Solapur City Development Corporation Limited

REQUEST FOR PROPOSAL

Revisions: Nil

Particulars	Details
Client	Solapur City Development Corporation Limited, Solapur, INDIA
Project Name	Implementation of projects under Smart City Mission in Solapur City
Assignment Name	Request for proposal for Selection of System Integrator for Implementation of Command and Control Center for Solapur under Smart Cities Mission.
Document Name	**Volume II: Scope of Work**
Document Issue Date	18/01/2017
Document Number	2016-17/11

Solapur City Development Corporation Limited, Solapur, Maharashtra, India
Indrabhuvan, Ambedkar Chowk Solapur-413001.

January 2017

Contents

1. Project Scope of Work

The key components of smart city solution with scope of work are:

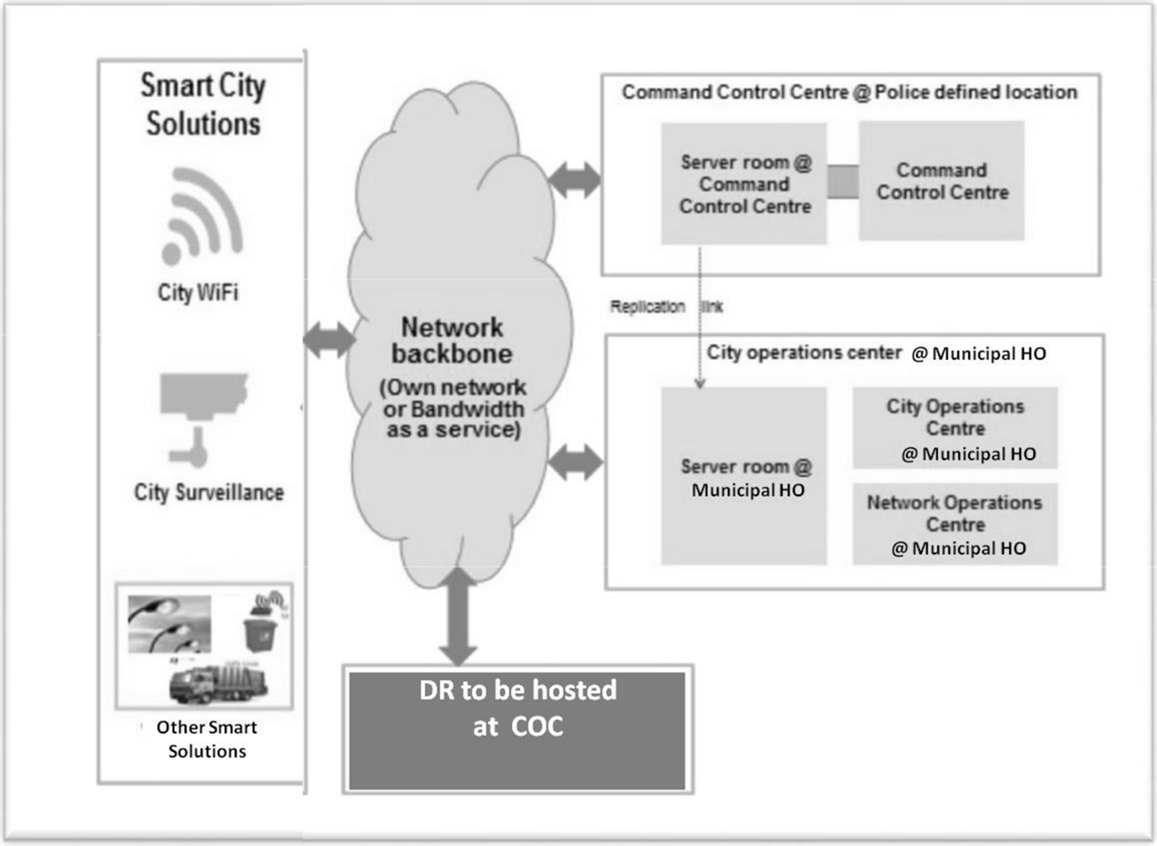
1. **Component 1: City Network**
2. **Component 2: City WiFi**
3. **Component 3: City Surveillance**
4. **Component 4: ICT Enabled Solid Waste Management**
5. **Component 5: Smart Lighting**
6. **Component 6: Smart Traffic**
7. **Component 7: Smart Parking**
8. **Component 8: Environmental Sensors**
9. **Component 9: City Bus Intelligent Transportation System**
10. **Component 10: Smart Governance and Citizen Services**

The above components shall be supported by:

1. **Police Command Control Centre (CCC)**
2. **City Operation Centre cum Bus Transport Management center**
3. **Data Centre and Disaster Recovery Centre**

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

The subsequent sections detail out the solution and scope with respect to each of the solution component. 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.


Smart City Solutions
City WiFi
City Surveillance
Other Smart Solutions
Network backbone
(Own network or Bandwidth as a service)
Command Control Centre @ Police defined location
Server room @ Command Control Centre
Command Control Centre
Replication link
City operations center @ Municipal HO
Server room @ Municipal HO
City Operations Centre @ Municipal HO
Network Operations Centre @ Municipal HO
DR to be hosted at COC

Diagrammatic representation of scope of work for System Integrator

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

1. Project Planning, execution and Management
2. Assessment and Gap analysis of requirement for all smart city components under scope.
3. Solution Design, System Customization and development for all components mentioned in this volume.
4.
5. ICT items Procurement, deployment and commissioning
6. Site Preparation including required civil work, LAN Networking
7. Application and general awareness Training
8. Business Process Reengineering for the selected applications/ services
9. STQC Certification
10. UAT & Go live
11. Capacity Building
12. Technical Support
13. Operation & Maintenance (O&M) for 5 Years after complete system go Live date.

Finalisation of the detailed Technical Architecture for smart city network

The SI will be required to review the Technical Architecture suggested in the Tender and finalise the detailed architecture for the overall system, incorporating findings of site survey exercise. The network so envisaged should be able to provide real time video stream to the Command Centers and viewing centers.

All the components of the Technical Architecture should:
(a) at least comply with the published eGovernance standards, frameworks, policies and guidelines available on http://egovstandards.gov.in (updated from time-to-time); and
(b) be of leading industry standards and /or as per standards mentioned at Annexure –XI.

Finalisation and submission of a detailed technical architecture

SI shall submit the detailed Technical Architecture and description of each sub components , alongwith the bid, which should take into consideration following guiding principles:

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

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

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

- **Security** - The architecture must adopt an end-to-end security model that protects data and the infrastructure from malicious attacks, theft, natural disasters etc. SI must make provisions for security of field equipment as well as protection of the software system from hackers and other threats. Using Firewalls and Intrusion Prevention Systems such attacks and theft should be controlled and well supported (and implemented) with the security policy. The virus and worm attacks should be well defended with gateway level Anti-virus system, along with workstation level Anti-virus mechanism. There should also be an endeavour to make use of the SSL/VPN technologies to have secured communication between Applications and its end users. Furthermore, all the system logs should be properly stored & archived for future analysis and forensics whenever desired. The authority would carry out the security audit of the entire system upon handover and also at regular interval during O&M period.

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

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

I. The security services used to protect the solution shall include: Identification, Authentication, Access Control, Administration and Audit and support for industry standard protocols.
II. The solution shall support advanced user authentication mechanisms including digital certificates and biometric authentication.
III. Security design should provide for a well-designed identity management system, security of physical and digital assets, data and network security, backup and recovery and disaster recovery system.
IV. The solution should provide for maintaining an audit trail of all the transactions and should also ensure the non-repudiation of audit trail without impacting the overall performance of the system.
V. The overarching requirement is the need to comply with ISO 27001 standards of security.
VI. The application design and development should comply with OWASP top 10 principles

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

- **Interoperability** - The system should have capability to take feed from cameras installed by private / Govt. at public places, digitize (if required) & compress (if required) this feed & store as per requirements.

- **Open Standards** - Systems should use open standards and protocols to the extent possible.

- **Single-Sign On-** The application should enable single-sign-on so that any user once authenticated and authorized by system is not required to be re-authorized for completing any of the services in the same session. For employees of the department concerned, the browser based application accessed on the intranet, through single-sign-on mechanism, will provide access to all the services of the departments concerned (based on their roles and responsibilities), Help module, basic and advanced reporting etc. Similarly, for external users (citizens, etc), based on their profile and registration, the system shall enable single-sign on facility to apply for various services, make payments, submit queries /complaints and check status of their applications.

- **Support for PKI based Authentication and Authorization-** The solution shall support PKI based Authentication and Authorization, in accordance with IT Act 2000, using the Digital Certificates issued by the Certifying Authorities (CA). In particular, 3 factor authentications (login id & password, biometric and digital signature) shall be implemented by the SI for officials/employees involved in processing citizen services.

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

(a) at least comply with the published eGovernance standards, frameworks, policies and guidelines available on http://egovstandards.gov.in (updated from time-to-time); and
(b) be of leading industry standards and /or as per standards mentioned at Annexure –XI.

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

- Passive networking & civil work during implementation and O&M period,
- Viewing manpower at Command / viewing centers & Mobile Vans during post-implementation
- FMS staff for non- IT support during post-implementation

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

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

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

- **Application Architecture**

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

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

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

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

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

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

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

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

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

The standards should:

(a) at least comply with the published eGovernance standards, frameworks, policies and guidelines available on http://egovstandards.gov.in (updated from time-to-time); and

(b) be of leading industry standards and /or as per standards mentioned at Annexure –XI.

V. The application should have a module for management of digital signature including issuance, renewal and suspension of digital signatures based on the administrative decisions taken by the State.
   - SI shall ensure using Digital signatures/eAuthentication(Aadhar Based) to authenticate approvals of service requests etc.

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

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

VIII. Complete mobile enablement of the Smart City System

1.1.3.3. Other expectations from SI

1. SI shall engage early in active consultations with the Authority , City Police and other key stakeholders to establish a clear and comprehensive project plan in line with the priorities of all project stakeholders and the project objectives.
2. Study the existing fiber duct (if any) layout in the city and existing network to understand the existing technology adopted in each of the following areas (not limited to):

   City WiFi
   ii-Surveillance Infrastructure – CCTV Cameras, Data communication, monitoring, control room and Infrastructure
   iii 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 indicated (but not limited to) in the tentative Bill of Materials included in the RFP and their appropriate quantity & capacity.
6. SI shall be responsible for supply of passive components indicated in the Bill of Materials section of the RFP viz. Housings, Fiber Patch Cords, Racks etc. Civil work required for the site shall be undertaken by the SI.
7. Validate / Assess the re-use of the existing infrastructure if any with Authority 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 Authority'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 all designated locations.
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 Authority.
14. SI shall ensure that the infrastructure provided under the project shall not have an end of life within 24 months from the date of bidding
15. SI shall ensure that the end of support is not reached during the concurrency of the contract and 5 years thereafter.
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. Authority shall not be responsible if the SI has not provisioned some components, sub-components, assemblies, sub-assemblies as part of Bill of Materials in the RFP. The SI shall have to provision these & other similar things to meet the solution requirements at no additional cost and time implications to Authority.
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 Authority 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 for duration of the contract for respective components to meet SLA requirement. The SI shall ensure that all the OEMs have an understanding of the service levels required by Authority. SI is required to provide the necessary MAF (Manufacturer Authorization Form) as per the format provided in the RFP in support of OEMs active support in the project.
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 authority's requirements
    ii. Size and propose for network devices (like Router, switches, security equipment including firewalls, IPS / IDS, routers, etc. as per the location requirements with the required components/modules, considering redundancy and load balancing in line with RFP.

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

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

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

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

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

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

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

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

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

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

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

1.1 SOLUTION 1 - City Network

1.1.1 Overview

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

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 Authority wishes to implement a dedicated and secure fiber network backbone to be established across Solapur.

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

MPLS based network or better is expected to be provisioned for the backbone network.

The network backbone is expected to help the *Solapur* 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

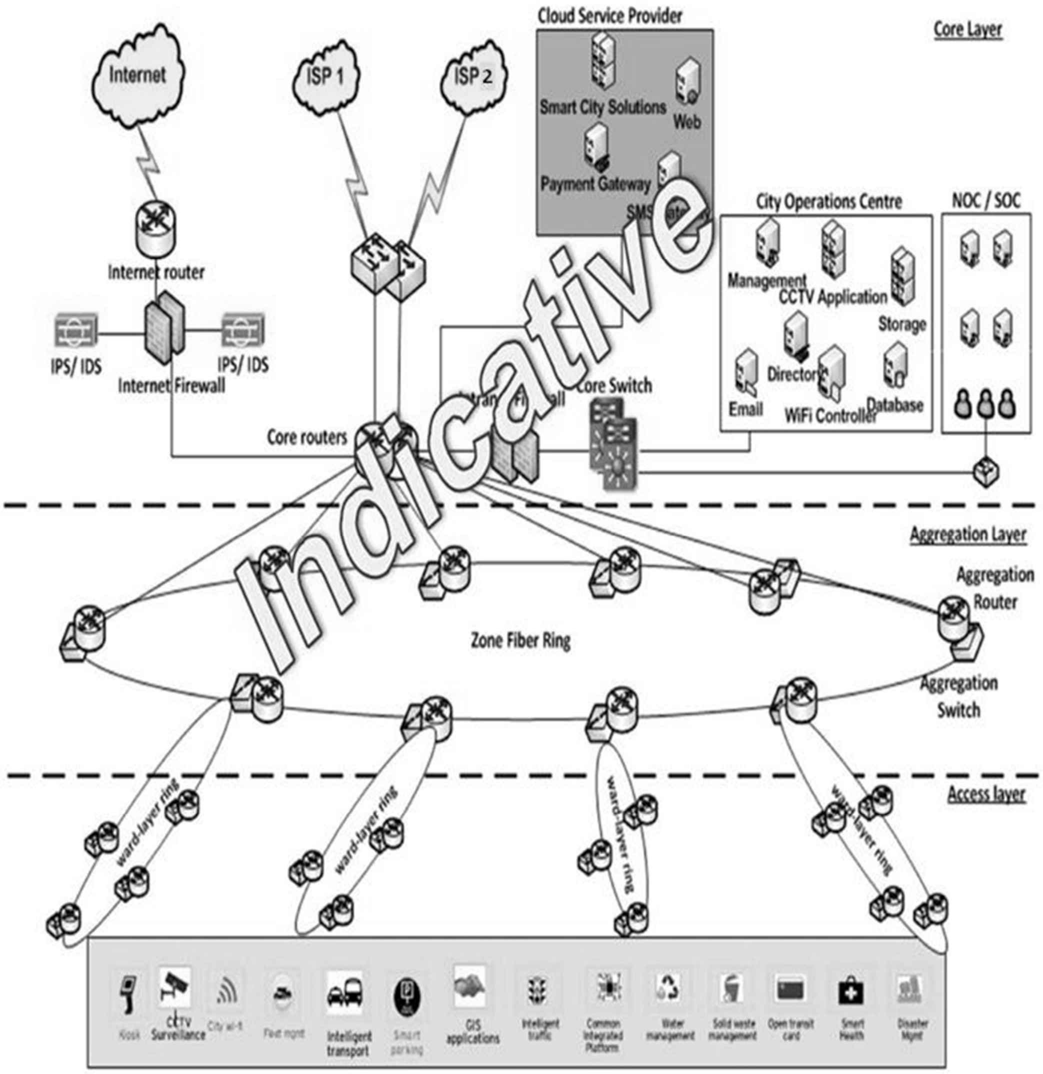
d. Adoption and usage of distributed compute and storage services, location services, and security services

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. However, the standards of design and services should (a) at least comply with the published e-Governance standards, frameworks, policies and guidelines available on http://egovstandards.gov.in (updated from time-to-time); and (b) be of leading industry standards and /or as per standards mentioned at Annexure –XI.

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



The envisaged layers of the City Network Backbone are:

a. **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 command control center and City Operations Centre. This layer shall enable all applications hosted at command control center and 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.

b. **Aggregation Layer – Zone Level:** The aggregation layer is envisaged at Zone level. The traffic coming from respective wards shall get aggregated at the Zone level. 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.

c. **Access Layer –Ward Level**: The Access layer shall be formed at the wards of authority. 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 city. The service layer shall enable the smart city solutions such as City Surveillance, City WiFi, Smart lighting, Smart parking,smart traffic 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	Command control center and city operation center.
2	Aggregation layer	Identified aggregation point as mentioned in ANNEXURE V. These are mostly Authority 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: • City Surveillance • City WiFi • ICT based Solid waste ,management • Smart Lighting • Smart traffic • Smart Parking • City Bus Intelligent transport system, • Envioment sensors • E-governance

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. 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. For any change applicable, based on the type/severity/complexity of change, the change should be proposed with due justification and to be implemented upon approval from the Authority.
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 Authority 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

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 Authority for their approval..
   b. The bidder 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:**

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 to be indicated in the Bill of Material (BoM) and to be 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 fiber cable (OFC) laid and the unit 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
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 Authority.
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.
i. The core shall adhere to ITU-T G.655 standards for Non-zero dispersion shifted Metal-free unarmoured optical fiber cable conforming to TEC specification GR/OFC-07/02. Jul 2007 or latest and the raw material used in its manufacture will conform to TEC Specification TEC/GR/TX/ORM 01/04.

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 Authority.
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 Authority.
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 and other smart city components 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 and approval from the Authority.

b. List of Authority 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 authority 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 Authority 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 authority.
      - 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 room 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 electric meter shall be in the name of the Authority; however the provisioning and the electricity expenses to be borne by the SI during the contract period.
      - 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 *Solapur*, 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 Authority. SI can make use of the publicly available data and tools such as Google Maps, ArcGIS, NIC developed maps etc.
However the ownership of the accuracy and validation of the data map information shall be with the SI.

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 authoritty's fiber ducts (if any) 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 and other smart city components.
   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 Authority.

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 be responsible for gathering the Bandwidth and LAN connectivity requirements at junctions, Data Centers, Command Centers, and viewing centers. The LAN connectivity may involve setting up the structured cabling, commissioning of active and passive components for operationalization of the Smart City System.

m. The actual bandwidth requirement and storage parameters required to meet SLAs should be calculated by the SI and the same shall be clearly proposed in the Technical Bid with detailed calculations for all smart city components.. *Solapur* also requires the SI to meet the parameters of video feed quality; security & performance and SI is required factor the same while designing the solution.

n. SI shall also consider the terrain, topography, climatic conditions etc. while designing the network architecture.
o. The Network Architecture once approved shall be base lined either in part or in whole and the Authority shall institutionalize the processes for Architecture Change management to undertake any change in the respective location, as required during the contract phase.
p. 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 etc.
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 Authority 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 Authority's owned ducts (if any) and new ducts.
b. The Authority shall facilitate the SI to get all the necessary permission(s) for fiber laying including the Right of Way. SI shall be responsible for coordination for all the activities in this regard.
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. Technical Specifications of HDPE Pipe. The HDPE pipe will conform to TEC specification GR/CDS and latest amendments thereof or better. The HDPE pipe used will be of 40 mm outer diameter with minimum wall thickness of 3.5 mm.

j. 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.

k. 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.

l. Mechanical splicing shall be used for temporary splicing of fibers or where fusion splicing is impractical or undesirable.

m. At all other location and during initial installation of optic fiber cable, fusion splicing shall be adopted.

n. Authority 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. Authority 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 Authority

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. Authority 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 authority or other service 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				1310 nm	1550 nm	

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 Authority and maintenance team

List of items to be handed over to Authority / 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:

i. Power supply equipment
- Main. of Charger and In/Out voltages and currents
- Checking of fuses and terminations
- Check of Earthing

ii. Optical fiber cable

iii. Cable route
- Integrity of cable route
- Protective works on bridges & culverts
- Cable route markers
- Earthing of sheath of cable

iv. 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. Alternate Network Connectivity Provision

The SI has the option of sourcing the bandwidth from the telecom service provider .Connectivity infrastructure will connect the project sites like DC, DR, CCC, City operation center Camera Locations, Access points and other smart city components etc.

The SI will undertake the following:

a. The coordination with Telecom Service Providers to ensure last mile connectivity of all project sites.
b. LAN within all Project sites including but not limited to IP addressing scheme, physical cabling, router/switch configuration, V-LAN configuration, load balancing configuration, and fail over mechanism. The SI should coordinate with the local department offices while designing and installing the LAN.
c. All networking equipment required providing the LAN / WAN connectivity to meet the requirements of the Project is also to be provided by the SI as part of this RFP **scope.**

The SI to ensure that while sourcing the bandwidth from the telecom service provider , the deliverables as mentioned in this section 1.1 (as in case of laying dedicated fiber network) are adhered to and the necessary design to be adopted by the SI accordingly under approval from the [Authority].

][1]

[1] The option of Alternate Network Connectivity shall be applicable in case the city does not want to invest in the network backbone initially but rather source the bandwidth from the telecom service provider. The clause, however, needs to be deleted if the city decides to lay the network backbone.

1.2. SOLUTION 2 – 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, Authority intends to provide public Wi-Fi services at identified locations across the *Solapur*. 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 *Solapur*). 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 Authority 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 Authority 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 Data center. The proposed solution shall include access points and related infrastructure as per specifications mentioned in the RFP. However, the standards of design and services should (a) at least comply with the published e-Governance standards, frameworks, policies and guidelines available on http://egovstandards.gov.in (updated from time-to-time); and (b) be of leading industry standards and /or as per standards mentioned at Annexure –XI.

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 Data center. 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 Service Set Identifier 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 (for the entire duration of contract period). Based on need, SI shall be required to supply additional access points as per the unit rate quoted in the financial bid.

1.2.2 Solution requirements

Key expectations from the system include:

a. The network shall support user devices with 2.4 GHz as well as 5.8 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.

m. New users should be given the free access of say 50/100 MB to use limited services (for better interaction with the Government and availing citizen services) for subscribing the available plans.

The access points may be deployed outdoor or indoor depending on the requirement of the Authority 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 Authority.

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 Authority 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 *Solapur*. 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. Authority estimates provisioning of City WiFi services at [No. of locations] 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. Multiple payment gateway integration required so subscribers can make the payments using online/ offline mode, including prepaid mobile balance & wallet applications.

6. Advertising platform integration -AAA to support advertisements from multiple parties.

7. 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.

    c. City Wi-Fi Locations

        i. Authority 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 Authority.

            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. The network should support Low Power WAN. The few common technical specifications/parameters of similar networks like LoRa, LoRa WAN, Sigfox, Weightless, NarrowBand internet of things (IoT) and likewise. The specification towards LPWAN should be:

- Minimum 5-10 km of communication range
- Higher capacity towards number of nodes that can communicate
- Long battery life
- Low interference
- Operational into the free wireless band
- Secure bi-directional communication
- Localisation services
- Ability to integrate with backend Cellular/Wi-Fi network
- Longer battery life for end-devices/nodes

f. 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

g. Set up Wi-Fi network across locations proposed in phased manner

h. Procurement, planning, design, installation, commissioning and support of all end point equipment (IT and non IT) required to set up WiFi locations.

i. Providing adequate security mechanisms in City WiFi service equipment to prevent unauthorized access or interfaces to services, calls, protocols and data.

j. Providing complete network diagram including detailed technical documentation, survey, drawing and detailed Project Plan for all the locations mentioned.

k. 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.

l. 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 Authority or its authorized entities shall be responsible for any non-compliance on account of non-adherence by the SI.

m. The SI should provide all the usage data/log/analysis for further usage like usage prediction, planning towards additional resource deployment.

