
253.		Jaystambh Chowk	1	4
254.		R.B.I. Chowk	1	4
255.		Akashwani Chowk	1	4
256.		Ladies Club Chowk	1	4
257.		Mohd. Rafi Chowk	1	4
258.		RaviBhavan Main Gate	1	2
259.		Futala Talao Road Ramgiri Banglow Chowk	1	4
260.		RajBhavan Rear Gate Chowk	1	4
261.		Mangalwari Bazar Complex	1	2
262.		Tahsil Office	1	2
263.		Sadar Karachi Galli Residency Road Gandhi Chowk	1	4

Sl.No.	Name of Police Station	LOCATION	CCTV CAMER A PTZ	CCTV CAMER A Fixed
264.		Administrative Building No. 1, 2 and District Compound Bazar	2	3
265.		In Front of Shriram Tower Parking	1	2
266.		Chhaoni Y point	1	3
267.		GPO Chowk	1	4
268.		In Front of Tahsil Office Gate	1	2
269.		In front of Collector Office Gate	1	2
270.		District Court Main Gate	1	2
271.		Jaystambh Chowk DRM Office	1	2
272.		RajBhavan Sadar Bus Stand	1	2
273.		In front of DCP Zone II Office	1	2
274.		Chhaoni Police Chowki T Point	1	3
275.		MangalDeep Chowk T Point	1	3
276.		Hanuman Mandir sewa Banglow	1	2
277.		Liberty Talkies Chowk	1	4
278.	Gittikhada n	Japani garden square	1	4
279.		juna Katol naka square	1	4
280.		New katol naka	1	4
281.		Gorewada square	1	4
282.		Dabha square	1	4
283.		Awasthi nagar T point	1	3
284.		Rajbhawan rear gate square	1	4
285.		Seminary Hills Near Balodyan vihar	2	3
286.		T.V. Tower Chowk	1	4
287.		Veternary college Chowk	1	4
288.		In front of Botanical Garden	1	2

Sl.N o.	Name of Police Station	LOCATION	CCTV CAMER A PTZ	CCTV CAMER A Fixed
289.		L.A.D. College Chowk	1	4
290.		Near Telangkhedi Hanuman Mandir	1	2
291.		Japani Garden Chowk	1	4
292.		Katol Naka Chowk	1	4
293.		Gittikhadan Chowk	1	4
294.		K.T.Nagar Katol Road	1	2
295.		Surendragadh Bajrang Chowk	1	4
296.		New Katol Naka Chowk	1	4
297.		N.M.C. Dabha Naka	1	4
298.		Gorewada Ring Road Chowk	1	4
299.		Anant Nagar Chowk	1	4
300.		Borgaon Chowk	1	4
301.		Awasthi Nagar Chowk	1	4
302.		Friends colony Chowk	1	4
303.		Kadbi chwok,	1	4
304.		kamal chwok	1	4
305.		Char Khamba Chowk	1	4
306.		Rani Dugawati Chowk	1	4
307.		AwaleBabu Chowk	1	4
308.	Panchpaoli	Under Mehandibagh Over Brigde	1	2
309.		NIT Chowk Vaishali Nagar Cement Road	1	4
310.		Teka Naka chowk Kamthi Raod	1	4
311.		Motibagh Railway crossing Guard line Road	1	2
312.		1 No. Pull Chowk Kamthi Road	1	4
313.		BuddhNagar Kalgidhar Gurudwara Turning Kamthi Road	1	2

Sl.N o.	Name of Police Station	LOCATION	CCTV CAMER A PTZ	CCTV CAMER A Fixed
314.		Gamdur Bar Chowk kamthi Road	1	2
315.		Baba Buddhaji Nagar Gate Kamthi Road	1	2
316.		Chirag Ali Chowk New Wasti, Teka	1	4
317.		Mohd. Rafi Chowk	1	4
318.		Mulchand Saoji Bhojanalaya Turning Mehendi bagh Road	1	2
319.		Chakna Chowk Mehendibagh Road	1	4
320.		Raut Chowk Mehendibagh Road	1	4
321.		Naik Talao Near Tadi Shop	2	3
322.		Prakash Pan Mandir Chowk, Tandapeth	1	4
323.		Laldarwaja Chowk, Railway Gate	1	4
324.		Pachpaoli Over Brige Nandgiri Road T Point	1	2
325.		Dr. Ambedkar Garden Vaishali Nagar	2	3
326.		Asinagar Chowk	1	4
327.		Ashoknagar Chowk	1	4
328.		Chambhar Nala Turning	1	2
329.		Pachpaoli over bridge toward Barse Nagar Road And toward Thakkargram Road	1	2
330.		Front side of Sindhu College	1	2
331.		Buddha Chowk Ara Machine Road	1	4
332.	Jaripatka	Indora chowk	1	4
333.		Jaripatka chowk	1	4
334.		Barakholi Chowk	1	4
335.		Bhim Chowk	1	4
336.		Khobragade Chowk	1	4
337.		Jaripatka Bazar	2	3