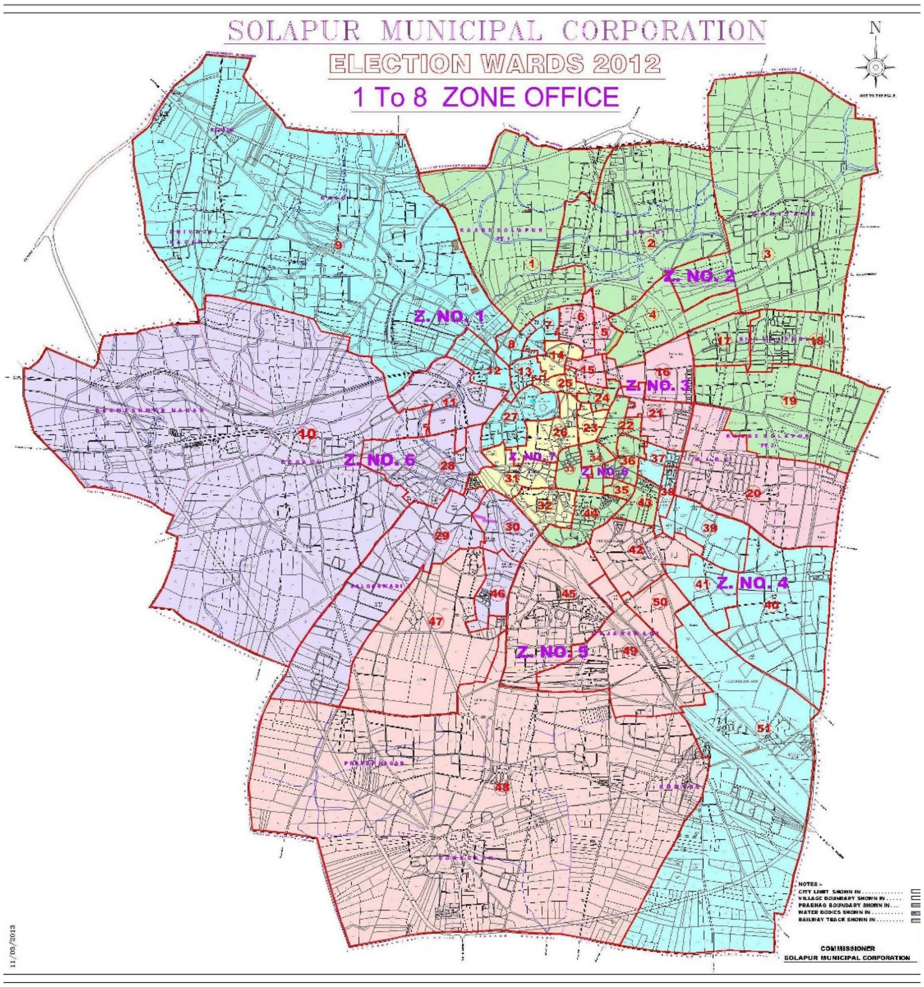
1.3 SOLUTION 3 – City Surveillance

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 [State], under the smart city initiative, intends to implement a holistic City Surveillance System in City Police Jurisdiction limits in the *Solapur*.

1.3.2 Geographical Spread

The *Solapur* Police covers an area of about 180 Sq. km. The following map represents the Geographical spread of the area and zone wise distribution of police jurisdictions. This includes the *Solapur* Municipal Corporation limits.



Solapur Municipal Corporation Map

1.3.3 Solution requirements

The SI shall be responsible for Supply, Installation, Implementation and Operation & Maintenance of *Solapur* Surveillance System for a period of Five Years from the date of Go Live of the respective phase independently. The standards should (a) at least comply with the published eGovernance standards, frameworks, policies and guidelines available on http://egovstandards.gov.in (updated from time-to-time); and (b) be of leading industry standards and /or as per standards mentioned at Annexure –XI.. The indicative requirement for SI is broadly categorized into following:

Category	Scope of Work
Min Surveillance System Infrastructure at field locations	Supply, install, implement and maintain: ▪ Full HD IP Pan–tilt–zoom camera (PTZ) Camera ▪ Full HD IP Fixed Box Camera ▪ Full HD IP Dome Cameras ▪ Thermal Camera ▪ Pole, Junction box, UPS, LAN switch, passive items etc.
	1. Cameras to support ANPR 2. Cameras to support RLVD 3. Cameras with online FRS 4. Cameras to support analytics Other components: 1. Public Announcement System 2. Variable Messaging System 3. Drone 4. Mobile Surveillance Vehicle **Data retention period: 90 days** Kindly refer [*Annex-XX*] for detailed location wise camera Distribution.
Network Infrastructure	1. Between camera & aggregation point – Field location 2. Between aggregation points & Data center 3. Between Data center & command control center and city operation center. 4. Between Data center & viewing/monitoring center 5. Between drone ground station / mobile surveillance vehicle & Data center It is envisaged that the system shall leverage City Network Backbone infrastructure that is being created for *Solapur*. 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.
Data center	1. Supply & installation of IT Infrastructure including server, storage, network components and peripherals to handle 100% load along with provisioning for redundancy 2. Supply & installation of Non IT infrastructure like furniture, AC, and interior work etc. excluding civil work at the space provided by the Authority. 3.Set up of DR site with 100% redundancy of infrastructure.

Category	Scope of Work
Command Control Center	1.Supply & installation of IT & Non IT infrastructure like video wall, workstation, furniture, AC, and interior work etc. excluding civil work at the space provided by Authority 2. Supply & establishment of Mobile Command Control Center 3. Establishment of Forensic Investigation Room 4. Establishment of Dial 100 control room
City Operation Center	City Operation Center establishment at the identified location for viewing and controlling the selected field locations in a fully automated environment including: 1. Supply & installation of IT & Non IT infrastructure like video wall, workstation, furniture, AC, and interior work etc. excluding civil work at the space provided by Authority
Surveillance System Applications	1.Video Management System (VMS) 2.Video Analytics (VA) 3.Red Light Violation Detection (RLVD) System 4.Automatic Number Plate Recognition (ANPR) System 5.Facial Recognition System (FRS)
Video feeds at few selected locations	SI is expected to provision for viewing of feeds at selected key police locations
Training/Capacity Building	Technical & functional training to the designated officials on a continuous basis

1.3.4 Scope of Work:

1.3.4.1. 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 the *Solapur* authority

A detailed survey shall be conducted, by the SI along with a team of Authority and the *Solapur* 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 Authority 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 Authority. 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. Outdoor 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.

1.3.4.2. 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/Authority Branding) of poles and junction boxes, to warn mischief mongers against tampering with the equipment at the junction.

1.3.4.3. Installation of Poles/Cantilevers/Gantry

1. The SI shall ensure that all installations are done as per satisfaction of Authority.
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 cameras and Variable Messaging Sign boards

10. SI shall provide structural calculations and drawings for the approval of Authority. The design shall match with common design standards as applicable under the jurisdiction of Authority/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.

1.3.4.4. 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 and other field equipments 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 the *Solapur* throughout the year.

1.3.4.5. 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 the *Solapur*'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 *Solapur* throughout the year.

1.3.4.6. 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, as 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 Authority.
15. SI shall house the electricity meters inside the power cabinet as mentioned in the controller Cabinet section as above.

1.3.4.7. 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

1.3.4.8. Miscellaneous:

1. Authority 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 (except the RoW charges) shall be applicable to Authority 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 O&M from the SI throughout the contract 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 Authority. 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 Authority or its designated agency.
7. 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.

8. 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.
9. In case of request for change in location of field equipment post installation, the same shall be borne by Authority at either a unit rate as per commercials or a mutually agreed cost.

1.3.4.9. Public Address system

Public Address system shall be used at intersections, public places, market places or those critical locations as identified by Authority 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.

1.3.4.10. 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/ wi-fi/ Ethernet/SMS Channel. GSM data channel (GPRS) / wi-fi/ 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 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.

1.3.4.11. 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 360^0 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.

The drone should be low weight and should have a min flight time of 60 min. It should be able to operate in all weather conditions including night time. It should have min 30 min battery back up and should cover min 5 km range.

It should record videos in all the common video formats. There should be provision to take snapshots. It should have PTZ and altitude control functionality and functionality to download maps upon entering the GPS location.

1.3.4.12. 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 Authority/the *Solapur* Police.
5. The vehicle can be divided into three main sections:
    a. Driver Side
    b. Monitoring Side
    c. Power Compartment

6. Provision for Fire fighting equipment in the MSV

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

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 Command control 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.

1.3.4.13. Data center

- SI is required to co-locate all the hardware/software and related items as per the design offered for the smart city infrastructure including SLA monitoring and Help desk management, in a Tier III or above data Center complying to standard guidelines as per Telecommunications Infrastructure UPTIME/TIA-942.

- The Data center shall be available for 24x7x365 operation.

- The smart city infrastructure shall have built in redundancy and high availability in compute and storage to ensure that there is no single point of failure.

- The SI is free to take the colocation services from any existing data center located within India (preferably in the same city where possible) which meets the prevailing data center standards, since this is one of the most critical components of the smart city infrastructure. However the system SLA as defined in the tender to be met soleby by the SI.

- The SI shall submit to Authority adequate documentation/ evidences in support of the choice of the data center to meet the project requirements.

- **Min Guiding factors for selection of the Data Center:** Following are the benchmark requirements which should act as guiding factors for the SI to select and propose the locations for the Data Center

.

  - There should be dedicated rack space available in the data center for the entire Smart City project Infrastructure.
  - Access to the Data Center Space where the Smart City Project Infrastructure is proposed to be hosted should be demarcated and physical access to the place would be given only to the authorized personnel
  - Racks to be caged.
  - Smart City Data Center should be at least a Tier III Data Center as per Telecommunications Infrastructure Standard for Data Centers and should be 27001 Certified. The required certification to be enclosed along with the technical bid response.
  - It should have access control system implemented for secured access.
  - Indoor CCTV Cameras would be required to be installed to monitor the physical access of the system from remote location
  - Physical Access to the building hosting Data Center should be armed and it must be possible to even depute police personnel for physical security of the premises.

Min 90 days Data Backup of the video feeds and the transaction data for min 1 year shall be stored within the Data Center infrastructure preferable in a cost effective and innovative manner.

In case the data center services are to go down due to any unforeseen circumstance, the Command Center should have access to the video feeds of previous 90 days and the transaction data for min 1 year from this data backup facility.

Access logs to be stored for the entire duration of contract and handed over to Authority upon termination/expiry of the contract.

DATA CENTER SPECIFICATION

- Design Standard: Tier-III or above
- The availability of data must be guaranteeing to 99.982% availability.
- Receiving Power: Commercial power substation next to DC
- UPS: UPS system with N+N redundancy
- Generator: Gen-set with N+1 redundancy
- Power Provision: Dual power feed, PDU sources to each rack, Power supply to a rack as per requirement
- Cooling Features:
  - System: Air-cooling system with N+2 redundancy, Management of temperature and humidity
  - Blow-out Type: Raised flooring air conditioning system, Down-blow below raised floor and drawn into ceiling

- Fire Protection: High Sensitive Smoke Detectors, Fire Suppression System
- Security: CCTV surveillance cameras, 24x7 on-site security presence, building Access (Photo Id Card must) along with biometric authentication

Disaster Recovery (DR) Site

The SI is required to provision for a Disaster Recovery (DR) Site same as of main Data Center (DC) capacity & standard for Smart City Solution. The DR site should not be in the same seismic zone and should be at least 50 km from Main DC site.
DR site shall provision to cater to 100% load of the smart city system.
There shall be no loss of video recording in case of failure of any single server and storage component. Both DC and DR Site shall work in an Active-Active mode with 100% recording of cameras and application availability of all smart city components.
The SI shall establish dedicated connectivity between the DC and DR Site for replication & failover. The SI shall submit the detailed solution document for the DR Site solution with justification for the proposed design meeting the requirements.
Authority would carry out a detail assessment of the proposed location for the Smart City Data Center on the parameters of Safety & Security and reserves it right to accept or reject the proposed site for data center. In case the proposed site is not acceptable to Authority, Successful Bidder shall suggest alternatives matching the requirements mentioned above.

Authority may also ask the respective bidder to arrange for a visit during bid evaluation stage.

The SI needs to offer the cost of the colocation, both for DC and DR site considering the requirement of Rack space, Seating space for the technical/Project team and the electricity charges on yearly basis.

Tier 3 DC Min characteristic

1. Tier 3 Data Center Availability: The availability of data from the hardware at a location must be guaranteeing to 99.982% availability.

2. Redundancy and concurrent maintainability. It requires at least n+1 redundancy as well as concurrent maintainability for all power and cooling components and distribution systems. Any such component's lack of availability due to failure (or maintenance) should not affect the infrastructure's normal functioning.

3. No more than 1.6 hours of downtime per year

4. N+1 fault tolerant providing at least 72 hour power outage protection

5. All IT equipment is dual-powered and fully compatible within the topology of a site's architecture.

The Data center shall primarily be divided into two zones:

1. **Server Infrastructure Zone**
   This zone shall host servers, server racks, storage racks and networking components like routers, switches to passive components. All the Data center LAN connections shall be provided through switches placed in this area. The approximate size of the Server Infrastructure zone shall be approx. ……sq.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.

1.3.4.14. IT Infrastructure for Data center

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

1. **Hardware and Network Provisioning**
   SI shall be responsible for the following but not limited to:
   a. Appropriate sizing and provisioning of IT infrastructure like servers/storage, network devices (like routers/switches etc.), security equipment including firewalls, etc. with the required components/modules considering redundancy and load balancing in line with minimum technical requirements
   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 Data center 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. Authority may at its sole discretion evaluate the hardware sizing. The SI needs to provide necessary explanation for sizing to Authority
   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 Data center 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 Data center 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 Data center 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.
   c. SI should provide the unique identity schema similar to addressing schema for all hardware components.

4. **Sub-Networks & Management of Network operation**
   a. The proposed architecture of Data center 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 Authority
   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 Data center, 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 Data center.
   b. Necessary IDS/ IPS shall be provided for monitoring the traffic of all the VLANs at Data center.
   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 Data center shall be provisioned by the SI.
e. SI shall implement management systems and procedures that adhere to Authority'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 Authority's resources from internal and external threats.

k. SI shall provide Authority with the necessary hardware/software required for efficient intrusion management.

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

Both DC and DR Site shall work in an Active-Active mode.

The SI shall establish dedicated connectivity between DC and DR Site for replication & failover.

The SI shall design the DC and DR 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 DC and DR site shall be periodically audited, updated and mock drills shall be performed. along with the findings and improvement /corrective steps to be taken to concerned authority

The bidder shall submit the detailed solution document for Dc and DR Site solution with justification for the proposed design meeting the requirements alongwith the bid.

1.3.4.15. 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 Authority, 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 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, FRS 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). The integration with such systems will be in the scope of the SI.

Location for Command Control Center shall be provided by the Authority. 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 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.

Dial 100 control room

A Dial 100 Control Room shall be established as part of the command control center in the city. A Dial 100 based police control room would empower people to connect to police and get police assistance anytime, anywhere at very short “response time”.

The objective of the Dial 100 Police Control Room is to receive and respond immediately to emergency calls made by the public seeking police assistance by directing the patrolling police vehicles available for the purpose. The centre will be equipped with latest technological tools like GIS MAP, CAD (Computer aided dispatch) and GPS enabled PCR VANs to attend to handle public distress calls for services.

The dial 100 control room shall be provided with one PRI line inline hunting-single telephone number (100) to a group of 30 lines. Number of incoming and outgoing calls can be defined as per requirement for each city. The Dial 100 control system aims to ensure that:

i. Calls can be made to 100 from any phone whether landline or mobile.

ii. System has multiple caller interface and is capable of receiving 30 calls at a single instance.

iii. Caller's name and address is automatically visible saving precious time.

iv. Exact location of the place of incident and nearest available police vehicle identified on GIS map which saves time.

v. Status of response by police vehicle can be monitored by control room.

vi. Information received and police actions taken are automatically logged into the system generating a fool proof database of events.

vii. The system should have facilities such as cell ID, Observed Time Difference of Arrival (OTDOA) and assisted GPS to acquire and push accurate location information for both wireless and wireline phone to emergency.

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

a) Functional Requirements

1. The basic requirements of Police for setting up Dial 100 Control Room include but not limited to:
   a. Establishing a quick and efficient emergency response system
   b. Dispatch vehicles rapidly to required location
   c. Automation of Call-taking & Dispatching
2. The Computer aided dispatch (CAD) software platform integrates various modules:
   a. CAD framework
   b. Call Reception System
   c. Call Recording and Logging
   d. GIS (Geographical Information System)
   e. AVLS (Automatic Vehicle Location System)
   f. Responder Systems (Mobile Data Terminals)
   g. Incident Reporting System
   h. Video Interface (CCTV Video Integration to GIS)
   i. Converged Communication Platforms [PSTN, Wireless (Cell Phone), SMS, e-mail]

The Integrated Software Platform supports all features required for efficiently handling all stages of a call made in emergency situation.

b) Operational Requirements

1. Dial 100 control room shall be equipped with EPABX comprising of 1 PRI line inline hunting-single telephone number (100) to a group of 30 lines in each city.
2. The Control room shall have seating capacity of minimum 15 operators in each city.
3. Citizen can dial 100 for any complaints related with police. The system shall have capability to display name, address and find the geographical position of the caller at the time of receiving call in call center.
4. All phone calls shall be recorded for future references. The phone calls of last at least 90 days shall be stored in SAN Storage.
5. Dial 100 operators shall be able to receive call, Dispatch calls, use GIS maps and can send the alerts to the nearby free Patrolling vehicles on their MDT and also inform the nearest Police Station about the event.
6. Dial 100 operator shall be able to view the nearest Fire Station, Hospital, Blood Bank for providing additional assistance at the site of incident.
7. Dial 100 operator shall also be able to use police radio network for emergency handling and for communication with PCR Vans etc.
8. A web based incident analytic software shall be made available that will help the Police to do detailed analysis and analytics so that the response can be made proactive and also the effectiveness of the service improved.
9. After the Call has been logged in by the call taker, the Dial 100 System shall send a SMS to the Caller stating the CFS/Tracking Number along with a password as acknowledgement to the call made to the control room. The caller can use this number on department website to access the event progress details such as Action Taken Reports (ATR), file attachments, remarks, or other information’s as per the prevailing departmental policy for data sharing.
10. The analytics should have Social Media Analytics as one of the components. The city police and public functionalities need to be in touch with and being accessible to the general citizens especially the youth, older citizens and media etc. especially through social media. The analytics would leverage highly unstructured social media data in real time by using streaming social media analytics to identify rumors, potential threats and evolving events, find evidence through photos or track down witnesses. The analytics would also acquire location and tactical information of victims or criminals from information posted on Twitter, Facebook or other social media

Forensic Investigation room

The Command Control Centre will also have a room identified for IT Analytics and Forensic Experts where they will analyse the incriminating video clips and certify its integrity & chain of custody. The analysis would primarily relate with Video Analytics. The forensic Investigation room shall be equipped with one video wall, five workstations, IP telephone and at least five operators. Each city shall have its own forensic investigation room. The operators in the forensic room shall have access to live as well as stored video.

The operators would be able to run video analytics software on video feed being received from camera selected for the purpose. The forensic operators shall have access to all recorded voice communications of Dial 100 control room.

The analysis in C4 would be graphical user interface for search, replay and to simultaneously search and replay recorded telephone systems, GPS data on GIS maps, conventional and digital radio channels as well as trunked radio communications. All communications regarding a specific incident should be able to be replayed together in the sequence in which the communications occurred on a synchronised timeline.

System should support following Analytics:

- Unidentified object detection

- Intruder detection
- Camera tampering detection
- Virtual Fence / Tress Passing / Tripwire
- People / Mass movement
- Wrong direction monitoring

SI should provide option to run these analytics at edge level so that bandwidth can be saved or server based analytics can also be offered in case of proposed camera do not have capabilities of running analytics on the edge.

Video Analytics system shall provide mechanism to allow alerts to be raised in a customized manner for C4, Police officials and automatic decision support system. System shall be capable to avoid generation of false alarms

The VMS shall allow access of the video feeds on Tablets/iPads/select devices on user request. Such an access shall be based on MAC Address authentication over SSL (Secure Socket Layer) and/or by creating a VPN (Virtual Private Network). In addition, the VMS should be able to stream feeds from authorized Tablets/iPads/mobiles/select devices on the Video Wall.

The C4 should have the facility of integrating Police (100), Fire (101) and Health (102/108) Services. Coordination with these agencies is critical. The integration shall be for recording of all the data types of the above services as well as for real time transactions and response. The operators within C4 (Video Surveillance room and dial 100 room) shall make prompt and accurate decisions as per requirement of the incident, using the available technology. The center should also be able to group locations and connect surveillance systems in order to respond quickly to any emergency.

The suite of software modules would be required to be scaled up to support any number of cameras, control rooms and client operators and would have multiple redundancy and security level options.

Forensic Investigation Room – Operational Requirements

1. Forensic Investigation room shall be equipped with one video wall, four workstations, IP telephone and at least five operators in the city.
2. The forensic investigation room shall have seating capacity for min. 5 operators.
3. The forensic operators shall have facility to see live as well as playback videos of any camera. They shall keep a special watch on few selected cameras.
4. The video analytics software shall run on selected camera feeds to be further investigated by forensic operators.
5. The forensic operators shall be equipped with software for :
    - examination of authenticity of uploaded photos and videos
    - repair and recover videos
    - match photographs
    - provide forensic video enhancement of video evidence for identifying suspects,
    - provide recorded and archived media to authorized persons
    - transfer the evidence into a format that can be used for legal purposes etc.
    - Post analysis of video provided through secondary source through various attributes like identified object, size, color etc.
6. The forensic operators shall also have access to recorded voice communications of dial 100 control room and radio gateway.
7. Forensic Analyst/Operator may have following roles and responsibilities:

i. Examine, enhance and authenticate digital and analogue CCTV video evidence for both criminal and civil litigation

ii. Assist the police in respect of preparation of evidence for legal and judicial purpose in court.

iii. Providing recorded and archived med ia to authorized persons.

iv. Transfer the evidence into a format that can be used for legal purposes

v. Provide Forensic video enhancement of video evidence for identifying suspects.

vi. Attending and examining scenes of crimes

vii. Repair and recovery of evidence

1.3.4.16. Application Environment:

a. 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.

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

1. The VMS shall support a flexible rule-based system driven by schedules and events.
2. The VMS shall be supported for fully distributed solution for monitoring and control function, designed for limitless multi-site and multiple server installations requiring 24/7 surveillance with support for devices from different vendors.
3. The VMS shall support IP cameras of different makes.
4. All the offered VMS and cameras shall have ONVIF compliance.
5. The VMS shall be enabled for any standard storage technologies and video wall system integration.
6. The VMS shall be enabled for integration with any external Video Analytics Systems .

7. The VMS shall be capable of being deployed in a virtualized environment without loss of any functionality.

8. The VMS server shall be deployed in a clustered server environment for high availability and failover.

9. All CCTV cameras locations shall be overlaid in graphical map in the VMS Graphical User Interface (GUI). The cameras selection for viewing shall be possible via clicking in the camera location on the graphical map. The graphical map shall be of high resolution enabling operator to zoom-in for specific location while selecting a camera for viewing.

10. The VMS shall have an administrator interface to set system parameters, manage codecs, manage permissions and manage storage.

11. The VMS day to day control of cameras and monitoring on client workstations shall be controlled through the administrator interface.

12. Whilst live control and monitoring is the primary activity of the Operator workstations, video replay shall also be accommodated on the GUI for general review and also for pre and post alarm recording display.

13. The solution design for the VMS shall provide flexible video signal compression, display, storage and retrieval.

14. All CCTV camera video signal inputs to the system shall be provided to command control Center, and the transmission medium used shall best suit the relative camera deployments and access to the CCTV Network.

15. The VMS shall be capable of transferring recorded images to recordable media (such as CD/DVD and/or DAT tapes) in tamper evident and auditable form. All standard formats shall be supported including, but not limited to:

    a. AVI files
    b. Motion- Joint Photographic Experts Group (M-JPEG)
    c. Moving Picture Expert Group-4 (MPEG-4)

16. All the streams shall be available in real-time (expecting the network latency) and at full resolution. Resolution and other related parameters shall be configurable by the administrator in order to provide for network constraints.

17. The VMS shall support field sensor settings. Each channel configured in the VMS shall have an individual setup for the following minimum settings, the specific settings shall be determined according to the encoding device:

    a. Brightness
    b. Contrast
    c. Color
    d. Sharpness
    e. Saturation
    f. Hue
    g. White balance

18. The VMS shall support the following minimum operations:

    a. Adding an IP device
    b. Updating an IP device
    c. Updating basic device parameters
    d. Adding\Removing channels
    e. Adding\Removing output signals
    f. Updating an IP channel
    g. Removing an IP device
    h. Enabling\Disabling an IP channel
    i. Refreshing an IP device (in case of firmware upgrade)

19. The VMS shall support retrieving data from edge storage. Thus when a lost or broken connection is restored, it shall be possible to retrieve the video from SD card and store it on central storage.

20. The VMS shall support bookmarking the videos. Thus, allowing the users to mark incidents on live and/or playback video streams.

21. The VMS shall be capable of intrusion detection*:* Detection of moving objects in selected areas covered by the camera (those that are specified as restricted areas like those before some major events, etc.). Avoid false alarms due to wildlife or other moving objects (e.g., tree leaves).

22. The VMS shall be capable of tracing of a specific person or object in multi-camera videos*:* Track a specific person or object across several surveillance (e.g., to trace and identify criminals and/or anti-social elements).

23. The VMS shall be capable of counting of people and detection of abnormal crowd behaviour*:* Detection of people flow and counting of people in selected areas. To identify abnormal crowd behaviour and raise alarms to avoid untoward incidences in public places, and maintaining law & order.

24. The VMS shall be capable of summarize videos and create a content summary of the captured video depicting relevant movements or objects of interest. This would on *off-line* as well as *online* videos captured by the camera. For example, an hour-long surveillance video could be shortened by considering only the frames that depict major movements in the video.

25. The VMS shall allow the administrator to distribute camera load across multiple recorders and be able shift the cameras from one recorder to another by simple drag and drop facility.

26. VMS shall support automatic failover for recording.

27. VMS shall support manual failover for maintenance purpose.

28. VMS shall support access and view of cameras and views on a smartphone or a tablet (a mobile device).

29. VMS shall support integration with the ANPR application.

    a. VMS shall support integration with other online and offline video analytic applications.

i. VMS Core Components

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

ii. VMS General

1. The VMS shall be Codec and IP camera agnostic such that it can support devices that are not supplied by the manufacturer/developer of the VMS software and Codec hardware.
2. Each camera shall be identified by giving it a minimum thirty-two (32) character long, alphanumeric unique id followed by text description field.
3. When viewed on the GIS map, the text description of each camera shall be capable of being positioned anywhere on the monitor screen, on a camera by camera basis, shall afford options for size variations, and display with a flexible solid, semi-transparent or transparent background.
4.
5. The VMS shall support tamper detection for all cameras to warn of accidental or deliberate acts that disable the surveillance capability.
6. For alarm interfacing requirements, the VMS shall allow the selection of minimum five (5) cameras per single alarm source. The designated primary camera shall be automatically displayed as a full-screen image on the main GUI CCTV screen. The VMS shall also, on alarm, present associated pre/post event video allowing the Operator to assess the alarm cause. Other associated cameras, when called up, shall be displayed as split-screen images on the other monitor of the operator workstation.
7. Playback of any alarm related video, (including pre and post alarm video) shall start at the beginning or indexed part alarm sequence.
8. Video management software shall incorporate online video analytics on live video images. It shall include the following video analytics detection tools:
   a. Presence detection for moving and stopped vehicles
   b. Directional sensitive presence detection
   c. Congestion Detection
   d. Loitering detection
   e. Improper Parking
   f. Camera Tampering
   g. Abandoned objects detection
   h. Gun-shot detection

9. Off- Line Video Analytics should allow for quick retrieval of video footage to metadata stored with each image. System should provide results within few seconds, system should support for below listed the user's query.
   a. System should allow to specify the following search criteria:
      i. Motion in the zone, user-defined with any polyline
      ii. Detection of crossing a virtual line in a user-defined direction
      iii. Loitering of an object in an area
      iv. Simultaneous presence of a few objects in an area
      v. Motion from one area to another.
   b. System should support to apply below listed filters to search results:
      i. Object size
      ii. Object color
      iii. Direction of object motion
      iv. Speed of the moving object
   c. Defined area entry/appearance and zone exit/disappearance
10. Video clips of specific events via the VA or by the operator action shall be capable of being separately stored and offloaded by operator with appropriate permissions on to recordable media such as CD or Write Once Read Many (WORM) together with any associated meta-data for subsequent independent playback.
11. The system shall provide the capability to select duration and resolution of storage by camera, time and activity event and user request. Frequency/trigger of transfer shall be configurable by user.
12. The system shall provide the capability to digitally sign recorded video.
13. **Live video viewing:** The system shall allow the viewing of live video from any camera on the system at the highest rate of resolution and frame rate that the camera shall support on any workstation on the network.
14. **Recorded video viewing:** The system shall allow the viewing of recorded video from any camera on the system at whatever rate the camera was recorded.
15. **Storage of video:** The system shall store online thirty (30) days of video for all cameras. Balance 60 days will be on low cost secondary storage /tape library
16. The system shall provide the capability to manage the video storage to allow selective deletions, backups, and auto aging.
17. VMS shall have an extensive reporting capability with ability for administrator to define reports in a user friendly manner. The pre-existing reports shall include, but not limited to, the following:
   a. Reports on alerts received by type, date and time, location
   b. Reports on system errors and messages
   c. Reports on master data setup including cameras, decoders, locations
   d. Reports on cameras health check
   e. Reports on audit trails such as user actions
   f. Reports on system health including storage availability, server performance, recordings

iii. VMS GUI Capabilities

1. The user interface shall be via a GUI providing multiple video streams simultaneously on multiple monitors.

2. The GUI shall have the minimum capability of naming locations, users, and cameras events be displayed correctly on users screen.

3. The system shall have the capability to store and record operator specific options, such as screen layout, video layout, action on alarm, and automatic video transmission settings on events.

4. The GUI shall conform to standard Windows conventions.

5. The system shall provide unified GUI camera control at an operator's workstation for all types of cameras installed whether existing or new or connected via another agency.

6. By means of this unified control the following functions shall be provided:

    a. Selection
    b. Display
    c. PTZ
    d. Setup and adjustment
    e. Determination of pre-sets
    f. Any other commissioning and camera setup activity

7. All user interfaces shall support English Language and shall confirm to standard Windows protocols and practices and allow the control of all functions via a simple easy to use interface.

iv. VMS Map Functionality

1. The system shall support a mode of operation whereby a map of all or part of the map (at operator request) is displayed on a separate or same screen and that status information can be provided via an icon, and access to any cameras shall be accessible by means of an icon on that screen.
2. These Maps shall be defined so that an operator may make a selection from the same source of mapping that is available to the other systems within the comamnd control center, displaying whichever Map or section the operator needs, and it shall be displayed within one (1) second.

v. VMS Configuration

1. The VMS shall include a configuration facility to provide system administrators with a single interface utility to configure all VMS operating parameters.
2. The configuration tool shall be capable of supporting multiple concurrent users of the system, providing the ability to automatically update. It shall also allow the codec and camera configurations to be imported and exported in excel format.
3. The import/export tool shall be as sophisticated as necessary to support the following:
    a. Log every action so an audit or report can be completed
    b. Only update and log configurations where there is a difference between the system configuration and the new configuration file to be loaded

c. The import configuration file can contain any amount of data
d. Ability to run an update on the fly - i.e. no or minimal downtime to the system
e. Not require a reset or restart after any upgrades
f. Definable update times

4. The VMS configuration tool shall define:

a. Cameras (whether via codec units or directly connected IP cameras) and text based names
b. Camera Groups
c. User Groups
d. Monitors
e. Codec parameters
f. Alarms
g. Workstations
h. storage

5. The configuration utility shall allow the system administrator to:

a. Install new devices
b. Configure all aspects of existing devices
c. Configure and set up users/user groups and their rights/permissions/priorities
d. To define multiple camera groups
e. Each group to be defined for combinations of viewing and control rights
f. Individual Operators to be assigned multiple groups
g. Each group to be allocated to multiple Operators
h. Each camera may be in multiple groups
i. To program macros for individual and group camera characteristics
j. Program camera/monitor selection and configuration of the video wall(s) in response to an incoming alarm
k. Designate workstation destination for picture presentation in response to alarm initiation

6. User permissions/privileges, to be allocated, shall extend from full administrator rights down to basic operation of the system, and shall include the ability to designate workstations to an operator, and to designate one or more camera groups to an operator for viewing and/or control.

7. The configuration utility shall store all changes to the system, including but not limited to:

a. User log-ins
b. User log-offs
c. Human interface device inputs (key strokes)
d. External alarm commands
e. Error messages

8. A copy of the system configuration shall be stored external to the system to allow system restoration in case of hardware failure. External would mean another site, to be agreed with (City) during detail design.

vi. VMS User Hierarchy

1. The System Integrator shall request a detailed User Prioritization List (UPL) from the

(City) during the project.

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

vii. VMS Recording Requirements

1. All images shall be recorded centrally as a background process at configurable parameters.
2. It shall not be possible to interrupt, stop, delay or interfere with the recording streams in any way, without the appropriate user rights.
3. The CCTV recording system shall enable pre and post event (PPE) recording, presentation and storage, initiated automatically in response to system alarm sources received by the VMS.
4. The PPE recording clips shall be provided by the VMS and retrieved from the central video archive on the buffer storage system. This PPE stream shall be totally independent of the background recording stream provided to the central video archive such that central video archive recording, as programmed, continues under all circumstances.
5. The information stored shall be full real-time and full resolution from each incoming camera channel. In the absence of a trigger from a manual input or from a programmed alarm source, the PPE video recording shall be written to buffer storage on a FIFO basis.
6. PPE periods initiated by a single alarm occurrence shall be configurable via the VMS as follows:
   a. Pre – 0 to 30 seconds
   b. Post – 30 to 300 seconds
   c. Shall be variable for each camera according to each individual alarm and the alarm type
7. In the event of a trigger, the VMS shall ensure that the programmed sections of pre

and post event video are immediately presented to the Operator to complement the alarm display and simultaneously saved as an identified indexed video clip, complete with time/date stamp, in a reserved and protected area of the storage system. Such PPE recording shall then be capable of later retrieval via search criteria.

8. Once tagged and saved, the PPE video clip shall NOT be overwritten except by an operator with the required permissions i.e. it is excluded from the normal FIFO regime of the bulk storage system. Recording shall also be initiated on-demand by manual triggers from system operators e.g. keyboard key-stoke.
9. The VMS shall support the following recording modes:
   a. Total recording – the VMS shall constantly record the video input. The VMS shall allow for continuous recording of all video inputs
   b. Event based recording – the VMS shall record the video input only in case an event has occurred
10. VMS shall support the following triggers to initiate a recording
    a. Scheduler – the recorder will record the video inputs based on a specified schedule.
       i. The VMS shall allow recording based on a time schedule for all or some of the video channels
       ii. The VMS shall allow for multiple recording periods per day, per channel
       iii. The VMS shall have the option to set any available trigger in the system (VMD, TTL and/or API) to trigger the channel
       iv. The VMS shall have the option for individual channel setup of pre/post-alarm recording for defined interval (e.g. up to 10 minutes pre-alarm and 30 min post-alarm recording)
       v. The VMS shall have the ability to enable/disable triggers through a daily time schedule
    b. Manual – the user shall be able to initiate a manual recording upon request.
       i. The VMS shall work in conjunction to the any previous alarm operations
    c. The VMS shall allow API Triggers
    d. All trigger information shall be stored with the video information in the VMS data set and shall be made available for video search

viii. Manual or on demand recording

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

ix. VMS review system

1. The VMS recording and replay management systems shall support the following features and operations:
   a. Play back shall not interfere with recording in any way
   b. Support either analogue cameras connected via Codecs or IP-cameras directly

connected to the network

c. Stream live images through the network using IP Multi-cast techniques
d. Stream images from the Codec to the attached storage system
e. Store the recording stream from all cameras simultaneously with no degradation to any individual camera recorded image stream unless the system is configured by administrator to allow for change in quality
f. Deliver live video to VMS workstation within a period of one second from manual call up
g. Deliver live video to VMS workstation within a period of three seconds from automatic alarm receipt on alarm interface
h. Storage of each camera's images at a rate and resolution as defined in the Codec or IP camera configuration. The system VMS programming shall automatically vary these rates in response to time profiles, alarm inputs
i. Support multiple, configurable recording time schedules per camera. Each schedule shall support different recording parameters and automatically implement against the configured time schedule e.g. operational and non-operational hours shall be scheduled with different recording parameters on designated cameras
j. Support streaming of recorded files using IP Unicast directly to hardware decoders for display on analogue monitors or software decoder when/if required
k. Playback multiple, synchronized recorded streams at differing speeds and frame rates
l. Record and playback a video stream simultaneously at differing speeds and frame rates
m. Time stamping of every recorded video field based upon Network Time Protocol (NTP) time
n. Selectable on-screen-display of time and camera title during playback
o. Security file lock to prevent specific recorded files from being overwritten regardless of their date and time, in addition to those records stored as PPE clips. The duration and policy for retention of such videos would be same as that of the PPE clips
p. Configurable granularity of video files
q. Generate alarm when storage medium has fallen below a user selectable threshold
r. Stored video files can be "down-loaded" to directly CD ROM and/or DVD or WORM for replay using the VMS video replay application, and shall incorporate proof of authenticity
s. Download video records in common (e.g. AVI) file format for remote, cursory review and assessment prior to generating tamper-evident auditable copies

x. VMS alarm handling

1. The video alarm handling shall provide the following facilities for the handling and management of video images generated by alarms associated with other systems integrated with the VMS.
2. Whilst the pre and post alarm requirement has been included (up to thirty (30) seconds pre alarm, three hundred (300) seconds post alarm per camera at fifteen (15) FPS) the VMS shall display and manage the pre and post alarm information as follows for a maximum of two hundred (200) alarms per day:

a. The pre and post alarm video clip shall be displayed full screen, in real-time and shall continuously play the 'loop' until the operator accepts the initial alarm activation or clears down the event

b. The pre and post alarm shall be displayed on a dedicated monitor
c. Each monitoring station shall be able to display simultaneous alarms
d. The 'video clip' associated with the alarm shall be tagged with date and time etc. and stored in a dedicated location for retrieval at a later date
e. Alarm archived video shall be readily available for one month but accessible for six months
f. The VMS shall accommodate at least 100 simultaneously alarm activating CCTV cameras
g. All alarm based images shall be displayed

3. The VMS shall have the capability to automatically display a primary camera, plus minimum of four additional cameras associated with each alarm based on either camera locations with respect to the alarm, or a programmed set of parameters defining the associated cameras.
4. The VMS shall also accommodate operator-initiated recording of a given camera. The operator-initiated recording shall:

   a. Accommodate up to a total of atleast 50 cameras simultaneously (all operators)
   b. Record the selected camera/s for an administrator configured number of hours or until stopped, whichever is the sooner

xi. VMS Integration requirements

1. VMS shall be integrated within a consolidated GUI that would include other command control Center systems as well. All events, activations and alarms that occur with the VMS and its sub systems will interact seamlessly between the command and control center sub systems as required
2. Either the OPC or the SDK shall manage the interface between the VMS, GUI and the other City Management systems as required.
3. The OPC or SDK shall allow the operator workstations to control the VMS irrespective of the vender chosen by duplicating all control functionality of the VMS used for normal day-to-day activities.
4. Alarm linking between VMS sub-systems shall be done at VMS sub-system level to, for example, call up relevant pictures to screens and move PTZ units to pre-set positions in response to alarm and activate video recordings, modifying recording parameters as necessary.
5. All OPC software shall be fully compliant with the OPC specification as set down by the OPC foundation. Any software or products which are not compliant shall be highlighted in the Technical Proposal return. The SI shall indicate in the technical proposal return how the OPC interface shall be implemented.
6. If an OPC interface cannot be provided, an alternative solution shall be provided for this data using a standard open protocol and confirmation as to how this shall be implemented shall be provided in the technical proposal return.
7. If an SDK solution is provided the system shall allow reconfiguration by (City) and end users without recourse to special languages. A system SDKs shall be supplied with all required supporting software to allow the integration of the system with new devices

and systems.

xii. VMS System Size

The VMS shall enable handling of 50 cameras, on day one, as well as future scalability as may be required.

a. 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.

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

1 Presence detection for moving and stopped vehicles
2 Directional sensitive presence detection
3 Congestion Detection
4 Loitering detection
5 Improper Parking
6 Camera Tampering
7 Abandoned objects detection
8 Gun-shot Detection
9 Unattended object
10 Object Classification
11 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

b. 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.

c. 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.

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

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

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

d. 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 Authority. 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.

e. 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.Data center

1.3.4.17. 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.

1.3.4.18. 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, Data center 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 the *Solapur* including City Surveillance.

1.3.4.19. Implementation of Network connectivity

SI shall ensure that redundant, high quality, seamless connectivity is provided to all cameras across the city. Connectivity to Data center and Command 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 Box camera	ANPR Camera
Resolution (Pixels)	1920 x 1080	1920 x 1080	1920 x 1080
Frames per second (FPS)	25 FPS	25 FPS	50 FPS
Viewing & storage			
Normal Time	25 FPS	25 FPS	50 FPS
No Movement Period / Night Period	12 FPS	8 FPS	As required

SI shall provide adequate bandwidth for each camera to maintain high quality HD 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 Authority:

1. **Provisioning Network Links**
    a. All field locations shall be connected to Data center & 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. **Infrastructure 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 complete infrastructure 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 Authority.
    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 to monitor the non IT components such as UPS, DG set, LT Panel, Air conditioning system, as well through a common dashboard
    m. 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 Infrastructure Management System (IMS) 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 Authority'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. Infrastructure 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 with a prior permission from the concerned authority.

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 Authority 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 Authority.

1.3.4.20. 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 Authority 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 Authority covering all the observations. The same shall be dually vetted by Authority and changes if any suggested shall be highlighted.

The SI shall ensure the observations/ changes suggested by Authority 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 – ICT Enabled Solid Waste Management

1.4.1 Overview

Authority is responsible for collection, segregation, transportation, dumping and processing of the city waste from door to door. Authority has deployed vehicles [*vehicle details*] for collection of door to door waste and dumping into the bins/collection points at strategic [*no. of location*] locations. From these bins/collection point separate 4 wheelers (loaders) carries the waste to the single location called waste processing plant. Also, Authority has approx. [ ] 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 Authority. 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. *Physical visit required to verify employee performance*
5. *The waste keeps lying unattended for several days.*
6. *There is no quick response to urgent cases like truck accident, breakdown, long time idling etc.*]

Authority intends to implement a GIS/GPS enabled Solid Waste Management System practices within the existing landscape to:

1. Manage routes and vehicles dynamically through an automated system.
2. Real time manage of missed garbage collection points
3. Efficient monitor and manage of waste collection bins
4. Do Route optimization which shall help in reduction of trip time, fuel saving and serving more locations
5. Reduce the human intervention in monitoring process
6. keep history of vehicle routes, attended sites and other details
7. 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

1.4.2 Scope of Work

1. Total No. of waste collection vehicles – ~50
2. Total No. of Bins – 200
3. Total No. of Loaders – [ ]

4. Total Field Staff of Authority (PAN City) – [ ]

1.4.2.1 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 ICT based Solid Waste Management System which includes:

ICT Interventions	Key Features
Solid Waste management System	a. GPS tracking of the waste pick up vehicle for real time tracking b. Route Optimization which shall help in reduction of trip time, fuel saving and serving more locations c. Manage routes and vehicles dynamically through an automated system d. Efficient monitoring and management of waste collection bins e. Attendance Management System - Field Staff f. Ensure complete coverage of door to door and community collections served by vehicles g. Monitor and track other municipal corporation vehicles under Solid Waste Management Dept. h. Record history of vehicle routes, attended sites and other details i. RFID devices with vehicle and RFID/QR based tagging of Bin to ensure serving by requisite vehicle j. Weight & Volume Sensor based bin to indicate maximum utilization status and trigger vehicle pick up k. Alert / Alarm management - Real time management of missed garbage collection points l. Monitoring & Reporting Application - reports of vehicles, garbage collection status, bin status etc.

The standards for above should (a) at least comply with the published eGovernance standards, frameworks, policies and guidelines available on http://egovstandards.gov.in (updated from time-to-time); and (b) be of leading industry standards and /or as per standards mentioned at Annexure –XI.

I. Automated Vehicle Locator Management System –

Web Based Vehicle Tracking and Monitoring Application customized to meet the functional requirements of the solution is envisaged. Authority intends to implement the Automated Vehicle Locator Management System of the City Bus Intelligent Transport System with 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/QR code 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. 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.

Ultrasonic or IR based level Sensors to be provided to allow the system to identify the fill level and empty levels in a percentage basis and thereby garbage collection can be scheduled as a function of fill levels at different locations in the city.

Foul smell detection sensors/ Animal repellant sensors to be installed at select locations to the garbage bin to detect the quality of air being released into the atmosphere.

IV. Mobile GPS based Staff Attendance Management System –

GPS based mobile device shall enable Authority'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 feed the data through GPRS/GSM network to the city operation centre central application for reporting generation and alerts.