Sl.No.	Name of Police Station	LOCATION	CCTV CAMER A PTZ	CCTV CAMER A Fixed
338.		Itarsi Pulia	2	3
339.		Patankar Chowk	1	4
340.		KapilNagar Chowk	1	4
341.		Kamgar Nagar Chowk	1	4
342.		Automotive Chowk	1	4
343.		Koradi naka	1	4
344.		koradi mandir T point	1	3
345.		Karemore Complex Chowk	1	4
346.	Koradi	Mahadula T Point	1	3
347.		Smuti Nagar turning Point near Bridge	1	2
348.		Mordern School near Goyal Kirana Stores	1	2
349.		Arya Nagar Chowk	1	4
350.		Faras gate square	1	4
351.		Mankapur square	1	4
352.		Mental Hospital Square	1	4
353.		Mankapur Kalpana Talkies Chowk In Front of Krida Sankul	1	4
354.		Zingabai Takli Faras Chowk	1	4
355.	Mankapur	Zingabai Takli Zenda Chowk	1	4
356.		Shrikrishna Mangal Karyalaya Godhni Road	1	2
357.		Godhni Toll Naka	1	4
358.		Zingabai Takli Shafi Nagar Chowk	1	4
359.		Sadikabad T-Point Mankapur	1	3
360.		Koradi Road under the Over Bridge near Baba Farid Nagar	1	2
361.		Godhani Naka Godhani Raod	1	4



Sl.No.	Name of Police Station	LOCATION	CCTV CAMER A PTZ	CCTV CAMER A Fixed
362.		Gorewada Durga Chowk Mankapur Ring Road	1	4
363.		Itarsi Pulia near NADT Campus	2	3
364.		Police Talao T Point	1	3
365.		Gorewada Chungi naka Pithesur Raod	1	4
366.		Baba Farid Nagar under the over bridge Koradi Road	1	2
367.		Mahatma Phule Chowk Godhani Village	1	4
368.		Godhani Railway Station	2	3
<b>ZONE 3</b>				
369.		Telephone Exchange chowk	1	4
370.		Sarda chowk	1	4
371.		Mahavir chowk	1	4
372.		Vaishno Devi chowk	1	4
373.		Azad chowk	1	4
374.		Darodkar chowk	1	4
375.		Chandrashekhar Azad chowk	1	4
376.		Kolba Swami chowk	1	4
377.	Lakadganj	Telephone Exchange Chowk	1	4
378.		Chapru Nagar Chowk	1	4
379.		Ambedkar Chowk	1	4
380.		Wardhman Nagar Chowk	1	4
381.		Vaishnov Devi Chowk	1	4
382.		Day To Day chowk	1	4
383.		Prajapati chowk	1	4
384.		Sukhsagar Apartment	1	2
385.		Power House Chowk	1	4

Sl.N o.	Name of Police Station	LOCATION	CCTV CAMER A PTZ	CCTV CAMER A Fixed
386.		Sudarshan Chowk	1	4
387.		Sunil Hotel Chowk	1	4
388.		Juna Motor Stand Chowk	1	4
389.		Balaji Mandir Chowk	1	4
390.		Masurkar Chowk	1	4
391.		Vande Materam Chowk	1	4
392.		Nehru Putla Chowk	1	4
393.		Maskasath Chowk	1	4
394.		Lalganj Raut Chowk	1	4
395.		Mehandibag chowk	1	4
396.		Premnagar Zenda Chowk	1	4
397.		Shantinagar Ghat Chowk	1	4
398.		Kawrapeth Railway crossing	1	2
399.		Ratan Tower	1	2
400.		Gangabai Ghat Chowk	1	4
401.		Hiwri Nagar Chowk	1	4
402.		Marwadi Chowk	1	4
403.		Zade Chowk	1	4
404.		Dosar Bavan chowk	1	4
405.		Sevasadan chowk	1	4
406.		Agrasen chowk	1	4
407.	Tahsil	Gandhi Putala chowk	1	4
408.		Sona Restorent chowk	1	4
409.		Golibar chowk	1	4
410.		Gitanjali chowk	1	4

Sl.N o.	Name of Police Station	LOCATION	CCTV CAMER A PTZ	CCTV CAMER A Fixed
411.		Bhagvagar chowk	1	4
412.		Meyo Chowk	1	4
413.		Dosar Bhavan Chowk	1	4
414.		Gitanjali Chowk	1	4
415.		Sewa Sadan Chowk	1	4
416.		Agresan Chowk	1	4
417.		Darodkar Chowk	1	4
418.		Tanga Stand Chowk	1	4
419.		Sahid Chowk	1	4
420.		Nikalas Mandir Chowk	1	4
421.		Bharat Mata Chowk	1	4
422.		Tinal Chowak	1	4
423.		Ganjakhet Chowk	1	4
424.		Golibar Chowk	1	4
425.		Timki Tin Khamba	1	3
426.		Mominpura Chowk	1	4
427.		Kabrasthan Road	1	2
428.		Bhankheda Ambedkar Putla	1	2
429.		Saifi Nager T Point	1	3
430.		Garib Nawaz Masjid Boriyapura	1	2
431.		Gurd Line Chowk	1	4
432.		Bhagwagar Chowk	1	4
433.		Jama Masjid	1	2
434.		Mominpura	2	3
435.		Nalshab Chowk	1	4

Sl.N o.	Name of Police Station	LOCATION	CCTV CAMER A PTZ	CCTV CAMER A Fixed	
436.		Dhondba Chowk	1	4	
437.		Lal Imli Chowk	1	4	
438.		Sut Market	1	3	
439.		Nanga putla Chowk	1	4	
440.		City Post Office Itwari	1	2	
441.		Dharaskar Road Itwari	1	2	
442.		Memon Jamat Bangali panja	1	2	
443.		Piewli Marbat Chowk	1	4	
444.		Timki Dadra Pul	2	3	
445.		Dobinager Dargah	2	3	
446.		Resham oli Bohara Masjid	1	2	
447.		Kotwali	Chitnis Park chowk	1	4
448.			Gangabai Ghat chowk	1	4
449.	Badkas chowk		1	4	
450.	Ramkular Gate		1	2	
451.	Zenda chowk		1	4	
452.	C.A. Road Gandhi square		1	4	
453.	Badkas square		1	4	
454.	Sona restorent square		1	4	
455.	Chitanawis park square		1	4	
456.	Aaychit Mandir bus stop		1	2	
457.	Zenda chouk		1	4	
458.	Gangabai ghat square		1	4	
459.	Gandhi Gate		1	2	
460.	Ram cooler square	1	4		