V. Mobile Device Software Specifications:

The Software should support applications such as:

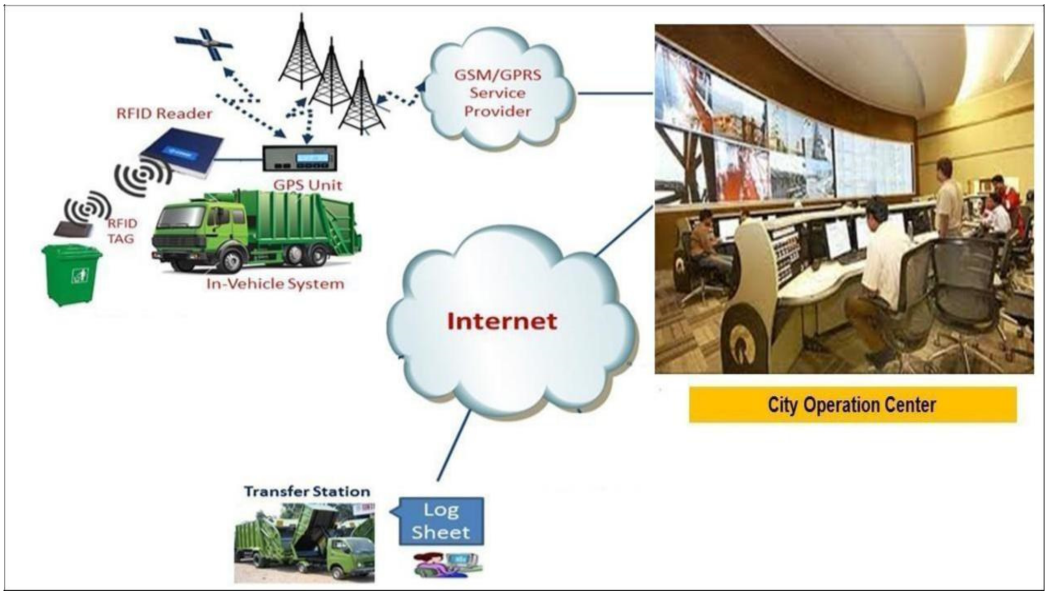
a. QR Code scanning
b. Job completion description
c. Crowd sourcing application for compliant registration and grievances

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 and volume sensors installation at collection point/ bin
e. CCTV Cameras at Secondary and Final Dumping sites
f. Network connectivity for vehicles, bins and city operation center

ICT Based Solid Waste Management System Schematic Solution Overview



Functional requirement for the sensors shall be as under:

Sr.#	Category	Functional requirement
1	Communication	GSM/GPRS or 3G/4G, wifi, or better communication technology.
2	Software	Software should have: a. Over the Air programming interface for realtime program flashing b. Mechanism to change threshold parameters, through remote access c. Data uploading support over standard TCP/IP based protocols d. Support for network and data security e. Configurable sensor periodicities to conserve power
3	Environmental Protection	Compliance to IP67 standard
4	Operating Conditions	Shall comply with all weather conditions.

1.5 SOLUTION 5 – Smart Lighting

1.5.1 Overview

The City has about [No. of streetlights] streetlights installations on poles. Out of these total street lights, [No. of streetlight to be covered under this project] streetlights is under the scope of work for Smart Light System.

These streetlights are to be replaced with Smart LED streetlights/ floodlights. In case the city has already installed LED Street Lights within the identified streetlights, these lights to be integrated with intended 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.
5. Lack of system to enhance security by lighting dark areas in human presence
6. Lack of centralized system to view energy consumption, current light status and real time map based visualization
7. Lack of system to get inputs from other sources to customize control

The Authority 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 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
6. Automatic illumination adjustment based on human presence by triggering multiple lamps to surround the person with a safe circle of light
7. Automatic status updates or failure alerts to remote server
8. Learn the existing occupancy pattern and predict occupancy patterns for future planning

1.5.2 Scope of Work

1. Total No. of Traditional Street Lights: 29202
2. Total No. of High Masts – 556 lights
3. Total No. of LED Street Lights – Nil

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 Light Management System which includes:

ICT Interventions	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
	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.
	Enhance security by lighting dark areas in human presence Intelligent weather adaptive lighting control
	Learn occupancy pattern and predict the occupancy patterns for future planning
	Crowd sourcing or defective light reporting

The standards for above should (a) at least comply with the published eGovernance standards, frameworks, policies and guidelines available on http://egovstandards.gov.in (updated from time-to-time); and (b) be of leading industry standards and /or as per standards mentioned at Annexure –XI.

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
d. automatically switched on /off on the basis of lux level. There should be a manual override and it should be monitored when used.
e. Amount of electricity used in street lighting. There should be information about the amount of natural lux levels and that created by the street lights on a 24 X 7 basis. This analysis would help Authority for allocating the amount of power required for street lights. The same analysis would also be used for changing the source of power to solar power in future.

f. Lux levels along with camera's on the street as well as capacity management report to help analyse if any Light has fused before time (before burn hours as specified in the supplier's documentation.)

g. 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, enhance security by lighting dark areas in human presence, time based scheduling with intelligent weather adaptive lighting control.

h. Learning occupancy pattern and predict occupancy state for future planning.

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

1.6 SOLUTION 6 – Smart Traffic

1.6.1 Overview

Authority is the nodal agency for regulating and managing the entire road network and traffic signals in the city. Currently, there are total [ ] 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

Authority intends to implement a Smart Traffic Management System within the existing landscape 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

1.6.2 Scope of Work

Total No. of Traffic Junctions (with traffic lights) – 16
No. of 5Arm Junction – 1
No. of 4Arm Junction – 12
No. of 3 arm junction – 1

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 Traffic Management System which includes:

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

	Variable Message System

The standards should (a) at least comply with the published eGovernance standards, frameworks, policies and guidelines available on http://egovstandards.gov.in (updated from time-to-time); and (b) be of leading industry standards and /or as per standards mentioned at Annexure –XI.

I. Adaptive Traffic Control System (ATCS) –

ATCS shall offer traffic signal optimizing functionalities, use data from vehicle detectors and optimize traffic signal settings resulting 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 signalized 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 isolated vehicle actuated 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

Health Monitoring should alos be available for the traffic lights with Auto / manual mode of controller,Flash mode or normal mode, Power interruption, Intrusion in controller, Aspect monitoring of traffic lights.

The solution should include following minimum reports:

- Stage Timing report
- Cycle Timing report
- Stage switching report
- Cycle Time switching report
- Mode switching report
- Event Report
- Power on & down
- Intensity Change
- Plan Change
- RTC Failure
- Time Update

- Mode Change
- Lamp Status Report
- Loop Failure Report
- Conflict
- Corridor Performance Report
- Corridor Cycle Time Report

The SI may also be requested to generate additional reports as per city requirements.

1.7 SOLUTION 7 – Smart Parking

1.7.1 Overview

Residents of *Solapur* 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 :

Authority	**Citizens**
1. Increase quality of life 2. Improvement in citizen's parking experience & satisfaction 3. More efficient use of parking 4. Reduces illegal parking 5. Reduces revenue leakages 6. Reduces Man power cost	1. Simplifies Payment 2. Easily finds the parking space 3. Time saving 4. Avoid traffic congestion

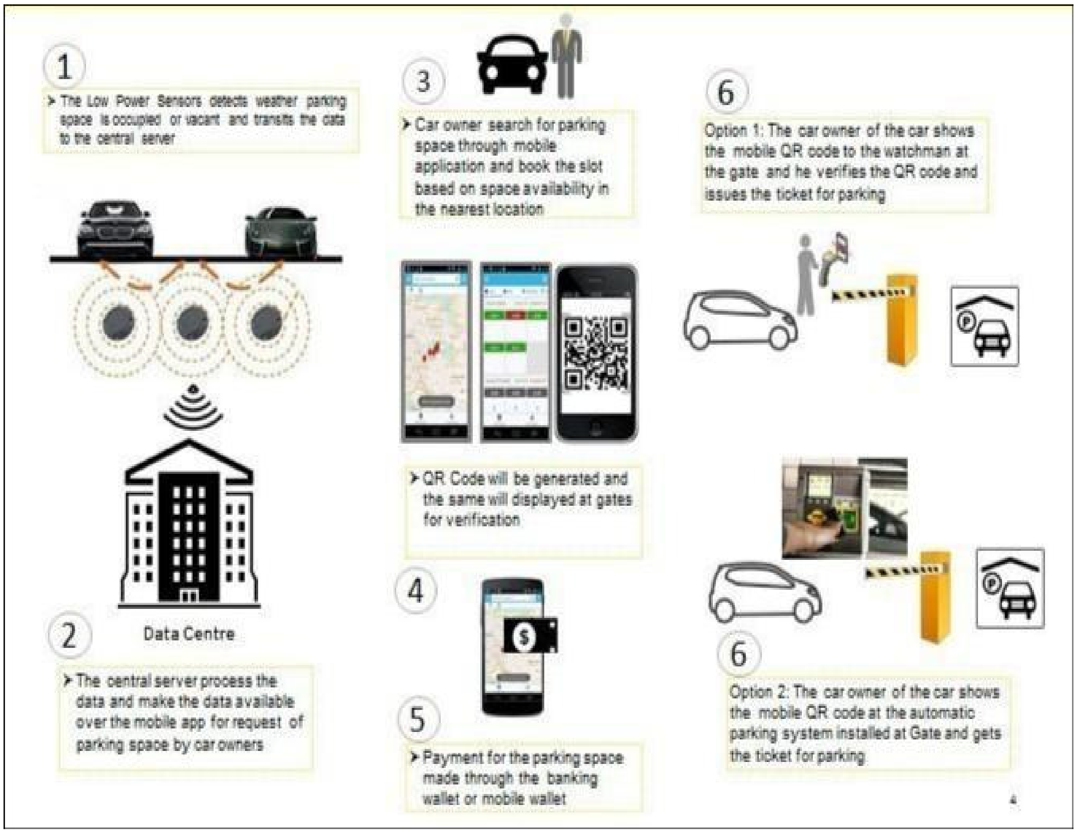
1.7.2 Scope of Work

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 requirement Overview


1
The Low Power Sensors detects weather parking space is occupied or vacant and transits the data to the central server
3
Car owner search for parking space through mobile application and book the slot based on space availability in the nearest location
6
Option 1: The car owner of the car shows the mobile QR code to the watchman at the gate and he verifies the QR code and issues the ticket for parking
QR Code will be generated and the same will displayed at gates for verification
4
Data Centre
2
The central server process the data and make the data available over the mobile app for request of parking space by car owners
5
Payment for the parking space made through the banking wallet or mobile wallet
6
Option 2: The car owner of the car shows the mobile QR code at the automatic parking system installed at Gate and gets the ticket for parking

1. Installation of sensors in each bay, which register whether the bay is occupied or vacant.
2. This information to relay live to local and Central system where parking management application is hosted, which collates and analyses the data.

   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

<u>Smart Parking Key Components –</u>

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

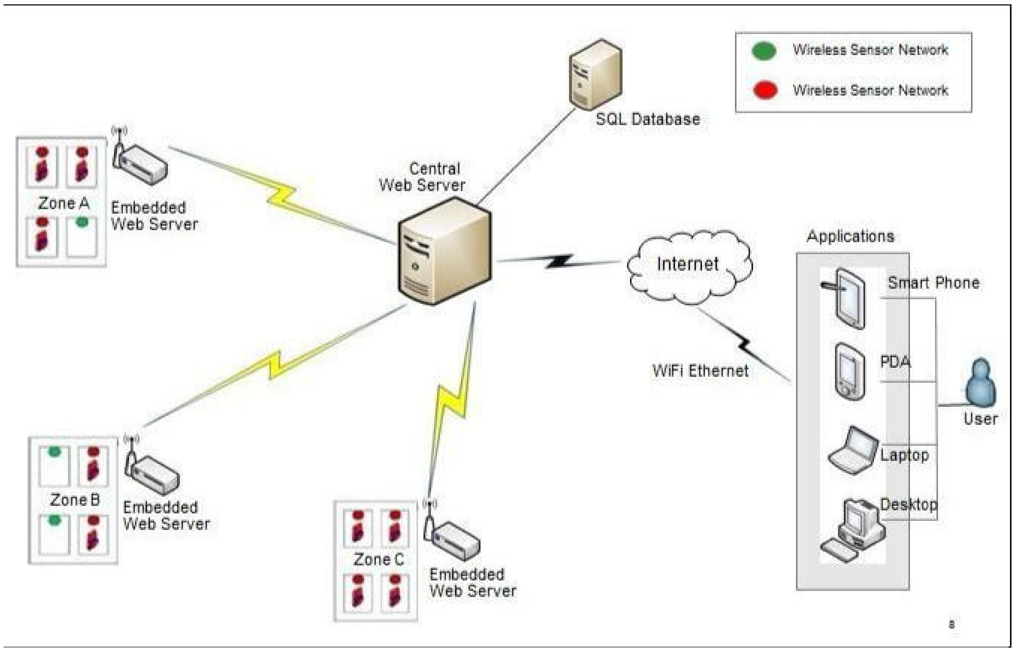
1. Receive parking slot information from embedded web-server
2. Display the parking slots state of parking zone in real-time
3. Send information to mobile phone application
4. Save information in SQL or equivalent database
5. Reporting & analytics

6. Boom Barrier & Digital Display Unit

1. Shall receive information from the Parking Information System and operate accordingly

The standards for above should (a) at least comply with the published eGovernance standards, frameworks, policies and guidelines available on http://egovstandards.gov.in (updated from time-to-time); and (b) be of leading industry standards and /or as per standards mentioned at Annexure –XI.

Smart Parking Technical Architecture –



Parking Management System : Functional Requirement

1. Entry Requirement

i. Entry to any parking space should have outdoor displays/screens showing overall availability of parking slots in that particular parking space.

ii. Each entry lane should be equipped with one Entry Device with the following capabilities:

a) The Entry Device should act as an Automatic Ticket Dispenser
b) It should have touch screen for motorist to enter Unique Booking Number
c) The Entry Device should have Near Field Communication (NFC) capability
d) The Entry Device should have capability to connect with Intercom, microphone, speaker and other subsystems

iii. The ticket, QR Code and Smart Parking Card or any other technology used by SI should be capable of capturing data that is easily retrievable at the exit.

iv. Every vehicle entering the parking space should be stopped by barrier. The barrier is raised when the motorist is issued a ticket or has been identified as a legitimate user.

v. In case the parking lot is already occupied to its capacity, the ticket issuing should automatically be blocked and therefore, the barrier should not open. A message should also be displayed on the outdoor screen stating the same.

vi. The Entry Device should be able to detect and report :

a) Anti-pass back
b) Back-out ticket
c) Low ticket stock

vii. The display on Entry Device should have capability to display messages in English, Hindi and other Regional languages.

viii. The solution should also include provision to capture the image of vehicle and license plate number of every vehicle entering any of the parking spaces using dedicated cameras.

2. Exit Requirements

i. Any vehicle, before leaving the parking area, should be stopped by a barrier system at the point of exit from the parking.

ii. The solution should have clearly instructed easy to use interface

iii. The solution should also include provision to capture the image of the vehicle including license plate number exiting any of the parking spaces and the all the information related to the same should be stored at a central server.

iv. Manual Pay Station:

a) Exit of every parking should be equipped with a manned Pay station (booth).

b) The exit booth should have appropriate space for keeping devices such as a computer with internet connectivity, QR code reader, credit card reader, printer etc.

c) For motorists who enter the parking lot using Smart Parking Card, Monthly pass or any other NFC capable card provided by SI, the exit booth should also have NFC facility for motorist to tap his/her Smart Parking Card for express exit. The payment can also be linked to the e-Wallet of the motorist with auto-debit option and corresponding limits and alerts to the same.

d) The personnel monitoring the exit Pay Station is also required to manually enter the License number details in the system so that the license number, along with date and time of exit, is stored in the database.

e) The payment for parking should be collected based on entry time stamp by any personnel stationed at the Pay Station.

f) The system will calculate the fee automatically and indicate this on the screen clearly visible to the motorist. No manual intervention should be necessary to compute the fee.

v. Once the vehicle exits a parking slot, the total parking slots available in that parking space should automatically get updated.

vi. Only after completing the full cycle correctly the transaction will be considered as valid within the car park. However, audit trail of each complete, incomplete and cancelled transaction should be available in the system.

vii. The solution should be equipped with Anti-pass back technology and be able to detect and report any instance pass back.

viii. The solution should allow full integration of third party devices with the Parking Management and Guidance System, and capture all transactions to generate customized reports.

ix. The solution should track each and every revenue source and should ensure no leakages due to manual intervention.

x. The Pay Station should be capable of charging devices.

3. Entry and Exit Barrier

i. The entrance and exit of each parking lot should have a barrier gate system using technologies such as boom barriers, bollards etc.

ii. The barrier should remain in open position for optimal period of time for the vehicle to pass at entrance and exit.

iii. The solution should also include provision to capture image of vehicle including license plate number of every vehicle entering and leaving any of the parking spaces and the all the information related to the same should be stored at a central server.

iv. Barrier should have capability of in built glowing direction signage

v. Barrier Arms should have the following options:

   a) In closed position the full arm should be illuminated red.
   b) During movement the full arm should be illuminated yellow.
   c) Once reached open position the full arm should be illuminated Green.

vi. Upon horizontal impact by a vehicle, the barrier arm should get detached from the barrier unit with minimal damage to the vehicle and the barrier motor mechanism. An alarm should also be raised and sent to the server and monitoring console, when the barrier is detached.

vii. An alert should be sent to the console and server to ensure that the administrator is informed that the barrier is not attached or barrier breakage.

viii. All vehicular passages during the time that the barrier is not attached should be recorded and displayed in the reports separately in order to audit the necessary revenue transactions during that time.

ix. Upon impact during closure, the arm will stop and stay in the same position. Under no circumstances should the arm re-open upon impact. This is to prevent keeping the arm open for illegal entries or exits.

x. The barrier arm should be easy to refit with barrier unit in a short duration (within one minute).

xi. If for any reason and external override (fire system) needs to be connected, then this should only be possible over the Entry/exit Device and the switch should be permanently monitored by the Parking Management System.

4. Wireless Handheld Device

The solution should include the use of wireless handheld device for on-street and off-street parking. This device shall be used in case of street parking or indoor parking or open parking during peak hours or as a fallback mechanism. However, this device must track every transaction limiting any manual transaction to zero.

i. **Street Parking Mode**:

   a. It should be possible to use wireless handheld devices in street parking model.

   b. On arrival of motorist, it should be able to dispense a ticket

   c. The same device should also be able to function as cash register

   d. The transactions should get uploaded instantly and automatically to the central parking management system using online connectivity.

ii. **Indoor or Open Parking Mode:** In case of high traffic at any of the parking lots or during peak hours, it should be possible for the wireless handheld device to be used as central cashiering device (i.e. it should be possible to scan the QR Code on tickets issued by the entry device and issue receipts post payment, so that the motorists could pay for the parking and then drive out quickly), without any time consumed for payment transactions at the exit.

iii. The device should have capability to print parking receipts and bar coded tickets in real time.

iv. Both the functionality of ticket dispensing & cash register should be possible to be combined in one device.

v. This wireless handheld device should be an online unit, connected in real-time with Command and Control Centre using either Wi-Fi or GPRS. However, in case of network failure, the device should have capability to transact offline and sync with the server as and when connection is restored.

vi. The wireless device to have batteries and power supply along with cradle for charging.

5. Payment options

i. The primary mode of payment for parking will be by cash at the Pay Station

ii. For bookings through Citizen App or Smart Web portal application, payment will be made using eWallet, net banking, credit card, debit card etc.

iii. Additionally, the SI can implement innovative and cost effective payment methods (such as e-vouchers).

Parking Guidance subsystem for motorists

1. Sensors for vehicle detection

i. The sensor should be intelligent and accurately detect if the car space is vacant or occupied.

ii. Appropriate sensors should be chosen based on the type of the parking spot and its external conditions. The preferred sensors would be geo-magnetic sensors, but the SI can propose innovative, advanced but reliable implementation approaches using other sensors.

iii. The sensor should be able to detect a vehicle irrespective of the depth or height of sensor installation.

iv. Each sensor should have its own unique identification in order to be accurately tracked by the Parking Guidance System.

v. Each sensor should have an accurate and real time feedback mechanism to be detected automatically by the system in case of faults.

vi. It should be placed appropriately per parking spot.

2. Parking aisle light indicators

i. Light indicators should be installed for all indoor parking lots for motorist to see the available and occupied spaces from the parking lane easily

ii. Once a parking spot is occupied the total parking slots should automatically get updated.

iii. The fixation of the light indicators to the ceiling should be easy and fast, and should use a quick fastening clips to easy the installation.

iv. The SI may suggest any similar innovative solution for Open Parking and Street Parking.

3. Informative Display Panels

i. The display panels units should indicate available spaces for each parking aisle, bay/zone/level, total parking and should be able to be customized by software.

ii. The display panel should be easy to understand and must have graphical directional and zone status indication (as red crosses for zone full or green directional arrows to guide drivers to zones with available spaces).

1.1.1.1. Smart Parking apps for Citizens

The Citizen App and Web Portal are required as a part of Smart Parking Solution.

a) Vehicle and License Plate Image Capture

i. The solution should have capability to automatically capture details of the license plates of the vehicles at every entry and exit of each parking lot.

ii. The image should be clicked at the entry point when the ticket is issued and at the exit point during payment. The image of the license plate should be linked to the details of the corresponding ticket issued in real- time and stored in the database for one month. This information will be stored in the city operation Centre.

iii. The system checks daily whether the vehicles that have entered the premises but are yet to leave. Thereby Parking management and Guidance system(PMGS) can generate alert if any vehicle is overstaying in the parking lot over 24 hrs.

iv. The SI shall install appropriate cameras at entry and exit of each Parking Lot.

b) Provision for Smart Card

i. Along with the paper ticket, the SI can propose a cost effective smart parking solution to include NFC enabled Prepaid Smart Card system for premium customers and customers opting for monthly reserved parking passes.

ii. The NFC enabled smart card reader would be available at Pay Station and would automatically deduct the required payment towards parking.

iii. NFC enabled smart card solution is implemented, its devices should be able to communicate to the centralized Command and Control Centre, to transmit all parking related information back and forth.

c) Real-time Monitoring and Dynamic MIS Reporting

i. The system should include central reporting system establishing the connection between the devices and sensors, and the centralized Command and Control Centre.

ii. The solution should include reporting dashboards with location specific thresholds to be set for generating customized reports

iii. The solution should be capable of monitoring the number of vehicles that entered or exited the parking premises during any given time

iv. The solution should generate reports for each parking spot, in each of the parking lots capturing utilization, cost, and revenue details, and details of assets, people and etc.

v. These reports should be available in all standard acceptable formats like .csv, .pdf, .txt, etc.

Technical Requirements

Integrated Industry Standard Open Platform should have API based access to the Parking Management and Guidance System as well as the devices utilized for parking. This section gives an overview of the technical requirements, specifications, standards and certifications required for this project.

1) Entry Requirement

i. The Entry of parking lot should have a color LCD display and should be integrated to display to the customer real time parking slots available for parking in English language

ii. The display should have capability to project dynamic digital advertisements. This sponsored advertisement will be relayed from centralized Command and Control Center

iii. Entry Device with the following capabilities:

a) The Entry Device should be capable of dispensing tickets with printed QR Code. The Entry Device should also be capable of scanning QR Code from mobile phones and other devices for Category B to Category F types of reservations. Upon pressing the 'Ticket' button, a ticket will be issued with the following details:

- Entry time & date
- Unique ticket transaction number
- Entry Device identification
- Site identification

b) The Entry Device should have touch screen to allow motorist to enter the Unique Booking Code (alpha-numeric code) received by the motorist in case of Category B to Category F types of reservations. In cases where the motorist enters Unique Booking Code, the Entry Device should dispense a QR Coded ticket with the following details:

- Pre booking authentication code
- Entry time & date
- Unique ticket transaction number
- Entry Device identification

a) The Entry Device should be NFC Ready and should have the capability to read Smart Parking Card, monthly passes, Corporate Cards or any other device.

b) An inbuilt integrated intercom capability should be available in the Entry Device, as an option. The intercom should allow VoIP communication with the centralized Command and Control Center and city operation center. Intercom will be a digitally integrated industrial intercom system, with background noise cancellation technology

iv. Tickets should be fan□folded in stack of about 2 x 7,000 pieces in each device, with advertising capability.

v. Entry Device should be able to switch automatically from one box to the other to ensure continuous feed of tickets from both boxes.

vi. Alarm should be raised when ticket box is about to get empty. And this alarm to be reflected at the monitoring console and server on a real time basis.

vii. All device activity must be logged in the system activity database.

viii. The Entry Device should be able to operate in Offline mode. It will retain maximum functionality even if the communication with the server is not available due to network failure or server crash.

ix. Every Entry Device should have a local memory of a few thousand transactions, in case of no connectivity. Upon reconnecting to the server the unit will update and restore all data.

x. Under all circumstances the system should be fully auditable for every single transaction.

2) Exit Requirement

i. Under all circumstances the system should be fully auditable for every single transaction.

ii. Manual Pay Station:

a. The Pay Station solution should be foolproof and tamper proof with users not allowed to install applications and change any settings of the operating system.

b. It should have all basic operability functions. It should be connected to the Integrated Industry Standard Open Platform via the network and be capable of remote monitoring from the same.

c. The transactions should get uploaded instantly and automatically to the central server using on□line connectivity via Wi-Fi. This should be in a real time mode, rather than at intermitted intervals.

d. It should be possible to have a view of the health check/ status of the entire parking system from a Manual Pay station using a high level administration password or service technician password.

e. Handheld QR Code Scanning Device or any other device used should be connected using a USB Interface

f. Automatic receipt issuing is a must.

g. Operators should log in and out of their shift using a unique authentication password.

h. The system should be capable of accepting all supported means of payment like cash, credit cards, and debit cards.

i. At the end of the shift a shift□report should be printed.

j. It should be possible to accept the validations and issue free or discounted parking for the short term parkers.

k. It should be able to send a report to the validation provider with the amount billed to them automatically at a defined time.

3) Entry and Exit Barrier

i. The barrier at entrance should receive open and close commands from the Entry Device over the communication interface once ticket issue button is pressed.

ii. The barrier at exit should receive open and close commands from the Pay Station.

iii. Barrier should be allowed to be open and close remotely through the server and console with detailed logs associated with this to ensure no unauthorized opening and closing of the barrier is done.

iv. The entry and exit barrier should communicate with the Entry Device and Exit POS over an intelligent communication protocol to ensure that the system cannot be bypassed.

v. Open and closing time for the barrier should be within limits as per latest industry standards.

vi. Barriers should be monitored for collision or forced entry and provide indication to the Integrated Industry Standard Open Platform via its associated Entry Device or Manual Pay station.

vii. The barrier should have 100% Duty Cycle.

viii. It should be a non–hydraulic mechanism for low maintenance.

ix. It should have Self-locking gear system to ensure that the Barrier arm cannot be lifted manually.

x. It should be free of any front line maintenance requirements – no need to grease application etc.

xi. The Barrier should have an integrated two-channel induction loop detector

4) Wireless Handheld Device

i. On arrival of motorist, the wireless handheld device should be able to dispense a ticket (with printed QR Code).

ii. The same device should be able to scan the same QR Code ticket while leaving and generate and print receipt after receiving payment

iii. The Handheld device should have the capability to allow personnel to enter the Unique Booking Code of the motorist

iv. The Handheld device should also have NFC capability to be able to read NFC enabled Smart Card, Monthly Passes and similar other data carriers.

v. The handheld device should be IP based and Wi-Fi enabled, to be included on the secure Wi-Fi network of Smart devices and monitored from the centralized Command and Control Center

vi. This handheld device will have the basic parking metering and management application, which will be synced with the overall Parking Management System, and its data will be communicated back and forth from the centralized Command and Control center

vii. A wireless handheld device should be provided to the parking managers and operators to manage the parking related operations on the ground.

5) Parking Management and Guidance Solution

i. The solution will be implemented in the Integrated Industry Standard Open Platform to manage, monitor and control the Smart parking initiative.

ii. The solution should be able to monitor and configure all devices with respect to parking (sensors, displays, and signal converters).

iii. It should control the system functionality and monitoring should be done from other computers and remotely.

iv. It should provide capability to create full report of exact location with respect to floors, areas, levels, etc. It should be customizable and update about occupation and movements of vehicles in real time.

v. It should provide real time monitoring of all system status.

vi. It should report alarms when devices are not connected or when any equipment failure so it displays on screen alarm.

vii. The software should notify alarms after a period of time if a car is abandoned.

viii. The software should provide full graphical plan information of the car park with exact locations.

ix. The software should allow downloading the information and configuration of fields for maintenance purpose.

x. The software application should have built in tools for third party integration to obtain real time information

xi. Should provide access at user levels with passwords.

xii. The software should have historic log for available spaces, period of time.

xiii. The software should be able to handle manual overriding of available spaces, special parking requirements for reserved spaces and handicapped lots.

xiv. The software should be able to manage energy saving of the car parks according to car park occupation.

xv. The software should be able to reduce brightness of light indicators manually or automatically according to occupation.

xvi. Software should be able to monitor any CCTV camera with IP connection.

xvii. Software should be able to monitor electricity consumption, voltage, energy, and harmonics.

6) Sensors:

i. Sensor should be used for detecting the real-time status of the parking space.

ii. It should be able to upgrade its firmware functionality remotely from the centralized Command and Control Center.

iii. It should be able to permit an optimal angle between the sensor output and the target.

iv. Sensors should be able to work in all weather conditions relevant to the project site.

v. Sensors should preferably have magnetic and optic technology

7) Parking aisle light indicators

i. This feature should be available for indoor parking lots

ii. The light indicators for external view should be high intensity LED which helps the motorist to see the available spaces from the parking lane easily

iii. The preferred parking aisle indicator should be visible from all directions for traffic, and have high intensity LEDs.

iv. Once a parking spot is occupied and the indicator must turn red, the total parking slots available in that parking space should automatically get updated.

8) Indoor LED Display

i. The display panels should have high intensity LED.

ii. The display panels units should receive information directly from same communication line and its update time should be less than 5 seconds to increase/decrease any car availability value.

iii. The display panel should have optional numerical length, i.e., according to each parking, it should be possible to display up to 4 digits

9) **Corner protectors**: Rubber matting with Black and yellow stripes with Installation

10) **Bumper**: Stripped Teflon coated Bumpers at entry, exit and aisles of parking lots

1.8 SOLUTION 8 – Environmental Sensors

1.8.1 Overview

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

The Air quality should be monitored by a network comprising:

- fixed monitoring stations
- Data processing
- Data transmission to a central system
- A central processing system

1.8.2 Scope of Work

The SI should

1. Install environment sensors (as per the functional requirement) to display environment related information at various strategic locations through variable message system
2. The environment sensors shall be integrated with the central control system at City operation center to capture and display/ provide feed on Temperature, Humidity, Pollutants like SoX, NoX, CoX, etc PM2.5, PM10, 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 citizens 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.
6. Develop mobile app for Grievance Redressal of Citizen – where citizen can take the picture, upload the same with Geo Tagging. The complaint should be automatically forwarded to the respective staff, with escalation within specified timelines supported with multilingual text to speech, speech to text and speech to speech systems.

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 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

Functional requirement for Environmental Sensor:

- They should be ruggedized enough to be deployed in open air areas on streets and park
- They should be able to read and report at least the following parameters
  - Temperature
  - .Humidity
  - .Ambient Light
  - Sound
  - .CO
  - NO2
  - Mosquito density
- The sensor should be able to communicate its data using wireless technology
- The data should be collected in a software platform that allows third party software applications to read that data.
- The sensor management platform should allow the configuration of the sensor to the network and also location details etc.

Air Quality Parameters to monitor

- NO2 upto 10ppm
- CO upto 1000 ppm
- SO2 upto 20 ppm
- O3 upto 1000 ppb
- PM 2.5 0 to 230 micro gms / cu.m
- PM 10 0 to 450 micro gms / cu.m Weather Parameters
- Temperature 0 to 100 Deg. C
- Relative Humidity upto 100%
- Light upto 10,000 Lux
- UV upto 15 mW/ cm2
- CO2 upto 5000 ppm

The standards for above should (a) at least comply with the published eGovernance standards, frameworks, policies and guidelines available on http://egovstandards.gov.in (updated from time-to-time); and (b) be of leading industry standards and /or as per standards mentioned at Annexure –XI.

1.9 SOLUTION 9 – City Bus Intelligent Transport System

1.9.1 Overview

Public transport should always be the hallmark of a good transportation system for a city or a state. The role of public transport is vital, particularly to reduce the use of personalized transport. This system should be such that it can work in co-ordination with the existing transportation systems. An efficient mass transportation system is very much needed for sustainability of not only the economy but also for reducing stress due to pollution on the environment.

Public transport management would need to follow a few fundamentals..

1. Easy access to passengers
2. Passengers feeling secured, when riding the transport
3. Cleanliness

The architecture drawn for the same, should consider the entire eco-system. Few of them could be:

1. Security (both IT and Infra security) – On the move and while at the depot
2. Regular maintenance of the buses.
3. Comfort and security to the stakeholders associated

The bus transport's business SLA's should be properly mapped by the ICT infrastructure SLAs. There are 2 primary segments of the System:

1. Management of the buses
2. Management of the transport infrastructure.

Management of the buses include:

- Cameras focusing inside the bus
- Passenger information system (PIS) inside the bus and outside(front, rear and middle)
- Panic buttons to raise an alarm
- Sensors adjudicating if the bus was getting rightly parked on any bus stand (keeping a log of the each no. of parkings, while also helping the driver to park at every bus station on daily route)
- Cameras to manage the Bus stands (passengers vs miscreants)
- GPS for tracking the bus location and their respective timings

Management of the overall eco-system

- Vehicle dispatch & scheduling system
- Bus terminal management system (BMS + Physical Security)
- RFID for the busses and their respective terminal for allowing only the accredited buses.
- Special security governance for the bus crew.
- GPS based fleet monitoring system
- Incident management system reflecting all SLAs and sub SLAs
- Business Intelligence systems to improve business and productivity

<u>Management of the overall eco-system</u>

1. The buses in each of the depots have to be grouped into few no.s, so that the buses can go through scheduled maintainance & repair work and be ready for the duties when asked for.

2. The bus terminals should be secured since so many lives get associated, when the buses are doing its daily duties. A simple and easy technology with some stringent processes can transform an ordinary bus depot/terminal into a substantial secured zone. An access control system shall be provisioned while entering the bus terminal/depot, Access control on the bus door **integrated** with GPS clock. Futuristic plan would be ignition of the bus with the right access control id.

   Management of the tickets and smart cards could be managed better with this solution. All bus stands doors (suggesting closed bus stands) access controls should only open with legitimate tickets and access control. All this would be controlled from either a bus terminal or a central location (secured zone).

   All the repair works and maintenance work (except for some unavoidable circumstances) to be built in-house to ensure more buses availability.

3. Left side of each bus and front side of each bus stand shall have sensors to see if the bus entered and parked appropriately in the bus stand. Drawing a rectangle and a cross in its middle on the road, infront of the bus stand would further help the driver to align.

4. The entire fleet of the buses from each bus depot would be mapped on GPS and tagged for routes. Each route would be mapped as a service and would have SLA's binding them. Deviations would be instantly tracked. In sometime with the start of the service, analysis can be done to improve various aspects of this business.

5. The analysed database finally to be showcased in the –City operation center for various requirements, business policies and future plans

The solution should be integrable to the extent of being called futuristic

1.9.2 Scope of work

The project will consist of design, development, testing, installation, commissioning, training, handholding operations, and management of facilities. This project shall be designed in a manner scalable to larger fleet size, depots and terminals including bus queue shelters.

The City Bus Intelligent Transport System shall bring a state of the art system for enhancement and monitoring of operational efficiency and automation to its transit and other allied operations. The system is expected to meet the Authority's objective of enhancing service standards, better planning and efficient operations; bring in commuter centric services, integration of para-transit, and automation of collection and payment of transit fares, revenue generation services like advertisement system.

the system will deliver the stakeholder requirements by integrating various solutions and technologies onto an integrated platform which will comprise of following distinctive application areas:

S. No.	System	Sub-System
1.	**Vehicle Tracking System**	A. Vehicle Location System
		B. Passenger Information System
		C. GIS information System
2.		A. Schedule Management System

	Operation & Management System	B. Integrated Depot Management with crew allocation and allied services
		C. Business Analytics Module
		D. Infrastructure Management System
		E. Fleet Diagnostic communication and management System (Vehicle Health Monitoring.
		F. Advertisement publishing and management system
3.	**Fare Collection System**	A. On Board and off board ticketing System
		B. Pass/ Smart Card system
4.	**Communication System**	A. EPABX integration System
		B. Crew Communication System
		C. Advertisement and Public Announcement System
5.	**Video Surveillance System**	A. Depot based Fleet video repository and Management System
		B. [Authority] based Fleet video repository and Management System
6.	**Command Centre management System**	A. Integrated Command centre Management with duty allocation and allied services
		B. Web based GIS map editing and GIS Map server management system
		C. Display management system
7.	**Command centre communication system**	A. E-mail server, voice and SMS application and management system
8.	**Green Corridor**	a. Expert charging systems; b. Centralised transportation management systems; c. Decentralised transportation management systems (Linked with 6 above); d. Broadcasting, monitoring and communication systems(linked with 4 above); e. Safety systems; f. E-administrative systems; g. Emissions footprint calculator systems

The standards for above should (a) at least comply with the published eGovernance standards, frameworks, policies and guidelines available on http://egovstandards.gov.in (updated from time-to-time); and (b) be of leading industry standards and /or as per standards mentioned at Annexure –XI.

1.9.2.1 Architecture of the system

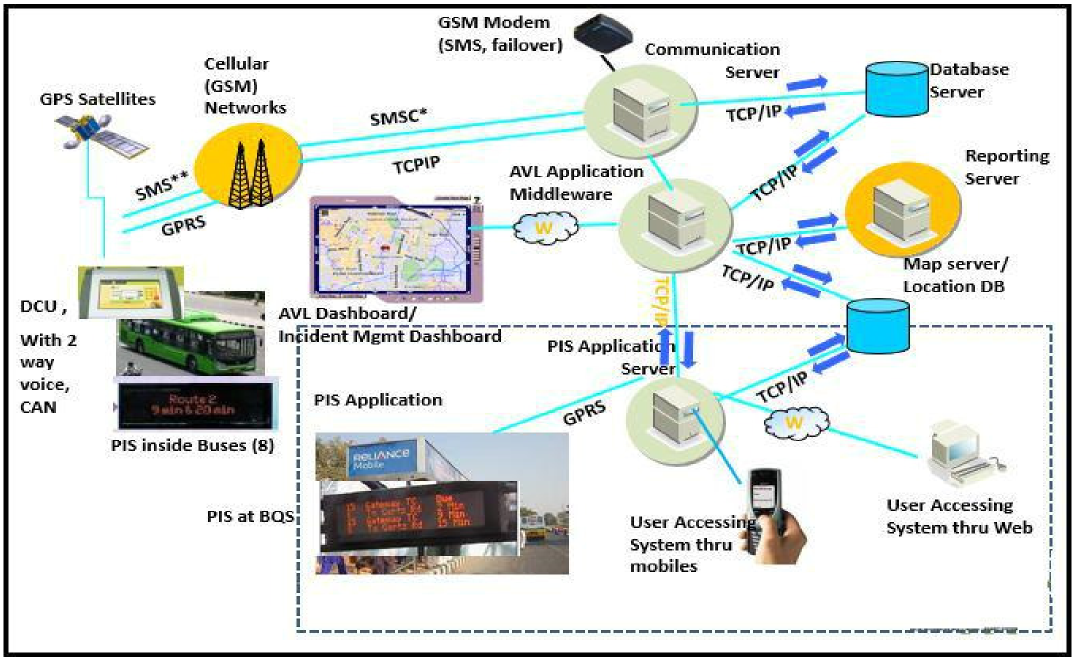
The architecture defines the overall inter connectivity of different sub systems including inside vehicle, communication within sub system and connectivity to backend solutions for the transmission of the real time vehicle information. The functional aspect of the systems and sub-systems are described as under:

1. Vehicle Tracking System

The Track & Trace Communication system will track & trace the location of vehicle running. The GPS based Automatic Vehicle Location System will be used for tracking and tracing the vehicle. The following systems are used for Track & Trace system:

a. Vehicle Location System & Passenger Information System

The Vehicle Location System gives an agency the ability to track, record, and analyze how vehicles are performing in real time. These features lead to improvements in public transit service through better on-time performance and quicker response time to emergencies. The Location information along with other details such as the speed of the bus, the route followed etc. is used to provide the passengers waiting at the bus stops with the expected arrival time of the bus. The information are displayed on boards installed at the bus stops as well as inside the buses using the Public Information System boards , announcement systems, websites, mobile apps etc. The system also helps in improving the efficiency of bus operation by generating various standard and exception reports.



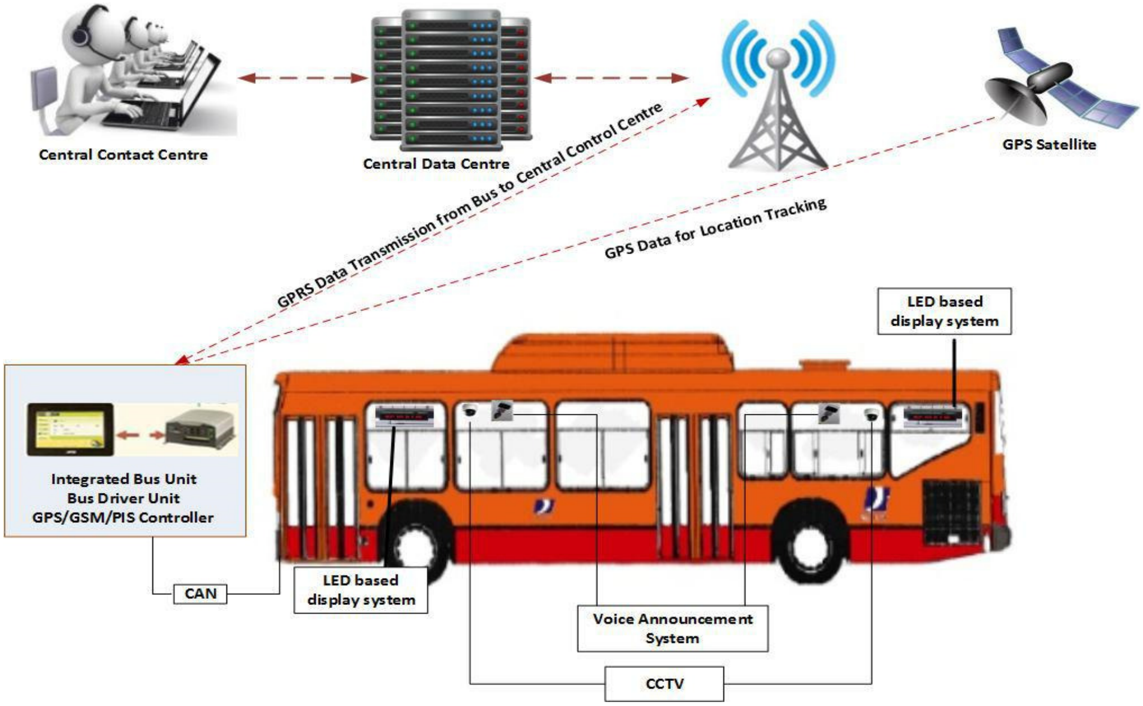
Conceptual Schematic of GPS based Vehicle Location System & Public Information System (PIS)

As shown in the figure above the Vehicle Location system consists of Bus Control Unit mounted on the buses which is used to send location as well as speed data to the central system for tracking the buses. The detail specification of bus mounted units shall be as per Urban Bus Specification II of MoUD, GoI. The Bus Control Unit provides the Location data to the Communication server as part of the City Operation Centre infrastructure which processes the information and saves the data in Database server to be stored and processed for other facilities by Vehicle.

Location System application which displays this information on GIS maps and also provides the location, speed and route data to the Estimated Time for Arrival (ETA) application to generated ETA for various bus stops. The Vehicle Location system will facilitate the Passenger Information System (PIS) to disseminated this ETA information to commuters in various modes like display screens, voice based information on buses and stop/station, web portal, mobile information delivery system, SMS based enquiry system.

b. On-Board System

The GPS/GPRS based bus control unit is an integrated control unit which will control the in bus display boards as well as the announcement system. A bus may have up to four display boards mounted inside to display the upcoming Bus Stop & other relevant information. The ITS system planned for bus operations include following:



Bus ITS Infrastructure Overview

c. ITS at Bus Stop/Station/BQS/Depot /Terminals

As passengers arrive at the bus station/Stop/Depot/BQS, they need information at different stages before their departure. With bus station PIS system, passengers can easily view bus arrivals and departures as well as schedule changes, service advisories, etc. Supply of such GPRS/SMS based PIS system will be in scope of work of the SI.. PIS system will be as below:

- PIS Display on Bus Stations
- PIS at bus stations will be connected through mobile communication to Central Control Centre GIS module to generate the ETA information for various bus stops.
- Web Portal for Bus Schedule & ETA/Mobile Application

The vender will develop integrated PIS system for web portal, Android and IOS and other leading mobile OS. This Application will have provision for advertisement. The SI must develop advertisement publishing and management system.

d. On Board Video Surveillance System

The buses shall have CCTV cameras with local video recording facility. The SI has to develop the Wi-Fi based system (With wifi network at depot) at all depot for daily storing the data and the same will be available to City operation centre immediately.

e. PIS at Depot cum Terminal and Bus Queue Shelter (BQS)

LED based Passenger Information Displays (Stations will have 2 number of LED based display terminals). The PIS information will also be made available via website, SMS and mobile apps. These applications will enable commuters to be able to plan their journey well in advance and will also ensure less waiting time at the stations). Each BQS will have two number of LED based display terminals. The SI shall be responsible for Supply, Installation and Insurance of PIS. All spares required for the smooth operation of the ITS system shall be maintained by the SI for the entire duration of the contract.

2. Fare Collection System

On board ticketing through ETM will be used for city bus system. The ETM machine may be mobile /online based so that the fare collection data is sent to the City Operation centre in real-time. The ETM will be procured by City bus operator as per specification suggested by [the Authority]. The Fare collection system application shall be developed by the SI.

3. Centralized control centre

One Central Control System at City Operation Center will generate the necessary management reports received from the GPS based Vehicle Tracking system and PIS. The Central control center will monitor the movement of vehicles to ensure their adherence to speed limits, routes and punctuality. Central control center will overall monitor and support entire operation like user creation, online support, Depot control centre/other control centre management and Data centre operation etc.

The SI shall develop application module for the smooth operation of Central control center, and shall deploy support and maintenance manpower at the central/depot control center.

4. Operations Management System

The operations management system for the city bus will consists of the following system modules in integrated mode with all other application system module. Basic functional requirement are as follows:

a. Scheduling Management System

The Schedule Management System will provide city bus operator the ability to react quickly to operational problems such as:

- Provide daily Fleet Service Schedule, Maintenance Schedule, pending Insurance and pending Pollution Check status
- Vehicle job cards are prepared based on complaints and scheduled service
- Define schedule of duties in various routes.
- Creation of Conductors and Drivers Duty Roster.
- Allows sending a vehicle in exchange of brake down/detained vehicles.
- Records fuel taken in by each vehicle and provides average fuel consumed per kilometer. Automatic updation of changed Time Table in the Duty Roaster.