Sl.No.	Name of Police Station	LOCATION	CCTV CAMER A PTZ	CCTV CAMER A Fixed	
461.		C.P.& Berar square	1	4	
462.		Apsara square	1	4	
463.		Bhola Ganesh chouk	1	4	
464.		Gajanan square	1	4	
465.		Tiranga square	1	4	
466.		Old Nandanwan square	1	4	
467.		Nandanwan cement road	1	2	
468.		Old shukrawari Gandhi statue	1	2	
469.		Mahal square	1	4	
470.		Kalyaneshwar Mandir	1	2	
471.		Matru seva sangha hospital	1	2	
472.		Navug school	1	2	
473.		Sangh building	2	3	
474.		S.D. Hospital square	1	4	
475.		Mahawir Gardan	2	3	
476.		Bhosla wed school	2	3	
477.		Manepura square	1	4	
478.		Jagnade square	1	4	
479.		Mahila mahavidyalaya square	1	4	
480.		Dakshinamurti square	1	4	
481.		Chitrs talkies gate	1	2	
482.		Agresan square	1	4	
483.		Ganeshpe th	Cotton Market chowk	1	4
484.			Agyaram Devi chowk	1	4
485.			Jadhav chowk	1	4

Sl.No.	Name of Police Station	LOCATION	CCTV CAMER A PTZ	CCTV CAMER A Fixed
486.		North Side of Jadhao Chowk Near Bus station	1	2
487.		South Side of Jadhao Chowk Near Bus station	1	2
488.		West Side of Jadhao Chowk Near Bus station	1	2
489.		East Side of Jadhao Chowk Near Bus station	1	2
490.		North Side of Baidhnath Chowk	1	2
491.		North Side of Cotton Market Chowk	1	2
492.		South Side of Cotton Market Chowk	1	2
493.		West Side of Cotton Market Chowk	1	2
494.		East Side of Cotton Market Chowk	1	2
495.		North Side of Gandhisagar	1	2
496.		South Side of Gandhisagar	1	2
497.		West Side of Gandhisagar	1	2
498.		East Side of Gandhisagar	1	2
499.		Railway Station East Gate	1	2
500.		Empress Mill T-Point	1	3
501.		Agyaramdevi Chowk	1	4
502.		Santra Market	2	3
503.	Kalamana	Hanuman mandir	1	2
504.		Kapsi chowk	1	4
505.		Juna Pardi Naka chowk	1	4
506.		Chikhali chowk	1	4
507.		Kapsi Over Brig	1	2
508.		Kapsi Under Bridge	1	2
509.		Outer Ring road Near Indiasan Dhaba	2	3
510.		Outer Ring road Tarodi over bridge	2	3

Sl.No.	Name of Police Station	LOCATION	CCTV CAMER A PTZ	CCTV CAMER A Fixed
511.		New Pardi Naka Bhandara road	2	3
512.		Pardi Bazar Hanuman Temple	2	3
513.		Bhandewadi Relway Station	1	2
514.		Punapur Road Ghatate Nagar chowk	1	4
515.		Subhan Nagar near Hanuman Temple	1	2
516.		Sharda chowk Netaji Nagar	1	4
517.		Bharatwada Road Near Nagpure School chowk	1	4
518.		Bharatwada Y Point	1	3
519.		Bharatwada Chowk	1	4
520.		Old Pardi Naka Chowk	1	4
521.		Bharat Nagar chowk	1	4
522.		Kalamna Market chowk	1	4
523.		Chikhli Chowk	1	4
524.		Kalamna Relway Gate	1	2
525.		Minimata Nagar chowk	1	4
526.		Depty Signal Relway Gate	1	2
527.		Depty Signal Udta hanuman Chowk	1	4
528.		Old Kamptee Road near Police chowky	1	4
529.		Old Kamptee Road near Rillayance Petrol pump	1	2
530.		Pavangao Chowk	1	4
531.		Dhargao Chowk	1	4
532.	Yashodhara	Maruti showroom chowk	1	4
533.		Vitabhatti chowk	1	4
534.		Kanji house chowk	1	4
535.		Yashodhara chowk	1	4

Sl.N o.	Name of Police Station	LOCATION	CCTV CAMER A PTZ	CCTV CAMER A Fixed
536.		PNR Off	1	2
537.		Yadav Nagar Petrol Pump	1	4
538.		Vinoba Bhawe Nagar	2	3
539.		Namdev Nagar	2	3
540.		Kamthi Naka	1	4
541.		Shiv Arket Bhilgao	1	2
542.		Nag Lock	1	2
543.		Tulsa lawn	2	3
544.		Shivam Aparment	1	2
545.		Yeshodhar Nagar Chowk	1	4
546.		Kanji House Chowk	1	4
547.		Shitla mata mandir chowk	1	4
548.		Sajay Gandhi Nagar	2	3
549.		Panchwati Nagar	2	3
550.		Bohara Koloni	2	3
551.		Jamdar Wadi	2	3
552.		Shahu Mohalla	2	3
553.		Wandewi Nagar Chowk	1	4
554.		Pili Nadi Chowk	1	4
555.		Mehbubpura	2	3
556.		Raja Chowk	1	4
557.		Kundanlal Gupta Nagar	2	3
558.		Shiwaji Chowk	1	4
559.		Transport Plaza	1	2
560.		Bara Nal Chowk	1	4



Sl.N o.	Name of Police Station	LOCATION	CCTV CAMER A PTZ	CCTV CAMER A Fixed
561.		Gosavi Akhada	2	3
562.		Anand Nagar	2	3
563.		Jay Bhole Nagar	2	3
564.		Jay Bhim Chowk	1	4
565.		Rani Durgawati Chowk	1	4
<b>ZONE 4</b>				
566.		Ajni Chowk	1	4
567.		Infront of PS	1	2
568.		Suyog Nagar Chowk	1	4
569.		Omkar Nagar Chowk	1	4
570.		Shree Nagar Chowk	1	4
571.	Ajani	Rameshwari Chowk	1	4
572.		Shatabadi Chowk	1	4
573.		Medical Chowk	1	4
574.		Trisharan Chowk	1	4
575.		Hanuman Nagar	2	3
576.		Narendra Nagar	2	3
577.		Netaji market Mehadiya Chowk	1	4
578.		Dev nagar	2	3
579.		Lokmat chowk	1	4
580.	Dhantoli	Shamtarka apt. javal	1	2
581.		Dhantoli Under Bridge Chowk	1	4
582.		Mehadiya Chowk to Panchshil Chowk	1	4
583.		West Park Road Lokmat Chowk	1	4
584.		Near Mount Carmal School, Ajni Chowk	1	4

Sl.N o.	Name of Police Station	LOCATION	CCTV CAMER A PTZ	CCTV CAMER A Fixed
585.		Anand talkies Chowk	1	4
586.		Munje Chowk	1	4
587.		Zansi Rani Chowk	1	4
588.		Yashwant Stedium	2	3
589.		Dhantoli Garden Area	2	3
590.		Mata Kacheri Chowk	1	4
591.		Devnagar Chowk	1	4
592.		Congress nagar T-Point Chowk	1	3
593.		Gajanan nagar Chowk	1	4
594.		Rahate Colony Chowk	1	4
595.		Janki talkies	1	2
596.		Ajni Railway Station	1	4
597.		Ajit Bekari	1	4
598.		Chharapati Chowk	1	4
599.		Bhiwapurkar Marg Dhantoli	1	2
600.		Sureteck Hospital Area	1	2
601.		Jail Road	1	2
602.		Pragati Colony	2	3
603.		FCI Godawn	2	3
604.		Surendra Nagar Garden	2	3
605.		Ajni Chowk, Near Yashwant Chavhan Putala	1	4
606.		Dhantoli Police Station Chowk	1	4
607.		Shani Madir, Bhuyari Marg	1	3
608.	Imamwad a	Sardar Patel Chowk	1	4
609.		Ashok Chowk	1	4

Sl.N o.	Name of Police Station	LOCATION	CCTV CAMER A PTZ	CCTV CAMER A Fixed
610.		Awari Chowk	1	4
611.		Reshimbag Chowk	1	4
612.		Krida Chowk	1	4
613.		Untakhana Chowk	1	4
614.		Jatatrodi Chowk	1	4
615.		Baidyanath Chowk	1	4
616.		Medical chowk to baidnath chowk	1	4
617.		Untakhana Chowk to Medical Chowk	1	4
618.		Ajni Over Bridge to Medical Chowk	1	4
619.		Krida Chowk to Amma Hospital Chowk	1	4
620.		Baidyanath Chowk to Untakhana Chowk	1	4
621.		Chandan Nagar, Near Ramabai Garden	2	3
622.		Rambagh Colony	2	3
623.		Sakkardara Chowk	1	4
624.		Sakkaradara fly over	1	2
625.		Bhande Plot Chowk	1	4
626.		Awari Chowk	1	4
627.		Tiranga Chowk	1	4
628.	Sakkarad ara	Gajanan Chowk	1	4
629.		Tukdoji Chowk	1	4
630.		Aurvedik Hospital, Budhawari Bajar	1	2
631.		Chota Tajbagh Chowk	1	4
632.		Sakkardara Lack Garden	2	3
633.		Dattatray Nagar Garden, Area	1	2
634.		Hussen Baba Dargah	1	2

Sl.N o.	Name of Police Station	LOCATION	CCTV CAMER A PTZ	CCTV CAMER A Fixed
635.		Old Ayodhya Nagar Bus Stop	1	2
636.		Gajanan Highschool T-Point	1	3
637.		Chamat Chakki Chowk	1	4
638.		Buland Get, Motha Tajbagh	1	4
639.		Shitala Mata Mandir Chowk	1	4
640.		Gurudev Nagar Chowk	1	4
641.		ESI Hospital Chowk	1	4
642.		Tukdoji Chowk to P.F. Office Road	1	2
643.		Buggewar, Ashirwad nagar chowk	1	4
644.		Reshimbagh N.I.T. Garden Area	1	3
645.		Shahenshaha Chowk	1	4
646.		Budhwari Bajar Main Road	2	3
647.		Tupkar Chowk	1	4
648.		Old Ayodhya Nagar Bus Stop to Baseshwar Putala Chowk	1	4
649.		Mahakalkar Building to old Ayodhya Nagar Bus Stop	1	2
650.		Boolywood Center Point Hotel	1	2
651.		Behine Shri. Binzani College gate, Budhwar Bajar	2	3
652.		Om Nagar Area	2	3
653.		Sangharsh Nagar Chowk	1	4
654.		Shitla Mata Mandir Chowk	1	4
655.	Nandanwan	K.D.K. college Chowk	1	4
656.		Opposite Area INOX Talkeis	1	2
657.		Nandanvan Main Road	1	2
658.		Opposite Area of Motha Tajbagh	1	2