- Record each vehicle's scheduled and actual out time from bus stand and depot and scheduled and actual entry time in depot using RFId as well as without RFId.
- Integrated depot management with crew allocation

Application will accomplish a series of specific tasks in the management of any or all aspects relating to a fleet of vehicles. Software, depending on its capabilities, allows functions such as driver and vehicle profiling, trip profiling, vehicle efficiency, etc.

The application will be suitable for any type of reporting structure. Detailed employee database shall be maintained along with the details of salary, attendance, leave and appraisal/promotion of each employee. Personnel module takes care of activities related to existing employees of the organization. Personnel Administration keeps a track of personal details; leave entitlements and PF details of all the employees. Leave entitlements for each leave type with respect to every employee can be tracked. Based on these entitlements leaves are given to the employees. HR Reports shall consist of Employee Details, EPF Details, Nominee Details, personal details, attendance summary and so on.

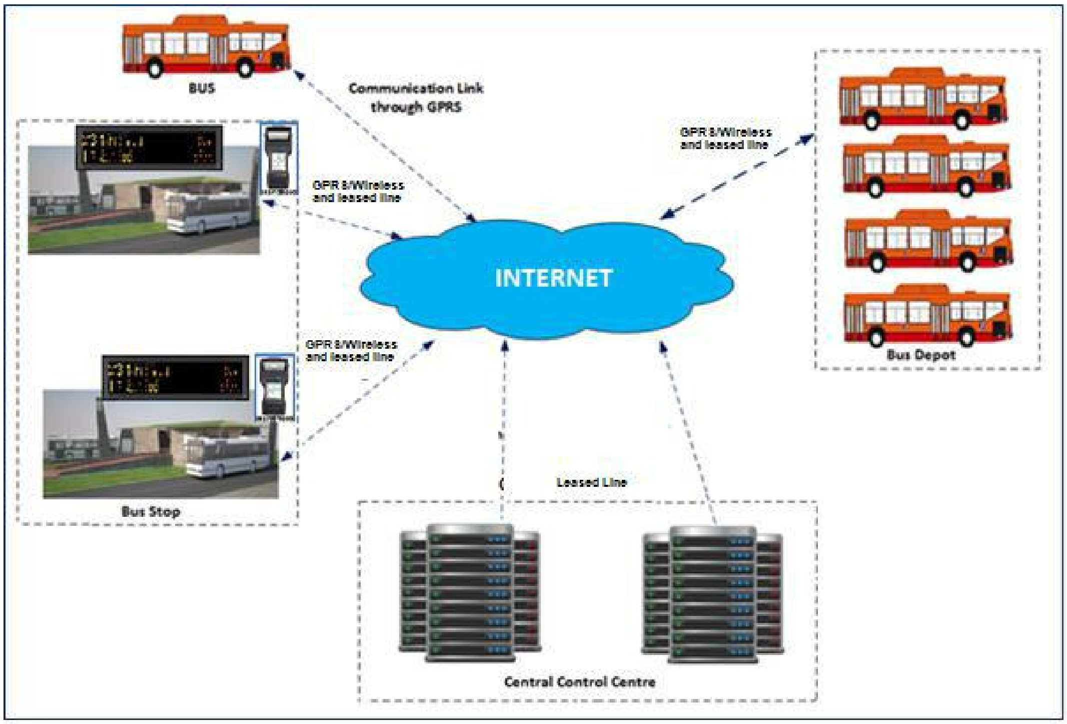
b. Payroll system

The module maintains detailed employee databases along with the details of salary & salary processing. This module will be integrated with Finance. The application will have features including the following:

- Payroll calendar – based on working days/payment days Professional tax according to locations
- Salary Slip Generation
- Category / employee wise salary processing taking into account attendance, salary components, PF, arrears, tax and reimbursements
- PF details of employees
- Periodical Allowances Leave Encashment

5. Communication Overview

The figure below shows a pictorial representation of the communication network plan for city bus system. The communication system design is a very important part of the overall system design as the appropriateness of such design will influence the sustainability and operability of the system as a whole. The communication network depicted above takes in account the operations requirement as far as bus, bus station, depots, terminal's, data centre, control centre and data recovery site is concerned.


BUS
Communication Link through GPRS
GPR S/Wireless and leased line
GPR S/Wireless and leased line
GPR S/Wireless and leased line
INTERNET
Bus Depot
Bus Stop
Leased Line
Central Control Centre

General Packet Radio Service (GPRS)

GPRS is required to be used for services such as Wireless Application Protocol (WAP) access, Short Message Service (SMS), Multimedia Messaging Service (MMS), and for Internet communication services such as email and World Wide Web access.

The information captured by the Bus Control unit is to be transmitted to the control station server through GPRS/GSM/City wifi network creating a communication network between Bus drivers, Bus stops along the road route, and passengers through passenger information system. The communication network is connected to the internet for accessing information regarding bus arrival, routes etc.

A. Overall basic system functional & operational requirement

The bidder will study the complete system including infrastructure, Buses, communications network availability etc. before bidding. The bidder through the study shall get a proper understanding of all aspect of project requirement-which might or might not be detailed in this document or may be added/amended/modified in SRS.

Track & Trace Communication System

The Track & Trace system will track & trace the location of vehicle running. The GPS based Vehicle Location System will be used for tracking and tracing the vehicle. The following systems are used for Track & Trace system. The GIS maps and map server will be developed by the SI.

GPS BASED AVLS & PIS

A General Requirement

i. GPS based Vehicle Location System will provide the following features:

a. Ability to locate a bus at a given time in its track to estimate its arrival/departure time at the next destination, based on traffic density, distance, speed, bus occupancy, run-time information from the previous bus arrival time for the same location etc.;
b. Ability to receive SOS and alerts from moving / stranded buses enroute
c. Facility to track defined vs. actual movement of vehicles, capture deviations if any.
d. Facility to view vehicle movements real-time on digital maps
e. Ability to provide dynamic location specific information as the vehicle approaches bus stop/station for the benefit of passengers
f. Facility to generate information such as travel time estimation, average time at bus stop, passenger traffic at different location, alerts on exceptions, and logging of the journey details of the bus for each trip
g. Facility for citizens to access and view position / location information on GIS maps near real time through web interface with historic data displayed on maps
h. Facility for providing current information location on demand
i. Provide 2-way voice communication between the driver of the vehicle and the control center for receiving SOS and alerts from vehicle
j. Facility for playing back the recorded details of the bus movement along the authorized route
k. It should enable operational managers to create locations, routes, schedules Vehicle service alerts for service and maintenance
l. Vehicle fleet summary dashboard – quick view on vehicle fleet performance
m. Register a bus on unscheduled route from backend on real time basis
n. Exception recording/ actions (over-speeding, off-route detection, non- stoppage at bus stops, trip cancellation)
o. Display of real-time dynamic movement of buses plying on a selected route on map, with real time ETA displayed on stop points plotted on map

The geographical position i.e. Longitude / Latitude coordinates, of each bus stop, Depot and bus station will be identified through a survey by the SI along with details of tourist centres / points of interest / places of attraction / monuments etc. along the route, precise distances between the bus stops in each route by the SI.

AVL system will provide these data on real time basis at pre-determined and configurable intervals over GPRS/wireless networks and shall support both the time mode (periodic updated based on time interval and distance mode (periodic update based on distance interval)

Transmission of Data on GPRS (primary mode of transmission) or City wifi network, SMS (used as back-up)

Facility to configure parameters over the air (should be supported over GPRS/SMS). These parameters include APN, Server IP or Fully Qualified Domain Name and port, Data Update frequency. Domain name registration service will be provided by [the Authority]

Data update rate to server (configurable): Multiple modes to be supported (ACTIVE, NORMAL and STANDBY)

AVL system will support dynamic trip configuration, enabling the crew / control room to activate individual trips, provide route numbers for the UP or DOWN trips.

B Operational Requirement

The web-based system will be capable of data communication with all the system components in real-time.

Uploaded data will not be deleted from device readers or workstations until the central system has provided confirmation acknowledgement that the transactions have been successfully received.

The web-based system will able to update its date and time using time synchronization application of servers. Also the date and time on all system devices and workstations should also be updated.

The SI will manage all device activity including data storage and processing.

All active equipment will have an internally maintained date and time clock that is synchronized using a time interval via the communications medium with the system date and time clock.

The systems will be driven by configurable parameters and should provide the flexibility for maximum configuration. The configurations will be for, but not limited to:

- Time based messages/reports
- User groups and users privileges
- Addition & deletion of equipment’s, nodes, stations, user groups, users
- Configurable messages in minimum English and Hindi languages
- Reports access

The system will handle all degraded conditions which can be, but not limited to the following:

- Any supplied equipment not functional
- Power failures
- Data connection lost
- Central server down
- Bus-station switch non-functional

C Software location playback

The SI will provide all software and hardware (to be housed in data center) that comprise the overall central system, including the required number of licenses for all users.

The software will provide controls to view the entire sequence of reported locations from the beginning of the time period or to step through the sequence incrementally forwards or backwards.

The software will be accessed on workstations and control centers of all user identified by [the Authority]. All communications and AVL data will be stored in a manner that allows direct access by the software for at least 120 days and reporting data for 18 months live in the system. The SI will provide Utilities to support archive and restore functions for older data.

The system will allow replay for a single vehicle, selected set of vehicles or all vehicles or cluster wise vehicle or route wise vehicle on the selected map view for selected time period.

The system will allow selection of any time period for the historical data. All data will be the property of [the Authority] and will be immediately available to [the Authority].

The replay data will include location and headway adherence data.

All users accessing the AVL software will be able to access the playback function.

The system will allow the ability to use playback without exiting from the current AVL operational view.

The system will be able to store a playback in a format that can be exported for viewing on any computer.

All servers will be fully redundant and capable of automatic failover without administrator intervention.

D Graphical Interface

The central system shall be delivered with a fully functioning Graphical User Interface (GUI)

The Graphical User Interface shall be based on standard web based browser controls or an equivalent system.

The system will only be accessible by authorized persons, controlled using login and password protection. The login and password will be a single system for entire system.

It will be possible to create different user classes/categories/roles with different access level.

The system will maintain a transaction log that records all users that access system reports. The pages/reports accessed, edits and changes to the database and the system logon and logoff times. The transaction log will maintain this information for a minimum of one year.

The system security will provide features to maintain data integrity, including error checking, error monitoring, error handling and encryption.

Features will be provided to ensure that all system-created files are uniquely identified, and that no files are lost or missed during data transfer.

System will have verification features to confirm that there have been no losses of data at any point in the transfers.

System needs to be tamper proof and SI would build features to confirm that there have been no unauthorized changes to, or destruction of, data.

Features will be provided to automatically detect, correct and prevent the propagation of invalid or erroneous data throughout the system.

All systems, sub-systems and devices will only allow access to authorized user classes.

All security breach detections will be confidential, and accessible only to users of the appropriate class.

For all data transactions, the system security will include authentication features to verify that all claimed source, recipient or user identities are correct and valid. All data transactions will include non-repudiation features to verify message content, and resolve claims that data was not correctly originated or received by a certain user.

E. Maintenance Mode-Operational Requirement

All the functions that are carried out in the maintenance mode will be reported separately similar to exception transactions

The maintenance mode will be possible to be activated based on a particular node wise.

The maintenance mode can be activated only by a person having the highest user privilege in terms of system operations.

Logins and logouts will be transmitted to the system, along with associated Date/Time, employee ID, equipment ID etc.

It will be possible to upgrade the firmware/ software from the central server using the internet communication available at the station level.

F. Scalability/Future Operational Requirement

The central software will be scalable to accommodate for buses, bus- station/BQS/terminal PIS, without any modifications to the central software except minor configuration changes, the details of how scalable the system is will be provided in the proposal by the SI at the time of bid submission. The minimum scalability will be for 2000Buses, 2000 PIS for BQS and Bus terminal, 50 bus depots. Authority will not pay any excess fees for increase in volume up to scalability.

The software will provide standard reports based on the AVL data. SI will provide details in their proposal related to reports that are offered and the degree to which they can be configured (at minimum all report will be configurable for a specified date/time range and route). Some of the expected standard reports are as follows:

a Headway adherence
b Active fleet (weekday and weekend)
c Service hours and mileage
d Schedule Adherence
e Speed Reports
f Route Deviation reports

The SI will facilitate generation of all the reports necessary to facilitate the payments to the bus operations team/contractor.

The software will have the capability to generate reports based on exceptions as per thresholds set by the Authority staff for various AVL components.

The SI will provide tools to generate ad-hoc reports on stored AVL data.

All reports will use standard reporting tools (e.g., RDBMS or SQL or Crystal Reports etc.) and will have the ability to export data into file formats that can be exported to and edited with standard tool i.e. excel, etc. The SI shall provide the relational database layout including related fields, key fields and definitions for all fields in all tables in the database.

Any portion of the transactional database will be exportable in standard formats (such as comma separated variable (.CSV, xls, xlsx files etc.) for analysis in third party programs.

It will be possible for users to build custom reports from the data in the transactional database with tools such as RDBMS or SQL. The reports will be capable to be exported to pdf, xls, xlsx formats easily.

A data dictionary will be provided to Authority to facilitate development of custom reports.

The Central System will provide sufficient summarized and detailed data including features to generate standard report based on pre-established criteria, as well as as-required reports based on a user-definable set of search criteria.

All reports will be generated using a query language and standard query engine that provides flexibility for future updates, and for creation of new reports.

Reporting software will include the ability to generate graphs and charts based on criteria and format defined by the user.

All reports will be generated with configurable time parameters, including as a minimum annual, monthly, weekly, daily, hourly and with user defined start-end date and time ranges.

The SI will provide an ad-hoc reporting function and interface into the data and reports server to allow Authority personnel to create, execute and receive custom reports without Authority assistance with integration with fare collection system. An Internet-based interface will be provided for this function, accessible by Authority personnel with appropriate permissions. Authority users will be able to generate ad-hoc reports and do additional analysis of ridership, revenue and other System data. The SI will provide Authority’s staff to generate reports and use the system. Examples of the types of reports include:

- Transaction-level reports by stop and for user-defined start and end points;
- Statistical and research reports using user-defined criteria

It will be possible to aggregate data (filter) for reporting, at a minimum, by:

1. Date/Time
2. Origin
3. Destination
4. Location
5. Equipment Serial Number

It will not be necessary that values be consecutive for the purposes of aggregation (e.g. non-consecutive months).

The actual bus operational business rules will keep varying and Authority will share the same with the SI from time to time and the SI has to reflect it in the ITS application for generation of any additional reports etc. The cost of which will be deemed to be included in bidder's proposal.

G Web Portal and Map

The SI shall develop a Modular CMS based website. The user will be able to enter in the route, direction, station/stop ID or select these from a sequence of drill down lists and from a map.

The SI will be responsible for the design and development of the website, including all required HTML, scripting, and integration with the AVL system. The SI will be responsible for the integration and setup of the website. The website GUI will allow for the graphical presentation of vehicle locations on GIS-based maps.

The AVL software will incorporate maps to support the functionality, comprised of a selection of individually selectable theme layers (e.g., stations, streets, names, water features, parks, major buildings etc.). SI may use [the Authority] existing GIS base-map or Google map for this purpose

The SI will provide a GIS based base map for the purpose of the project at at appropriate scale which would be acceptable to [the Authority] operationally

The system will include mechanisms to allow for 6 monthly updates by [the Authority] to the central software maps during the contract period

Develop additional overlay map layers to the external source map that can include polygons (e.g., municipal boundaries, fare zones), lines (e.g., route traces) and points (e.g., landmarks, transfer locations, time-points, stops), with the color, shape and thickness being selectable.

The software will allow users to view the map, including a selectable combination of the source map layers and new layers, at various user-defined zoom levels.

The map display icon for each vehicle location to display as the label the vehicle, block or route.

The display icon of the bus on the map will provide an indication if the latest reported location being displayed is older than the reporting interval or not, to identify packet losses and delay in communication transfer.

The system will track headways at corridor stations for each individual route serving the station, all routes serving the station, and for any user-specified combination of routes serving the station.

The system will highlight to the operator the vehicle IDs of those vehicles that are operating with incorrect headway, using tabular and map displays to indicate their current headway adherence status.

The system will provide a real-time output of the current location and schedule adherence for all fleet vehicles, for use by the next stop prediction software. The SI will document and provide to [the Authority] the communications protocols, command sets and message formats used in this interface.

H Real Time PIS Requirement: Prediction Software

The system will use the real time location and schedule adherence data to create a continuously updated table and XML data feed of the last reported location for all vehicles and the next arrival predictions for all stations/stops.

The system will provide this data table and XML data feed such that Authority and designated third parties have the right to perpetual and royalty-free access, for the purposes for integration with future Passenger Information System (PIS) or other public information methods and importing data into the long term database.

The SI will also provide a data dictionary and entity relationship diagram for the data tables and XML schema documentation. The information required by the algorithm(s) will be manually entered into a prediction support database.

The system will allow the user to configure the prediction support database values.

The percent error for next vehicle arrival time predictions at a given station/stop for a given minute in advance of arrival will be calculated as: absolute value of (predicted time to next arrival minus observed time to next arrival) divided by (observed time to next arrival). For example, if the observed time to next arrival was 7 minutes relative to a predicted time to next arrival of 8 minutes, the percent error would be 1/7 (i.e., 14%).

The LED half-life (time until light output has diminished by 50% from the original rated value) will be a minimum of 100,000 hours

Real time duplex communication to the PIS will be through the GPRS connection to the sign.

The PIS will be able to display a message composed of any combination of alphanumeric character fonts and punctuation symbols. PIS will also allow both Hindi and English fonts to be displayed simultaneously.

I Documentation

The documents to be developed include:

a. Site and System Survey document that shall provide the understanding of the Bidder
b. Hardware Design document that shall provide the solution of the bidder
c. Software Design document that shall provide the details of the software,
d. including the AVL Application Software as per requirements of Authority.
e. System Requirement Specification (SRS) that will detail out the SI system design development, integration understanding and how they map with the requirements.
f. Installation diagrams for all supplied equipment.

The SI shall develop detailed test plans that cover the requirements. Test Plans shall be developed for all components of the project, including and would need to be approved by Authority:

a. Bus Control Unit (BCU) FAT
b. PIS Display Board FAT
c. ALL Application Testing
d. Software Testing
e. Hardware Testing

f. System Acceptance Testing
g. Operations Acceptance Testing

Hardware Requirements

A GPS Based Bus Control Unit (IN Built In All UBSII buses)

The GPS based BCU already installed on all buses.

GPS Based BCU will update the location information like Latitude and Longitude to the central server through GPRS.

The tracking system / GPS Based BCU fitted in the buses will calculate the positions from the GPS receiver and transfer the data to the Control Centre Server through GPRS interface for processing /prediction of arrival time of buses at different bus stops. The GPRS tracking unit fitted in the bus will also transfer the current LAT/LONG data to the bus mounted display for display /audio announcement of Bus Stops.

The GPS Based BCU with wireless communication module (based on GPRS) shall be used to provide vehicle tracking accurately and reliably. The following are minimum list of features required:

a. GPS based BCU will consist of a GPS receiver with inbuilt GPS Antenna, GSM/ GPRS receiver, etc. to enable services such as vehicle tracking, communication and control in connection with a backend control centre system.
b. The device is pre installed on each City Bus fleet vehicle and integrated with all the other in-vehicle ITS functions and hardware being installed (e.g., Automated Stop Announcement Variable Message Signs and Public Address amplifier with speakers, Cellular Data Modem, Transit Signal Priority Emitters, Bus Door Sensors), and will support the data transfer to/from the central system through a commercial cellular data network.

c. GPS Based BCU will be mounted inside the vehicle and shall be vibration & shock resistant, heat resistant, dust resistant and water / rain splash resistant and shall be tamper proof. It should as per to relevant Indian or International standards. The detail specification of BCU will as per JnNURM II guideline/specification.

d. The device will be operated from vehicle battery connection but will preserve battery life by tying its operation and that of the other on board equipment being installed under this contract to the bus ignition switch.

e. GPS Based BCU software will be upgradeable/ configurable. SI support team will help in such firmware upgrade.

f. The BCU within the bus shall be easily accessible for servicing to specified vendor but located to prevent tampering or unauthorized removal. SI must inform Authority for such unlawful activity.

B. In Bus Display System(IN Built in UBSII buses)

This inbuilt Bus display system will have front display board, rear display board, side display board each

The functionality of In Bus Display System is as follows:

a. PIS will be used to display information to passengers at each station along the corridor.

b. The next arrival bus stop information and the current bus stop information will be displayed inside the bus for the passengers based on the location information collected by bus control unit. This information will be sent from the control unit to display system.

c. The display will automatically display the bus stop name and produce audio announcement when the bus reaches a particular stop based on the signal derived from the AVL..

d. The display characteristic will be two lines English /one line Hindi language with upto 6 characters, on front, side and rear signs.

e. Fixed, scrolling and flashing mode (with fixed route number, upto 6 characters, on front, side and rear signs).

f. The detail specification of in bus display system will be as per JnNURM UBS II specification/guidelines.

Driver Voice Communication (IN BUILT in Buses)

Driver will be given an interface for the voice communication.

Communication Headset will be provided to the driver to interact with Central Control Center. The driver will use the two-way communication facility made available to communicate with the central control center. The central control center can also contact any of bus drivers instantly to communicate messages. The driver can also use the audio system for announcing information regarding arrival of bus stations and incident management.

In Bus Voice System

The buses will have the In Bus Voice System functionality. The next arrival bus stop information and other necessary information will be announced inside the bus. This system will be used for any data for the announcement like advertisement etc. This data will be sent from central Voice system to BCU. This in bus voice system will be in turn connected to a speaker.

C. Bus Terminal/Stop/Station/BQC

Bus Stop LED Display

The LED Display unit will display details of arrival and departure information of the buses in Hindi and English. The information of the buses such as Route Number, Bus Number, Terminal, Platform, Bay, Origin, Destination and Estimated Time of Arrival (ETA) & Estimated Time of Departure (ETD) will be displayed in both Hindi and English. The LED units should be GPRS capable with capability to configure the system remotely. The refresh timing for ETA & ETD should be 30 seconds.

The Bus Stop display system standards requirements is as follows:

a. Fitment provision will have to be provided in the Bus Stops along with necessary power supply made available. The source of power will be provided by the concerned department and power bills will be paid by concern department. The Display Unit will source power from here for its operation. Display will be located at a convenient height to have a clear view of the message of next arrival bus.

b. The Bus Stop Displays will periodically query the CBITS through GPRS request.

c. The Control Centre, which receives the current position of all the buses from the Tracking Unit, will disseminate the data received and transfer the relevant information like the Route No, Destination of the bus and the Expected Time of Arrival at that bus stop, to the bus stop display, which has requested for the data.

d. The Bus Stop Display, which receives all such information, will display continuously until the next set of data is received.

e. The Destination will be displayed in two languages i.e. English, and local language.

f. Along with the visual display, the next bus stop will also be announced in English and local language.

g. The Bus Terminal Displays, unlike the Bus Stop Displays will be connected through wired cable with the CS.