Sl.N o.	Name of Police Station	LOCATION	CCTV CAMER A PTZ	CCTV CAMER A Fixed
659.		Wathoda Chowk	1	4
660.		Opposite Area of Hasanbagh Police Chowky	1	4
661.		Hasanbagh Chowk	1	4
662.		Aurangjeb Chowk, Hasanbagh	1	4
663.		Kharbi Chowk	1	4
664.		Jaybhim Chowk, Hiwari Nagar	1	4
665.		Nadanvan Canal Road	1	2
666.		Gurudev nagar	2	3
667.		Ramana maroti Chowk, Nagpur	1	4
668.		Opposite area of Vyankatesh Nagar Gate	1	2
669.		Jagnade Chowk	1	4
670.		Shitala Mata Chowk	1	4
671.		Telephone Nagar Chowk, Umred Road	1	4
672.		Backside of Sutgirani,	1	2
673.		Chamat Cakki Chowk	1	4
674.		Tukdoji Putala Chowk	1	4
675.		Manewada Cement Road, Jawahar Nagar Chowk	1	4
676.		Manewada Cement Road, Vairagade Hospital Chowk	1	4
677.	Hudkeshwar	Manewada Chowk	1	4
678.		Besa Chowk	1	4
679.		Beltarodi T-Point Chowk	1	4
680.		Uday Nagar Chowk	1	4
681.		Mahalgi Nagar Chowk	1	4
682.		Rajapeth Hudkeshwar Road	1	2

Sl.N o.	Name of Police Station	LOCATION	CCTV CAMER A PTZ	CCTV CAMER A Fixed
683.		Pipala Chowk Hudkeshwar Road	1	4
684.		Gajanan Mandir Chowk, Mahalgi Nagar	1	4
685.		Dighori Chowk	1	4
686.		Telephone Nagar Chowk	1	4
687.		Dighori Naka Chowky	1	4
688.		Gajanan Highschool Chowk, Juna Subhedar Lay- Out	1	4
689.		Ayodhya Nagar Chowk	1	4
690.		Sharda Chowk	1	4
691.		Sai Mandir Ayodhya Nagar	2	3
692.		Swami Samartha mandir Besa	1	2
693.		Shahu Nagar T-Point Manewada Besa Road	1	3
694.		Tukdoji Putala to Manewada Cement Road	1	2
695.		Manewada Cemet Road to Besa Road	1	2
696.		Vihirgoan Outer Ring Road	2	3
697.		Dighori Umred Road	2	3
698.		Mahalgi Nagar to New Narsala Road	1	2
699.		Besa Chowk to Pipalagoan Road	1	2
700.		Beltarodi to Shankarpur Goan Road	1	2

**Annexure III: Solution Requirement - Locations:**

#	Solution Requirement	Indicative Locations
1	PTZ + Fixed Box Camera (including Critical Locations)	700
2	Automatic Number Plate Recognition	25
3	Red Light Violation Detection	92
4	Public Address System	50
5	Variable Messaging	50
6	Thermal Camera	20
7	Facial Recognition System	20

***Locations shall be provided by the purchaser***

**ANNEXURE IV: Indicative list of City Kiosks Locations**

#	Indicative City Kiosk Location	Indicative Count
1	NMC Head Office	10
2	Zone 1 Office	2
3	Zone 2 Office	2
4	Zone 3 Office	2
5	Zone 4 Office	2
6	Zone 5 Office	2
7	Zone 6 Office	2
8	Zone 7 Office	2
9	Zone 8 Office	2
10	Zone 9 Office	2
11	Zone 10 Office	2
12	Other Key Locations – Private franchises authorized by NMC	70



**ANNEXURE V: Proposed locations for Zone aggregation points**

SI #	Location	Approximate Co-ordinates
1	A –Head Office Civil Lines, Nagpur Mahanagar Palika Municipal Corporation Nagpur, Maharashtra, India, 440 001	79.077544,21.154022,0.0
2	B - Laxminagar, NMC ZO Near Water Tank, Laxmi Nagar, Nagpur	79.060803,21.124015,0.0
3	C- Hanuman Nagar, NMC ZO Near Nehru Nagar School, Manewada Road, Hanuman Nagar, Nagpur	79.10576500000002,21.122115,0.0
4	D - Dhantoli NMC ZO Near Bengali High School, Humpayard Road, Dhantoli, Nagpur	79.083193,21.13555,0.0
5	E - Nehru Nagar NMC ZO Near Nehru Nagar Garden, Infront of Janki Devi School, Nandanwan Road, Nagpur	79.117852,21.128649,0.0
6	F - Gandhi Baugh NMC ZO Near Town Hall, Mahal, Nagpur	79.107369,21.144674,0.0
7	G - Sataranjipura NMC ZO Marwadi Sq., Itwari Railway Station Road, Nagpur	79.116674,21.180431,0.0
8	H - Lakadganj NMC ZO Behind Petrol Pump, Near Telephone Exchange Square, Lakadganj, Nagpur	79.120591,21.149823,0.0
9	I - Ashi Nagar, NMC ZO Near Anand Buddha Vihar, Ashi Nagar, Nagpur	79.074669,21.163673000000003,0.0
10	J - Mangalwari, NMC ZO	79.081586,21.165804,0.0

SI #	Location	Approximate Co-ordinates
	Koradi road, Near NMC School, Mangalwari, Nagpur	
11	K - Dharampeth, NMC ZO Near Gokulpeth Market, Dharampeth, Nagpur	79.06019300000001,21.140361,0.0
12	Parvati Nagar Post Office	79.0940094,21.1115937,0.0
13	Police Station Pachpaoli	79.1029049,21.1643543,0.0
14	Regional Passport Office	79.05298249999998,21.16499079999999,0.0

*\* This is an indicative list of locations, SI is expected to carry out an independent assessment and propose for same or different locations for housing the zone level aggregation points. Ward Aggregation points are expected to be identified by SI.*

**ANNEXURE VI: Indicative Bill of Material – (Location)**

Mentioned below is the indicative Bill of Material for each proposed solution (at each location), however the below quoted numbers are indicative only and SI is required to access the exact requirement, location wise, for all the proposed solution components and shall accordingly size the hardware and software infrastructure requirement.