1.10 Solution 10: Smart Governance and Citizen Services

1.10.1 Overview

SMART captures the important attributes of Good Governance i.e. Simple, Measurable, Accountable, Responsive and Transparent governance. ICT in governance has been experienced in the form of E-Governance, which redefined the way Governments work, share information, engage citizens and deliver services to external and internal clients for the benefit of both government and the clients that they serve. Governments harnesses information technologies such as Wide Area Networks (WAN), Internet , World Wide Web, and mobile computing reach out to citizens, business, and other arms of the government to: Improve delivery of services to citizens, businesses and employees Engage citizens in the process of governance through interaction Empower citizens through access to knowledge and information and Make the working of the government more efficient and effective Results in enhanced transparency, convenience and empowerment; less corruption; revenue growth; and cost reduction

1.10.2 Solution Required

The components envisaged to be included in Smart Governance are:

a. Stamp Duty & Registration
b. Online Management Monitoring and Accounting System
c. Works & Account Management System
d. Web based Land Management System
e. Legal Management
f. Document Management System
g. Human Resource Management System
h. Intelligent Script Manager
i. Speech to Text

The features under Citizen Services shall include the following:

a. Grievance Redressal System
b. Universal Identity (Aadhaar)
c. Multi-purpose Smart card
d. Utility Services
e. Public & Digital Library
f. Women & Child Safety
g. Assistive living for differently abled
h. Property Tax
i. Registrations & Certification
j. License Facilities
k. Tourism & Heritage

The standards for above should (a) at least comply with the published e-Governance standards, frameworks, policies and guidelines available on http://egovstandards.gov.in (updated from time-to-time); and (b) be of leading industry standards and /or as per standards mentioned at Annexure –XI.

1.10.3 Scope of Work

The SI shall ensure that all the module under Smart Governance is integrated with the overall project. SI shall create enabling platform to link the relevant features with the Citizen Services. [*the SI shall be responsible for developing the Smart Governance solutions for the city and link the same with the citizen services.*] The Smart Governance shall consist of following solutions:

a. Stamp Duty & Registration (GAURI, KAVERI, SARITA)

A model of the BPR to reorient the Department of Registration and Stamps towards 100% automation in the registration process and speedy delivery of registered documents to the citizens. The application suite shall consists of:

- Registration Module
- Valuation Module
- Reports Module
- Vendor Management System (VMS)
- Utilities Module
- Societies, Firms and Marriage Registration Module
- Scan-Archival Module
- Data Transmission Module
- Website

b. Online Management Monitoring and Accounting System

OMMAS, a web based online system for the monitoring of schemes to be established so that all the information related to Release of Funds, Utilization of Funds, Status of Progress of work and quality monitoring reports are available to citizens & govt. officials for viewing & analysis. OMMAS would assist the department official in:

- Preparing the Proposal from the Core Network, scrutinizing by the State Technical Agency (STA) and sanction from respective department
- Capture the monthly physical and financial progress of the work
- Monitor the quality of the work under three stages i.e., In-Progress, Competed and Maintenance by State Quality Monitors (SQM) and National Quality Monitors (NQM)
- Quality of work is monitored using the Mobile based application enabling the monitor to upload the real time photographs of the roads right from the inspection site.
- Accounting modules helps to manage the funds transferred from Ministry of Rural Development to the State Executing Agency and account for the usage of funds in the implementation
- Accounting module also enables to capture the work wise expenditure
- All the accounting reports like Cash Book, Ledgers, Balance Sheet, Schedules, Registers and Monthly Account are generated after monthly closing based on simply posting Receipts and Vouchers.
- Works under maintenance can also be monitored based on periodic inspection of the Pavement Condition Index of the roads

c. Works & Account Management System

Works Management System – an integrated package for Designing, Estimation, Execution, Monitoring & Tracking of Civil Engineering Construction Projects. The key features of the solutions are:

- To generate electronically Contractors Bills, Budget estimates, Monthly Accounts and book keeping as per the statutory governmental procedures.
- Tracking, Processing, Consolidating and Reporting of Financial transactions
- Near real-time Assessment of Expenditure against the Grants/Allotment received as per the budget
- Assess Physical progress of various projects undertaken by the department with regards to the financials.
- Increase the efficiency of individual functional wings of the department.
- Achieve integration with the systems of other line departments/Nodal Agencies such as the AG and the treasuries for submission of data digitally and achieve online reconciliation.

d. Web based Land Management System

Web-based enterprise GIS solution which enables the Authorities / Government, Landowners and Public to access and share requisite information with high level of security and data integrity. The system shall incorporates facility to dole out compensation and enhanced compensation information along with the legalities involved in their business process.

It involves scanning, digitizing and geo-referencing of the Village Maps, Layout Plans, Master and Land use Plan. The spatial data and non-spatial data together with the developed application tools and GIS interface has helped the Administration in various aspects like perusing plot information, finding plot of land to be acquired and maintaining the detailed information with high level of integrity. The web enabling capability has enabled the common citizen to access information related to their plot of land through the Internet.

e. Legal Management

The objective of the solution is to create Trustworthy Digital Repository (TDR) a long term digital preservation environment for the disposed case records through adaptation of Open Archival Information System [OAIS (ISO14721:2003)]. The key features shall be:

- Tracking of workflow of documents and Users
- Correspondence Management
- Customizable Office Filing Environment
- Document Approval and Sign-off Sheet
- Document linking and annotation
- Document Monitoring
- Alerts & Reminders
- Report Generation Tool
- Access Rights Management and Control
- Profile Creation & Management
- Information Extraction, Search & Retrieval
- Graphical/Statistical representation of Information
- Automatic Summarizer
- Security Overlay

f. Document Management System

A Natural Language Processing based Document Management System to manage documents data throughout their lifecycle, right from inception stage through creation, review, storage and finally disseminate all the way to their destruction. The key features shall be:

- Social networking for Enterprise / Organization
- Individuals, Groups, Events areas (based on templates)
- Integrated calendar, activity stream, dashboard, and more
- Communicate ideas, information, events, artefacts
- Through use of pages, blogs, forums, files (image, document, video)
- Through interactive chat
- Powerful framework to build behaviour-analytics, data analytics, etc.

g. HRMS (Human Resource Management System)

The HR function consists of tracking existing employee data which traditionally includes personal Information, Skills, Salary, Leave, Tour Claims, Medical Claims etc.. To reduce the manual workload of these administrative activities, customized Human Resource Management System can be created. Key features shall be:

- Rule based Access control
- Work Flow
- Configurable Policies
- Payroll and Income Tax
- Provident Fund
- Leave Management
- Travel Bills
- Reimbursements
- Pay-slips
- Attendance tracking
- MIS Dashboards etc

h. Intelligent Script Manager

SM V6 will cater to diverse user requirements from word processing, database applications, web based applications, publishing and even custom built software. Whatever applications are available in Microsoft Word, will be available in Indian languages with this software. The keyboard for the languages will also come with a software kit which will be inbuilt.

- Provides the Indian language edge to existing application softwares as well as custom designed applications
- Support from Win 98 to Windows 8.1 for desktops and up to Win 2008 for Network Server for 32/64 bit
- Macros for Open Office, Libreoffice and MS-Word like find-replace, keyboard shortcut, converter, spellchecker, synonym dictionary, official language dictionary, mail merge now also available in UNICODE
- UNICODE sorting of data in Excel, Calc through macros
- Enhanced spellcheckers in [*Hindi, Gujarati, Bengali, Malayalam*]
- Features like insert date & time facility, number to word
- Easy phonetic keyboard

- Apart from BIS Enhanced INSCRIPT keyboard support for popular keyboard layouts like typewriter as well as custom designed layouts
- On screen keyboards to expedite content creation and facilitate learning
- The rupee sign is integrated on Enhanced Inscript keyboard. It is available on third layer. It can be typed using ALTGR+4.
- Documents which are created using ISM V6 are globally usable
- Convert data from various font encoding to Unicode
- nTrans is able to convert data (proper nouns) from English to Indian Language Unicode and vice versa

i. Speech to Text

Develop a speech recognition system keeping in view the local language such as ShrutLekhan-Rajbhasha, a Hindi speaker independent, continuous speech recognition system that enables a machine to recognise human speech and provide an output in Hindi Unicode.

1.14 Operation Centres

1.14.1 Overview

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

1. City Operations Center cum Integrated city operation (Internet of everything-IOE)
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
Surveillance Command Control Center with Data center	As specified by *Solapur* Police specified	*Solapur* Police
City Operations Center cum IOE platform with Disaster recovery center	As specified by Solapur Municipal Corporation	Collector Office
Network Operations Center and Help desk (NOC)	As specified by the Authority *NOC and Helpdesk is proposed to be co-located with City Operations Center*	System Integrator
Mobile command control center	As specified by *Solapur* Police specified	*Solapur* Police

Note: In case the bidder chooses to collocate the Smart City Infrastructure in a Third party Tier-3 data center, then Data center will not be housed in the same locations of City operation center and Comand and control center

The standards for above should (a) at least comply with the published eGovernance standards, frameworks, policies and guidelines available on http://egovstandards.gov.in (updated from time-to-time); and (b) be of leading industry standards and /or as per standards mentioned at Annexure –XI.

1.14.2 Surveillance Command control Center

Overview

The Surveillance Command control 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 command control Center shall be accessible by the operators and concerned authorized entities with necessary authentication credentials. The command control Center shall be used and manned by the [Police] team to keep surveillance on civil issues.

Location for Command Control Center shall be at the designated location as decided by the Authority. The main data center infrastructure of the entire smart city components will also be housed here for which the Authrity will provide space and power to the SI

The Command Control Center shall provide a comprehensive system for planning, optimizing resources and response pertaining to the standard functions of [the Authority]. The minimum technical specification for the equipment required at the Command Control Center is listed in this RFP (in the section 1.3).

The SI shall be required to undertake detailed assessment of the requirements at the Command Control center and commission required IT and non-IT infrastructure and also carry out the civil/ electrical work as required.

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.

The video feed from the surveillance cameras shall be received at the command control 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.

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

1.14.3 City Operation center

1.14.3.1 Integrated City Operation (Internet of Everything - IOE) platform

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.

IOE Platform involves leveraging on the information provided by different devices/ platforms & various departments and providing a comprehensive response mechanism for the day-to-day challenges across the city. IOE shall be a fully integrated portal-based solution that provides seamless incident – response management, collaboration and geo-spatial display.

IOE 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 (IOE) provides a Common Operating Picture (COP) of various events in real-time on a unified platform with the means to make collaborative and consultative decisions, anticipate problems to resolve them proactively, and coordinate resources to operate effectively.

The IOE platform should have high processing power and adequate data storage with a high performance information highway to provide process information in real time and serving decision support system. The IOE platform should also provide portability to meet changing city scenario. The SI is required to provision data storage and processing power of the platform adequately to meet the system design and functionality to be achieved.

IOE 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 Solapur Smart City Initiative it is intended to cover and integrate various disparate systems including:

- City WiFi
- City Surveillance and Dial 100
- Smart ICT based Solid Waste Management
- Smart Lighting
- Smart Traffic
- Smart Parking
- Smart City Bus Services
- GIS Application
- Smart governance

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

- Water Management

- Open City Card
- Smart Health
- Disaster Management

The proposed information should be sharable on intra city and inter cities levels based on approved rights on mutual consent.

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

The city Operation center will also provision for the monitoring and control for smart city components other than City Surveillance. However, the Authority intends to provision for city surveillance monitoring cum viewing for critical field cameras and other security equipment as per the city's requirement. Moreover , all this will integrate into IOE platform..

i. The inputs/feeds from the different components of Smart City Solutions 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 beworking on their respective monitors for assessing the inputs and triggering actions at ground level.

Types of Operation: Normal Operation

Normal operation is operating the services as per pre-planned operation schedule or methodology. Under normal operating conditions various members of Operations team shall coordinate their activities and exchange information through voice and data communications systems about the equipment / facilities under their supervision to facilitate a safe and secure arrangement throughout the city.

Under the normal condition, the operations team shall continuously supervise the main assets and identify any fault, anywhere in system promptly. Operation team shall isolate faulty element and operate the system in manner to arrange alternative wherever appropriate alternative is possible (element redundancy, rerouting of services, alternate feeding path etc.). Faulty elements are further referred to appropriate team for corrective action.

CCC framework shall enable faster isolation of faulty elements & identification & implementation of inbuilt alternatives in system.

Degraded Operation

Degraded modes of operation occur when certain systems fail to meet the levels of service that is expected of it. In such scenario the applicable Standard Operating Procedure (SOP) would be followed

For example: Various failures in power installation may affect as under

- The distribution of power in various sectors of the city. Load shedding need to be planned looking at many aspects, one of the few could be
  - Industries
  - Student exams
  - Hospitals

Emergency Operation

In a smart city the emergency situations, need to be averted beforehand…

Emergency operations are enforced in case of an unforeseen or abnormal situation, when it's not possible to carry on the services.

An emergency or disaster is a sudden or great calamity leading to deep distress affecting men and machinery. Many of the accidents / incidents like an act of vandalism, terrorist attack, an accidental fire, critical system failure, force majeure etc may lead to crisis / disaster.

In cases of disasters, the main objective is to disperse the affected persons, as early as possible, from the affected site of occurrence and avoid loss of life and properties. Management of such situation requires sharing of clear and accurate information and necessary actions shall be initiated without any delay to ensure the restoration of normalcy.

- This requires seamless & timely sharing of information amongst multi-disciplines (viz. Traffic, Engineering, Electrical, Signal & Telecommunication etc.) involved in Operations and
- Necessitates that appropriate actions are initiated without any delay and the situation is tackled in the most appropriate and efficient manner, so that distress is relieved expeditiously

Thus, for effective management of such scenarios, it is preferable to have visibility and ability to manage critical disciplines at one place.

CCC framework shall support Automation of Disaster Management Procedure.

CCTV Cameras throughout the city and analytical tools would perform the emergency operations ONLY during this situation.

The City Operation Center location will also house Smart city infrastructure as 100% DR Site. The authority will provide the space and power for the same to SI.

1.14.4 GIS Map for Solapur City

SI shall be responsible for providing GIS map of Solapur city which shall be a common platform across all the solutions including City WiFi, City Surveillance, Smart Lighting, Smart Traffic, Smart parking, ICT based solid waste management, City **bus** intelligent transport 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 bunks, 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.
- o The application shall support client requests to print the spatial data.
- o 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.
- o The system shall support geocoding and reverse geocoding
- o 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 Command control Centre and City Operation center . 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.

1.14.5 Network Operations Center

As part of this RFP, it is proposed that a Network Operations Center alongwith help Desk (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 [the Authority] 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 Authority / authorized entity.

The overall Scope of Work (SoW) for the SI includes the following:

a. Design, supply, installation and O&M of the necessary Network management application in City Operation Centre including 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. The hardware and application software shall be housed in DC and DR infrastuctyre.

b. SI shall take consultation and approval of Authority/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
- o Performance Management
  - § Provide efficient performance management procedures ensuring a reliable, high-quality network performance and service
- o Service and Network Provisioning
  - § Define all necessary actions to be performed when a request for a new service is issued , and control the actions performed at NOC level or field level until completion
- o 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
- o IT and DB Management
  - § Day-to-day management of all OSS systems, IT systems and databases (administration, backups)
- o Security Management
  - § Define and implement security policies, guidelines, and best practices, and check for compliance with security regulations
- o Quality Management
  - § Define quality management policies, and ensure implementation and usage for competitive quality of service o

Workforce Management

- § Manage field personnel to ensure timely interventions and respect of the preventive maintenance plan
- o Network Inventory Management
  - § Ensure consistent management of network equipment, and accurate, up-to-date documentation of it
- o Spare Parts Management
  - § Manage spare part handling and logistics to minimize repair/swap turn-around times for defective items, & keep low CAPEX for spare partsand consumables
- o Asset Inventory Management
  - § Ensure consistent inventory management for all assets including infrastructure, buildings, tools, spares, and equipment

- o Repair and Return
  - § Receive and repair defective boards, return repaired or replacement boards.

The SI shall ensure adherence to the following prerequisites:

a. All the IT 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. It should also be provisioned to bring Non-IT components on the common monitoring

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 of respective project phase by the Authority. The individual project phases will run independently. However, the 5 years of O&M shall start only after handing over and acceptance of complete system by the Authority.

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 Authority.

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 and Non-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 SI shall ensure that all resident engineers in the NOC are certified (of the OEMs of the network components) and are provided at City Operations Centre for 24/7 operations.

j. 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 WAN/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, 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 environment.

x. SI shall perform LAN/WAN problem determination.

xi. SI shall communicate changes affecting the LAN/WAN environment.

xii. SI shall maintain LAN/WAN 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.

xv. SI should provide the detailed plan towards DR site with all responsible people details.

k. 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.

1.14.5.1 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.

1.14.5.2 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 Authority. 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 (T and Non-IT) 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 Authority. 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 SI 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 component and services provisioned 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 and Non-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 Data center 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 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

VII. Traffic analysis

a. The proposed system shall enable the Data center to centrally manage user access privileges and allow deploying baseline security polices 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:
   - 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
   - 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.

- 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.
- 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.
- 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 (IT and Non-IT), 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 the Govt. of [State]. 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.

Root Cause Analysis (RCA) shall be conducted by the SI.

j. 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 the Govt. of [State].

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 to report desired SLA's for availability & performance of Various IT and Non-IT Components including Networks, Systems, OS, Power, UPS, DG set, access control etc . 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

1.14.5.3 NOC Operations Location

Location for the NOC shall be specified by [the Authority]. 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 50 seats in the NOC room of approximately 3000 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.

1.15 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 Authority/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 …. seater helpdesk at Command Control Center and a minimum of …. 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:

Category	Shift	Type of Helpdesk Support	Type of Field Support
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-Premises	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

Post implementation requirements :

Quality Assurance plan

The Quality Assurance Management process will be implemented in a structured and professional manner throughout various stages of the Project. It is intrinsically linked with the provision of safe and reliable systems since the application and control of applicable processes is the fundamental mitigation against systematic error. Achievement of ISO 9000 is the most common metric available to companies and an ISO 9001 compliant design methodology provides a high level of confidence that Quality Management is adequately implemented

System configuration management:

The system configuration management activity shall be carried out by the SI and will comply with the principles depicted in the System Configuration Management Plan.

The SI shall produce a System Configuration Management Plan to cover change control that occurs during the development phases and at the same time monitor the system configuration.

The System Configuration Management Plan shall address the configuration management in terms of configuration, change control, problem reporting, media control and appropriate configuration management tools.

Reliability Critical Items list should be made. Critical items are defined as System/Subsystem/Component, failures, which result into the highest disruption to service when ranked with other equipment in any system. This ranking will be based on the RAM (reliability, accessibility and manageability) analyses. Ranking severity will be considered for the number of instances, which would delay a service, due to the failure of the equipment.The length of the delay in any smart city schedule and the time taken to fix the failure would affect the criticality. The criticality of the item will also be based on the effect of that single item on the entire system.

The assessments include Failure Mode, Effects and Criticality Analysis (FMECA), Interface Hazard Analysis, Quantified Risk Analysis and quantitative analyses. It is recommended that the quantitative analyses be performed using Event Tree Analysis, Fault Tree Analysis or availability simulation modeling. ,

Class	Types of failures and incidents	Definitions

4	Significant	The failure leads to an incident that requires evacuation or immediate attn. to people, while restoration of the operation could take a long time, or lead to a delay greater than 30 min.
3	Major	The failure leads to a disturbance of the operation with a significant loss of missions degrading regularity and “offered service”. A delay greater or equal to 3 min but less than 30 min is suffered.
2	Minor	The failure leads to a disturbance of the operation with a delay. A delay greater or equal to 1 min but less than 3 min is suffered.
1	Negligible	The failure has no immediate consequence on the pursuit of the missions but may lead to an intervention in corrective maintenance.

1.3.4.21. 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 to the Command Control Centre shall also be there where possible.

1.16 Site Preparation for Command Control Center, Data center, 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 Data center, City Operation Center along with Data center, Network Operations Center and Helpdesk as per the requirement in consultation with the Authority but not limited to the following:

1.16.1 Civil and Architectural work

The scope for civil work in this RFP is to furnish the Command Control Center, City Operation Center and Data center, 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

1.16.2 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.

1.16.3 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.

1.16.4 Electrical Distribution System

The SI shall be responsible for proper and uninterrupted working and shall ensure this by having the Data center 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.

1.16.5 Air Conditioning and Natural Convection

Since Data center 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.

1.16.6 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 Data center. The specifications of UPS are provided in this RFP.

1.16.7 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.

1.16.8 Electrical work for Data center

The electrical cabling work shall include the following:

- Main electrical panel in Data center
- 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

1.16.9 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 Data center environments) fire suppression system appropriately sized for the given size of the Data center.

1.16.10 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.

1.16.11 CCTV system

The SI shall provide CCTV system within the Data center and Command and Control Center on 24X7 bases. All important areas of the Data center, 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.

1.16.12 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.

1.16.13 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.