**1. City Network Backbone**

#	Line Item	Unit of Measurement	Indicative Quantity
1.	24 Core Optical Cable	KM	1200
2.	24 Core Rack Mounted LIU	No.	500
<b>Aggregation Layer - Zone Level covering 10 zones</b>			
1.	Aggregation Router	No.	10
2.	Aggregation Switch	No.	10
3.	Network Access Switch	No.	5
4.	Network Switch Ruggedised	No.	5
5.	SFP Module	No.	200
6.	Fiber Testing and Automated solution management system	No.	1
7.	42 U Rack	No.	30
8.	Power Equipment (-48 Volt power source with battery, distribution box etc.)	Lot	1
9.	UPS (sizing as per proposed solution)	No.	20
10.	Air Conditioning 2 Ton	No.	30
11.	Site Preparation Cost	Lump Sum	1
<b>Access Layer - Ward Level covering 136</b>			
1.	Access Router	No.	136
2.	Network Access Switch	No.	72
3.	Network Switch Ruggedised	No.	200
4.	SFP Module	No.	1088
5.	Junction Box	No.	136
6.	Site Preparation Cost	Lump Sum	1

#	Line Item	Unit of Measurement	Indicative Quantity
7.	Air Conditioning 2 Ton	No.	As per requirement
8.	UPS (sizing as per proposed solution)	No.	2

## 2. City Operation Centre

#	Line Item	Unit of Measurement	Indicative Quantity
	<b>Core Infrastructure</b>		
1.	Core Router	No.	2
2.	Core Switch	No.	2
3.	Internet Router	No.	2
4.	Intranet Firewall	No.	2
5.	Internet Firewall	No.	1
6.	IPS / IDS	No.	2
7.	Network Access Switch	No.	4
8.	Network Switch Ruggedised	No.	2
9.	42U Network Rack	No.	As per requirement
10.	Blade Chassis	No.	As per requirement
11.	SAN Switch	No.	As per requirement
12.	UPS (sizing as per proposed solution)	No.	2
13.	Air Conditioning 2 Ton	No.	As per requirement
14.	Workstations (Desktop)	No.	10
15.	Multifunction Device	No.	5
16.	Site Preparation	Lump Sum	1
17.	Fire Alarm System	Set	1
18.	Biometric access control system	Set.	4
19.	Dome cameras for internal surveillance	No.	10
20.	Rodent Repellent system	Set	1
21.	Diesel Generator	No.	2
	<b>Core Solutions</b>		
1.	Integrated Operation Platform (IOP)	No.	1
2.	Antivirus Solution	Lot	1

#	Line Item	Unit of Measurement	Indicative Quantity
3.	GIS Map	Unit	1
4.	Enterprise Management System	Lot	1
<b>City Kiosk Operation Center Infrastructure</b>			
1.	Communication server	No.	2
2.	Web server	No.	2
3.	Application server	No.	2
4.	Database Server	No.	2
5.	Interface server	No.	2
6.	Storage	Tb	1
<b>City Kiosk Operation Center Software Solutions</b>			
1.	Server Operating System	No.	10
2.	Data adaptation management	FP	891
3.	Kiosk services management	FP	580
4.	Messaging & communication	FP	675
5.	Kiosk terminal management	FP	891
6.	Services interfacing component	FP	1,011
7.	Partner content management	FP	779
8.	Database Server Licenses	Lot	1
9.	Web Server Licenses	Lot	1
<b>City WiFi Operation Center Infrastructure &amp; Software Solutions</b>			
1.	Wireless Intrusion Prevention System	No.	2
2.	Centralised Wifi Management System	No.	1
3.	Application Server	No.	2
4.	Database Server	No.	2
5.	Wireless Controller with AP licenses	No.	2
6.	Server Operating System	No.	4
7.	Database Server Licenses	Lot	1
<b>CCTV Surveillance City Operation Center Infrastructure</b>			
1.	Video Wall	Unit	1
2.	Keyboard Joystick to control PTZ Cameras	No.	5
3.	Network Access Switch	No.	1
4.	Near DR Site infrastructure (as per requirement)	Lump Sum	As per requirement
<b>“Smart Strip” Infrastructure &amp; Software Solutions</b>			
1.	Storage	Tb	2

#	Line Item	Unit of Measurement	Indicative Quantity
	<b>Smart Transport &amp; ICT enabled Solid Waste Management Infrastructure</b>		
2.	VTS Server	No.	2
3.	Fleet Management & PIS Server	No.	2
4.	Database Server	No.	2
5.	Web Server	No.	1
	<b>Smart Transport &amp; ICT enabled Solid Waste Management Software Solutions</b>		
1.	Server Operating System	No.	7
2.	VTS, Fleet Management & PIS Application Server	No.	1
3.	Database Server Licenses	No.	2
4.	Web Server Licenses	No.	1
5.	Mobile Application	No.	1
6.	Centralised Attendance Management System	No.	1
	<b>Smart Light Infrastructure</b>		
1.	Application Server	No.	2
	<b>Smart Light Software Solutions</b>		
1.	Server Operating System	No.	2
2.	Smart Light Operation Management System	No.	1
	<b>Smart Traffic Infrastructure</b>		
1.	Application Server	No.	2
	<b>Smart Traffic Software Solutions</b>		
1.	Server Operating System	No.	2
2.	Adaptive Traffic Control System Application	No.	1
3.	PA System	No.	1
4.	VMS System	No.	1
	<b>Smart Parking Infrastructure &amp; Software Solutions</b>		
1.	Central Server	No.	2
2.	Smart Parking Information System	No.	1
3.	City Parking Information System Mobile Application	No.	1
	<b>Environmental Sensor System</b>		

#	Line Item	Unit of Measurement	Indicative Quantity
1.	Central Server	No.	2
2.	Central Environment System	No.	1
3.	Mobile Application	No.	1

### 3. City WIFI

SI #	Line Item	Unit of Measurement	Indicative Quantity
1.	Access Point	No.	1360
2.	Network Switch Ruggedised + SFP Module	No.	136
3.	Junction Box	No.	136
4.	UPS – 1 KVA	No.	136
5.	Site Preparation Cost	Lump Sum	1

### 4. City Surveillance

Total no. of locations across the city identified by Nagpur Police for implementing City Surveillance solution is 700. An indicative Bill of Material required for undertaking initial stage of implementation is specified below.

#	Line Item	Unit of Measurement	Indicative Quantity
1.	Fixed Camera + IR Illuminator	No.	2930
2.	Dome Camera	No.	100
3.	PTZ Camera	No.	611
4.	MultiSensor 360° Camera	No.	200
5.	Thermal Camera	No.	20
6.	Public Address System – IP based PA with speakers	No.	50
7.	Variable Message	No.	50

8.	Drone with complete ground station setup	No.	10
9.	Gantry Pole including site preparation cost	No.	50
10.	Pole including site preparation cost	No.	As per requirement
11.	Network Switch Ruggedised	No.	As per requirement
12.	Junction box	No.	As per requirement
13.	Rack Mounted LIU	No.	As per requirement
14.	UPS – 2 KVA	No.	As per requirement
15.	Power Cable	Meter	As per requirement
16.	Edge Processing Infrastructure (ANPR & RLVD)	Set	120

**Mobile Surveillance Vehicle – (per vehicle)**

#	Line Item	Unit of Measurement	Indicative Quantity
1.	PTZ Camera	No.	1
2.	Fixed Camera with IR Illuminator	No.	2
3.	3M retractable Pole structure for Cameras	No.	As per requirement
4.	UPS – 3 KVA	No.	1
5.	Laptop	No.	1
6.	21" LCD Monitors	No.	1
7.	Keyboard Joystick to control PTZ Cameras	No.	1
8.	Network Switch Ruggedised	No.	1
9.	Pre-fabricated Mobile Van	No.	1
10.	Vehicle customization	Set	1



#	Line Item	Unit of Measurement	Indicative Quantity
	<ul style="list-style-type: none"> <li>• Seat provision for 5 personnel plus driver &amp; co-driver</li> <li>• Ground Clearance: 175mm or better.</li> <li>• Fan</li> <li>• Flood Lights/LED light bar</li> <li>• Mobile sets</li> <li>• Water Containers with holder</li> <li>• Basic First Aid Box</li> <li>• Fire Extinguisher</li> <li>• Vehicle sticker</li> <li>• Storage Decks</li> <li>• Holders</li> <li>• Small Stretcher</li> <li>• Anti-Riot equipment</li> <li>• CSD Kit</li> <li>• Wind Shield Protector</li> <li>• Engine immobilizers</li> <li>• Convertible Mics with PTT option</li> <li>• Body Camera</li> </ul>		
11.	Siren with PA system	No.	1
12.	Generator Set	No.	1

N.B: The bidders should note that while quoting the unit price for Mobile surveillance vehicle in Commercial Bid format in Section 8.2 of RFP vol I, it should include the price for all sub-components specified above - PTZ Camera, Fixed Camera with IR Illuminator, 3M retractable Pole structure for Cameras, UPS – 3 KVA, Laptop, 21" LCD Monitors, Keyboard Joystick to control PTZ Cameras, Network Switch Ruggedised, Pre-fabricated Mobile Van, Vehicle customization (Seat provision for 5 personnel plus driver & co-driver, Ground Clearance: 175mm or better, Fan, Flood Lights/LED light bar, Mobile sets, Water Containers with holder, Basic First Aid Box, Fire Extinguisher, Vehicle sticker, Storage Decks, Holders, Small Stretcher, Anti-Riot equipment, CSD Kit, Wind Shield Protector, Engine immobilizers, Convertible Mics with PTT option and Body Camera), Siren with PA system, and Generator Set.

### 5. City Surveillance Command Control Center

SI #	Line Item	Unit of Measurement	Indicative Quantity
1.	Workstation Desktop	No.	25
2.	Video Wall	Unit	1

SI #	Line Item	Unit of Measurement	Indicative Quantity
3.	Keyboard Joystick to control PTZ Cameras	No.	10
4.	Biometric access control system, 4 door controller	No.	4
5.	Dome cameras for internal surveillance	No.	10
6.	UPS (sizing as per proposed solution)	No.	2
7.	Multifunction Device	Set	5
8.	IP Phones	Set	5
9.	Site Preparation Cost	Lump Sum	1
10.	Fire Alarm System	Set	1
11.	Rodent Repellent system	Set	1
12.	Diesel Generator Set	Set	2
13.	Air Conditioner 2 Ton	No.	As per requirement

## 6. Server Room at Command Control Centre

SI #	Line Item	Unit of Measurement	Indicative Quantity
	Server Infra (with redundancy)		
1.	Datacenter Network Switch	No.	2
2.	Access Router	No.	2
3.	Internet Router	No.	1
4.	Intranet Firewall	No.	2
5.	Internet Firewall	No.	1
6.	Video Management Server	No.	31
7.	Video Analytics Server	No.	16
8.	ANPR Server	No.	6
9.	RLVD Server	No.	6

SI #	Line Item	Unit of Measurement	Indicative Quantity
10.	Variable Message Signboard server	No.	1
11.	Database Server	No.	2
12.	Web Server	No.	1
13.	Storage Server	Tb	5000
14.	UPS (sizing as per proposed solution)	No.	2
15.	Blade Server Chassis	No.	As per requirement
16.	IP EPABX	No.	1
17.	42 U Rack	No.	As per requirement
18.	Air Conditioner	No.	As per requirement
19.	Site Preparation Cost	Lump Sum	1
	Software Solutions		
1.	Server OS License	No.	66
2.	Anti Virus License	Lot	1
3.	Enterprise Management System License	Lot	1
4.	Virtualization Software License	Lot	1
5.	Video Management Software License	Lot	1
6.	Video Analytics Software License	Lot	1
7.	ANPR Software License	Lot	1
8.	RLVD Software License	Lot	1
9.	PA Software License	Lot	1
10.	Variable Message Software License	Lot	1
11.	Facial Recognition System Software License	Lot	1
12.	Database Server Licenses	Lot	1
13.	Web Server Licenses	Lot	1

## 7. City Kiosk

### a. Self Service City Kiosk

#	Line Item	Unit of Measurement	Indicative Quantity
1.	Kiosk Terminal	No.	50
2.	Modem	No.	50
3.	UPS – 1 KVA	No.	50
4.	Network Switch Ruggedised + SFP Module	No.	50
5.	Junction Box	No.	50
6.	Site Preparation Cost	Lump Sum	1

### b. Manned City Kiosk

#	Line Item	Unit of Measurement	Indicative Quantity
1.	Kiosk Terminal	No.	50
2.	Modem	No.	50
3.	UPS – 1 KVA	No.	50
4.	Network Switch Ruggedised Switch + SFP Module	No.	50
5.	Junction Box	No.	50
6.	Site Preparation Cost	Lump Sum	1

## 8. “Smart Strip”

### 1.1 Smart Transport

S. No.	Line Item	Unit of Measurement	Indicative Quantity
<b>Bus Infrastructure s</b>			
1.	Vehicle Tracking System (VTS) GPS device	No.	400
2.	2 Line LED Display Board	No.	1200
3.	Public Address System – IP based PA with speakers	No.	400
4.	GPRS/GSM Connectivity- SIM Card & Service Plan	No.	400
<b>Bus Stop Infrastructure</b>			
1.	4 Line LED Display Board	No.	160
2.	Network Switch + SFP Module	No.	160
3.	Junction Box	No.	160
4.	UPS – 1 KVA	No.	160

### 1.2 ICT Based Solid Waste Management System

S. No.	Line Item	Unit of Measurement	Indicative Quantity
<b>Field Infrastructure</b>			
1.	Vehicle Tracking System (VTS) GPS device	No.	6
2.	RFID Devices on vehicles	No.	6
3.	RFID Tagging on Bins / Collection Containers	No.	6
4.	Bin Weight Sensors	No.	2
5.	Bin Volume Sensors	No.	6
6.	GPS based handheld device with Attendance management system application	No.	7850
7.	GPRS/GSM Connectivity- SIM Card & Service Plan	No.	7850

### 1.3 Smart Lighting

S. No.	Line Item	Unit of Measurement	Indicative Quantity
<b>Field Infrastructure</b>			
1.	Smart Light Fixtures (LED based with motion and Ambient Light sensors)	No.	320
2.	Street Light Smart Controller	Lot	1
3.	Passive components and site preparation	Lump Sum	1

### 1.4 Smart Traffic

S. No.	Line Item	Unit of Measurement	Indicative Quantity
<b>Field Infrastructure</b>			
1.	Public Address System – IP based PA with speakers	No.	6
2.	Variable Message System Display	No.	3
3.	Gantry Pole Set up	No.	3
4.	Adaptive Traffic Control System Unit – Detectors, Sensors and Interface	No.	10
5.	ATC Compliance Controllers	No.	10
6.	Passive Components and site preparation	Lump Sum	1

### 1.5 Smart Parking

S. No.	Line Item	Unit of Measurement	Indicative Quantity
<b>Field Infrastructure</b>			
1.	Wireless parking sensors	No.	50
2.	Embedded webserver	No.	2
3.	Digital Display unit	No.	1
4.	Boom Barrier	No	1
5.	Local System – Desktop & Printer	No	1
6.	Network Switch with junction box	No	1
7.	Site Preparation	Lump Sum	1

## 1.6 Environmental Sensors

S. No.	Line Item	Unit of Measurement	Indicative Quantity
<b>Field Infrastructure</b>			
1.	Environmental Sensors	No.	10

## 9. Helpdesk (Command Control Center and City Operation Center)

#	Line Item	Unit of Measurement	Indicative Quantity
1.	Hand Set	No.	5
2.	Head Set	No.	5
3.	IVRS Server	No.	1
4.	CTI Server	No.	1
5.	Automatic Call Distributor Server	No.	1
6.	Dialler	No.	1
7.	Voice Logger	No.	1
8.	Soft telephone	No.	5
9.	IP PBX	No.	1
10.	IP Phones	No.	5
11.	Workstation PC (including UPS, Computer chair, table etc.)	Set	5
12.	Automated Call Distribution Software	Lot	1
13.	Computer Telephony Integration Software	Lot	1
14.	Answering Service Software	Lot	1
15.	Interactive Voice Response Software	Lot	1
16.	Softphone Software	Lot	1
17.	Voice Broadcasting Software	Lot	1
18.	Server Operating System	No.	3