1.16.14 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 [the Authority] & Police staff shall be a part of Capacity Building. It is important to understand that training needs to be provided to each and every staff personnel of such operation centers. 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 Authority/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, Smart lighting, Smart traffic, smart parking, smart public transport' 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 Operation centers data centres , , & field Locations. End user training shall be conducted at a centralized location or any other location as identified by Authority 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 Authority 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 Authority 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 Authority 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 [the Authority] 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. Authority 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 Authority/authorized entity to review and track the progress, In case, after feedback, more than 30% of the respondents suggest that the training provided to them was unsatisfactory or less than satisfactory then the 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' 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

Authority 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 50 identified locations

b) City Surveillance - Supply, installation, commissioning, training & operationalization of City Surveillance at 50% of total 100 identified locations

c) Supply, installation, commissioning, training & operationalization of City bus intelligent transport, smart parking, smart traffic, Environmental sensors, Waste Management and Smart governance.

d) City Network Backbone – Deployment, installation, commissioning, training and operationalization of zonal layer for city network backbone

e) Design, supply, installation, commissioning including interior civil work & operationalization of Command Control Center and City Operation Center along with DC and DR

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 50 identified locations

b) City Surveillance - Supply, installation, commissioning, training & operationalization of City Surveillance at additional 50% of total 100 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 and other solutions

3.1 Project Deliverables, Milestones and Timelines

S. No.	Milestone	Deliverables	Timelines (in Months)
	Phase 1		T + 6 months
	Project Initiation	Detailed Survey Report including infrastructure assessment, phase wise location distribution, hardware deployment plans etc. . Detailed Project Plan including Operations management, Contract management, Risk management, Information Security and Business Continuity	**(in months)**
	Smart Traffic, City Bus, Parking, Solid Waste, smart governance		**T+6 months**
	Supply, installation, commissioning, training & operationalization of Smart	Delivery Report, inspection reports (component - wise) •Site Completion/readiness Report •Software Licenses •Training Completion Certificate • Acceptance /Go Live Certificate from Authority/authorized entity	T+6 months
	City Wi-Fi		T+6 months
	City WiFi Supply, installation, commissioning, training & operationalization of City WiFi at 50% of total [ ] identified locations	Delivery Report, inspection reports (component - wise) Site Completion/ readiness Report Acceptance Certificate from Authority/authorized entity	T+6 months
	City Surveillance		**T + 6 months**
	City Surveillance - Supply, installation, commissioning, training & operationalization of City Surveillance at 50% of total (……) identified locations Deployment, installation, commissioning, training and operationalization of zonal layer for city network backbone	Delivery Report, inspection reports (component - wise) Site Completion/ readiness Report Software Licenses Acceptance Certificate from Authority/authorized entity (components wise) Site Completion/readiness Report Software Licenses Acceptance Certificate from Authority/authorized entity	T+6 months
	City Network Backbone		
	City Network Backbone – Deployment, installation, commissioning, training and operationalization of zonal layer for city network backbone	Delivery Report, inspection (component - wise) Site Completion/readiness Report Software Licenses Acceptance Certificate from Authority/authorized entity	T+6 months
	Command Control Center & City Operation Center		**T + 6 months**

S. No.	Milestone	Deliverables	Timelines (in Months)
	Design, supply, installation, commissioning including interior civil work & operationalization of Command Control Center and City Operation Center including data center and DR center, Network Operation Center and Helpdesks	Delivery Report, inspection reports (component - wise) Site Completion/ readiness Report Licenses Acceptance Certificate from Authority/authorized entity	T + 6 months
	Phase 2		
	City Wi-Fi		
	City WiFi - Supply, installation, commissioning, training, operationalization & Go Live of City WiFi at remaining 50% of total [ ] identified locations	Delivery Report, inspection reports (component - wise) Site Completion/ readiness Report ·Licenses Training Completion Certificate · Acceptance /Go Live Certificate from Authority/authorized entity	T + 10 months
	City Surveillance		
	City Surveillance - Supply, installation, commissioning, training, operationalization & Go Live of City Surveillance at additional 50% of total [ ] identified locations	Delivery Report, inspection reports (component - wise) Site Completion/ readiness Report Software Licenses · Acceptance /Go Live Certificate from Authority/authorized entity	T + 10 months
	Phase 3		
	City Network backbone		T + 12 months=T1
	Deployment, installation, commissioning, training and operationalization of for city City-WiFi,City Surveillance and other smart solutions	Delivery Report, inspection reports (components wise) Site Completion/ readiness Report Licenses Training Completion Certificate Acceptance /Go Live Certificate from Authority/authorized entity	
	Operations and Maintenance phase		T1 + 60 months
	Operation & Maintenance	SLA Compliance Report	Every Quarter

Note:

- ***T is the date of signing of contract***
- ***T_1 is the date of Go Live of the last Phase***

3.2 Payment Terms and Schedule

1. The request for payment shall be made to the Authority in writing, accompanied by invoices 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 Authority, 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	T1 = T + 12months	10% of contract value
4.	Operations & Maintenance phase for a period of 60 months from the date of Go Live of the last solution	T1 + 60 Months	60% of Contract Value in equal quarterly installments

Note:

T is the date of signing of contract

T_1 is the date of Go Live of the last phase.

4. Annexures

Annexure I: Indicative list of City Wi-fi Locations

Sl. #	Area within the city	Wifi Locations in the area

Annexure II: Indicative List of City Surveillance Locations

a. Name of police station and locations

Sl. #	Name of police station	Location	CCTV Camera (PTZ)	CCTV Camera (Fixed)

Annexure III: Solution Requirement - Locations:

S. No.	Solution Requirement	Indicative no. of locations
1	PTZ + Fixed Box Camera (including Critical Locations)	16
2	Automatic Number Plate Recognition	16
3	Red Light Violation Detection	16
4	Public Address System	16
5	Variable Messaging	16
	Thermal Camera	16
	Facial Recognition System	16

Annexure IV: Indicative length of City Network Backbone

Details on City Network Back bone

Sl. #	Area within the city*	Length of the network to be laid
		Total (KM)

* Enclose a map showing area and alignment of network to be laid

Annexure V: Proposed locations for Zone aggregation points

Sl. #	Location	Approximate Coordinates

** This would be 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 list of Environmental Sensors installation locations

Sl. #	Indicative list of Environmental sensors installation Locations

Annexure VII: Locations for Smart Lighting

Sl. #	Locations of smart lighting (number and location)

Annexure VIII: ICT based Solid Waste Management System

A. Location of Secondary collection points

Sl. #	Locations of secondary collection points

B. Location of Bins (to be RFID tagged)

Sl. #	Locations of secondary collection points

C. Category wise fleet size for Solid Waste Collection and Transportation

Fleet Size	
Type of vehicle	Number

Annexure IX: Locations of Parking lots

Sl. #	Area/Location	Name of Parking lot	Possession	Space for four wheeler	Space for two-wheeler

Annexure X: Information on City Bus Services

A. Category wise fleet size

Sl. #	Fleet Size	

B. Number and Location of Bus stops (alongwith Map)

Sl. #	Bus Stops Locations

C. Location of Bus depots (alongwith Map)

Sl. #	Bus Stops Locations

Annexure- XI: Standards and Guidelines

Contents

Annex-A (BioMetrics Standard)

BioMetrics Standards

The Indian Government proposes to use biometric data for identification and verification of individuals in e-Governance applications. The biometric data includes fingerprint image, minutiae, face image and iris data.

The Indian e-Governance applications will have both biometric identification and verification phases, to ensure there is no duplication of identity and to verify the identity of a person for access to the services of the application.

1) Face Image Data Standard

Manual Facial recognition is not sufficient currently for de-duplication. . Computer based face recognition has reasonable accuracy under controlled conditions only. Hence for de-duplication purposes, other biometrics like finger print/iris image is also recommended.

With the objective of interoperability among various e-Governance applications, the face image data standard for Indian e-Governance Applications will adopt **ISO /IEC 19794-5:2005(E)**. While the ISO standard is broad to cover all possible applications of computer based face recognition and human visual inspection, this standard is more restrictive, as it is limited to human visual inspection.

The ISO standard specifications are tailored to meet specific needs of civilian e-Governance applications by specifying certain prescriptive values and best practices suitable in Indian context.

Standard	Description
ISO /IEC 19794-5:2005(E)	This standard includes capture and storage specifications of face images for human visual inspection and verification of the individuals in Indian E-Governance applications. It specifies a format to store face image data within a biometric data record compliant to the Common Biometric Exchange Formats Framework (CBEFF), given in ISO 19785-1. It also includes best practices recommended for implementation of the specifications in different categories of e-Governance applications. The scope of this standard includes: o Characteristics of Face Image capturing device o Specifications of Digital Face Image & Face Photograph Specifications intended only for human visual inspection and verification o Scene requirements of the face images, keeping in view a future possibility of computer based face recognition o Face Record Format for storing, archiving, and transmitting the information of face image within a CBEFF header data structure for the purpose of interoperability and usage in future for computer based face recognition.

2) Fingerprint Image and Minutiae Data Standard

Fingerprint is an important and unique biometric characteristic of an individual. There are many vendors selling finger print devices for acquisition of the data in different ways. Also various algorithms are available for fingerprint features extraction and matching.
It is necessary that these vendors follow fingerprint standards and best practices to ensure interoperability of devices and algorithms to avoid vendor lock-in, and also ensure long term storage of data with technology independence.

Usually, the fingerprint image data captured during enrolment is stored / transmitted for 1:1 (verification) and 1: N (identification) in an e-Governance application life cycle.

The matching of the fingerprints is done by extracting the minutiae of fingerprint data already stored in the enrolment stage, with the minutiae of data captured at the time of verification / identification. This process may even require transmission of fingerprint image data / minutiae data among various e-Governance applications by following the best practices.

Standard	Description
ISO/IEC 19794-4:2005(E)	This standard deals with usage of fingerprint image data and minutiae data for identification and verification of an individual. To ensure interoperability among vendors, it is required that these images be stored in a format compliant with the international standard ISO 19794-4, within the overall Common Biometric Exchange Formats Framework (CBEFF) as per ISO 19785-1. The Government of India would adopt ISO/IEC 19794-4:2005(E) as Fingerprint Image standard, and ISO 19794-2:2005(E) as Minutiae data format standard. The current version of Fingerprint image data standard has been tailored from the ISO 19794-4:2005(E) standard to meet specific needs of e-Governance applications in Indian context. It also includes best practices recommended for implementation of the specifications in different categories of e-Governance applications. This standard specifies fingerprint image specifications in different stages like acquisition for enrolment / verification / identification, storage and transmission. It also includes minutiae template specifications and best practices for implementation of the standard specifications in different categories of e-Governance applications based upon the volume of data, and verification/ accuracy requirements. The current version of the standard is applicable to all civilian e-governance applications as the present version does not include specifications for latent fingerprint data required by certain law enforcement applications.

3) Iris Image Data Standard

In the recent years, Iris recognition has emerged as an important and powerful Biometric characteristic. The Indian Government anticipates that, iris biometric would be deployed for identification and verification in e-Governance applications where identity management is a major issue.
In order to capture the Iris image, special devices are available in the market providing different formats for image acquisition and storage. Also many algorithms have been

developed by vendors to extract the features of iris images to decide on a match during verification / identification stage. To ensure interoperability among the e-Governance applications requiring iris recognition, it is necessary to standardize iris specifications including the storage and transmission formats.
Thus, to allow the application developer maximum flexibility in usage of algorithms and devices from different vendors and to address interoperability requirements, the iris image must be captured and stored as per standard specifications included in this document.
This Standard would be applicable to all e-Governance applications in India as per the Government's Policy on Open Standards.

There are two types of interchange formats to represent the Iris image data. The first is a rectilinear (rectangular or Cartesian) image storage format that specifies raw, uncompressed or compressed intensity values. The second format is based on polar image specification with specific pre processing and segmentation steps, producing a compact data structure containing only Iris information.

The Indian e-Governance applications will deal with Iris image data during multiple stages. Some of these stages are given below:

a. Image acquisition, its processing and its storage in the Enrolment stage
b. Image acquisition and storage for off line / on line verification of Iris image data in 1:1 matching stage
c. Image acquisition and storage for the purpose of identification in 1:N matching stage
d. Transmission of Iris image data to other e-Governance applications
e. Extraction of features of Iris images (enrolment or recognition stage), their storage, and matching (Not covered in the present version of the standard).

The interchange format type of the Iris images that is defined in this standard is for **rectilinear images only**.
If the image is collected by a camera that captures only one eye at a time and is stored using a rectilinear coordinate system no specific pre-processing is required. Cameras that capture images of botheyes simultaneously may use the following processing steps to calculate the rotation angle of the Iris images.

Standard	Description
ISO/IEC 19794-4:2005(E)	The Government of India would broadly adopt ISO 19794-6:2005(E) Iris Image Data Standard, by tailoring the standard specifications to meet specific needs of civilian e-Governance applications in Indian context and as per the GoI Policy on Open Standards. This Standard specifies Iris image data specifications, acquisition, storage and transmission formats. It also includes best practices for implementation of the Standard specifications in different categories of e-Governance applications, based on the volume of data and verification/ accuracy requirements. This version of the Standard does not include features extraction & matching specifications.

Reference Standards:

1. GoI Face Image data standard version 1.0 published in November, 2010
2. GoI Fingerprint Image data Standard version 1.0 published in November, 2010
3. GoI Iris Image Data Standard Version 0.4, document published in March, 2011

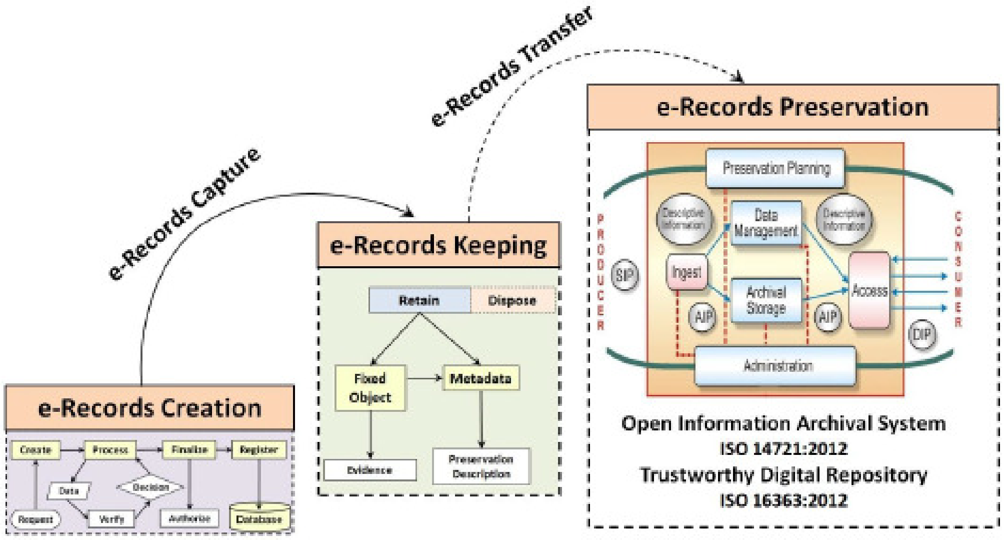
Annex-B (Digital Preservation Standards)

The **e-Governance Standard for Preservation Information Documentation (eGOV-PID) of Electronic Records (eGOV-PID)** provides a standardized metadata dictionary and schema for describing the "preservation metadata" of an electronic record. This standard proposes to capture most of the preservation information (metadata) automatically after the final e-record is created by the e-Government system. Such preservation information documentation is necessary only for those e-records that need to be retained for long durations (e.g. 10 years, 25 years, 50 years and beyond) and the e-records that need to be preserved permanently.

The implementation of this standard helps in producing the valid input i.e. Submission Information Package (SIP) for archival and preservation purpose as per the requirements specified in the ISO 14721 Open Archival Information Systems (OAIS) Reference Model.

The eGOV-PID allows to capture the preservation metadata in terms of cataloguing information, enclosure information, provenance information, fixity information, representation information, digital signature information and access rights information.

The core concepts of 'preservability' are based on the requirements specified in IT ACT, ISO/TR 15489-1 and 2 Information Documentation - Records Management and ISO 14721 Open Archival Information Systems (OAIS) Reference Model. It introduces 5 distinct steps of e-record management i.e. e-record creation, e-record capturing, e-record keeping, e-record transfer to designated trusted digital repository and e-record preservation which need to be adopted in all e-Governance projects.



Standard	Description
ISO 15836:2009	Information and documentation - The Dublin Core metadata elements
ISO/TR 15489-1 and 2	Information and Documentation - Records Management: 2001
ISO 14721:2012	Open Archival Information Systems (OAIS) Reference Model
ISO/DIS 16363: 2012	Audit & Certification of Trustworthy Digital Repositories
METS, Library of Congress, 2010	Metadata Encoding and Transmission Standard (METS) -
InterPARES 2	International Research on Permanent Authentic Records - A Framework of Principles for the Development of Policies, Strategies and Standards for the Long-term Preservation of Digital Records, 2008
ISO 19005-1:2005 Use of PDF 1.4 (PDF/A-1b) with Level B	Capture of e-records in PDF for Archival (PDFA) format - PDF/A-1a is based on the PDF Reference Version 1.4 from Adobe Systems Inc. (implemented in Adobe Acrobat 5 and latest versions) and is defined by ISO 19005-1:2005. Conformance is recommended for archival of reformatted digital documents due to following reasons: o PDF/A-1b preserves the visual appearance of the document o Digitized documents in image format can be composited as PDF/A-1b **PDF/A for e-governance applications** o Apache FOP 1.1 library can be used in the application logic for dynamically publishing the e-records in PDF/A format. **PDF/A for document creation** o Libre Office 4.0 supports the exporting of a document in PDF/A format. o MS Office 2007 onwards the support for “save as” PDF/A is available. o Adobe Acrobat Professional can be used for converting the PDF documents to PDF/A format.
ISO 19005-2:2011 Use of ISO 32000-1 (PDF/A-2)	Recommended for preservation of documents requiring the advanced features supported in it. PDF/A-2a is based on ISO 32000-1 – PDF 1.7 and is defined by ISO 19005-2:2011. Its features are as under: o Support for JPEG2000 image compression o Support for transparency effects and layers o Embedding of OpenType fonts o Provisions for digital signatures in accordance with the PDF Advanced Electronic Signatures – PAdES standard o Possibility to embed PDF/A files in PDF/A-2 for archiving of sets of documents as individual documents in a single file

	PDF/A-2 does not replace the PDF/A-1 standard but it co-exists alongside with an extended set of features. PDF/A-1a and PDF/A-1b compliance are minimum essential for e-government records as recommended in the IFEG technical standard of DeitY.
JPEG2000 (ISO/IEC 15444-1:2004) and PNG (ISO/IEC 15948:2004)	Image file formats - which support lossless compression are recommended as raster image file formats for e-governance applications as specified in Technical Standards for Interoperability Framework for e-Governance (IFEG) in India, published in 2012 by e-Gov Standards Division, DeitY.
ISO/IEC 27002: 2005	Code of practices for information security management for ensuring the security of the e-records archived on digital storage.

Annex-C (Localisation and Language Technology Standard)

1. Character Encoding Standard for Indian Languages

The lack of availability of information in the locally understandable language is the main reason for the slow progress in the Information and Communication Technology (ICT) sector. In today's age, access to ICT plays a major role in the overall development of a country, it has become a challenge to bridge the digital divide caused by the language barrier.

Standardisation is one of the baselines to be followed in localisation. Standardisation means to follow certain universally accepted standards, so that the developers from any part of the globe could interact through the application. Standardisation becomes applicable in almost everything specific to the language – for instance, a standard glossary of terms for translation, a standard keyboard layout for input system, a standard collation sequence order for sorting, a standard font etc.

Character Encoding standard for all constitutionally recognized Indian Languages should be such that it facilitates global data interchange.

ISCII is the National Standard and Unicode is the global character encoding standard.The average data packet size is less for representation of any Indian languages using ISCII. However, being limited code space, coexistence of multiple languages within the same code page is not possible in ISCII. The migration from ISCII to Unicode has become imperative due to the following reasons:

All major operating systems, browsers, editors, word processors and other applications & tools are supporting Unicode.

- It is possible to use Indian languages and scripts in the Unicode environment, which will resolve the compatibility issue.
- The documents created using Unicode may be searched very easily on the web.
- As Unicode is widely recognized all over the world and also supporting Indian languages, it will ease Localization applications including e-Governance application for all the constitutionally recognized Indian languages.
- Since Indian languages are also used in the other part of the world, it is possible to have Global data exchange.

Unicode shall be the storage-encoding standard for all constitutionally recognised Indian Languages including English and other global languages as follows:

Specification Area	Standard Name	Owner	Nature of the Standard	Nature of Recommend Actions
Character Encoding for Indian Languages	Unicode 5.1.0 and its future upgradation as reported by Unicode consortium from time to time.	Unicode Consortium, Inc.	Matured	Mandatory

Character: Character is the smallest component of any written language that has semantic value.

ISCII: Indian Script Code for Information Interchange (ISCII - IS 13194:1991) is the character-encoding standard approved by Bureau of Indian Standards (BIS). ISCII is an 8 bit-encoding scheme, catering to 128 code spaces for representation of Indian languages.
Nine Indian scripts are included in ASCII standard to represent 10 Indian languages i.e. Assamese, Bengali, Devnagari, Gujarati, Gurmukhi, Kannada, Malayalam, Oriya, Tamil and Telugu.

Unicode: Unicode is a 16-bit character-encoding standard. All the major written scripts of the world are included in the Unicode Standard. The first version of Unicode was published in year 1991.

Unicode vis-à-vis ISO10646
Unicode is a 16 bit Character Encoding standard. All the major written scripts are included in the Unicode Standard. Indian scripts are also included in the standard. There are 22 constitutionally recognised Indian Languages, written in 12 different scripts. ISO/IEC 10646 is the character-encoding scheme evolved by the International Organisation for Standardisation (ISO) in 1990.

In 1991, the ISO Working Group responsible for ISO/IEC 10646 (JTC 1/SC 2/WG 2) and the Unicode Consortium decided to create universal standard for coding multilingual text. Since then, the ISO 10646 Working Group (SC 2/WG 2) and the Unicode Consortium are working together closely to extend the standard and to keep their respective versions synchronised.

In addition to the code tables as per ISO/IEC 10646, the Unicode Standard also provides an extensive set of character specifications, character data, algorithms and substantial technical material, which is useful for developers and implementers.

2. Font Standard for Indian Languages

A single International Standard to comply with UNICODE data storage. This ensures data portability across various applications and platforms.

True Type Fonts (TTF) was used in various applications earlier by various vendors. TTF had no encoding standard due to which vendors and developers had their own encoding schemes, thereby jeopardizing data portability. ISO/IEC 14496-OFF (Open Font Format) on the other hand is based on a single International Standard and complies with UNICODE for data storage. This ensures data portability across various applications and platforms. Open type font is a smart font which has built- in script composition logic.
Most often it has been observed that the use of proprietary fonts of different standards in Government Offices, which are not compatible witheach other, is causing serious problems in information exchange amongst offices. By using Unicode compliant ISO/IEC 14496-OFF (Open Font Format) for font standard, the problem relating to the exchange of documents/files is completely solved.

Open standard under the International Organization for Standardization (ISO) within the MPEG group, which had previously adopted Open Type by reference, now adopted the new standard with appropriate language changes for ISO, and is called the "ISO/IEC 14496-OFF (Open Font Format)" for which formal approval reached in March 2007 as ISO Standard ISO/IEC 14496-OFF (Open Font Format) and it is a free, publicly available standard.

ISO/IEC 14496-OFF (Open Font Format) for font standard would be the standard for Indian Languages in e-Governance Applications. **ISO/IEC 14496-OFF (Open Font Format) for font standard is mandatory for all 22 constitutionally recognized languages.**

TTF (True Type Font)

A Font Format developed by Apple and licensed to True type, is the native Operating System Font Format for Windows and Mac operating systems.

ISO/IEC 14496-OFF (Open Font Format)

OFF fonts allow the handling of large glyph sets using Unicode encoding. Suchencoding allows broad international support for typographic glyph variants.

OFF fonts may contain digital signatures, whichenable operating systems and browsing applications to identify the source and integrity of font files, (including the embedded font files obtained in web documents), before using them. Also, font developers can encode embedding restrictions in OFF fonts which cannot be altered in a font signed by the developer.

Annex-D (Metadata and Data Standards)

Standardization of data elements is the prerequisite for systematic development of e-Governance applications.

Data Standards may be defined as the agreed upon terms for defining and sharing data. Data Standards promote the consistent recording of information and are fundamental to the efficient exchange of information. They provide the rules for structuring information, so that the data entered into a system can be reliably read, sorted, indexed, retrieved, communicated between systems, and shared. They help protect the long-term value of data.

Once the data standards are in place, there is a need to manage data, information, and knowledge. Metadata of standardized data elements can be used for this purpose.

Metadata is structured information that describes, explains, locates or otherwise makes it easier to retrieve, use or manage an information resource. Metadata is often called data about data or information about information. A metadata is a matter of context or perspective -what is metadata to one person or application can be data to another person or application.

In other words, Metadata facilitates the user by providing access to the raw data through which the user can have an understanding of the actual data. Hence, Metadata is an abstraction layer that masks the underlying technologies, making the data access friendlier to the user.

Data and Metadata Standards provide a way for information resources in electronic form to communicate their existence and their nature to other electronic applications (e.g. via HTML or XML) or search tools and to permit exchange of information between applications.

The present document “Data and Metadata Standards- Demographic” focuses on Person Identification and Land Region codifications. It includes the following:

a) **Mechanism for allocation of reference no**. to the identified Generic data elements, and their grouping.

b) **Generic data elements** specifications like:

- Generic data elements, common across all Domain applications
- Generic data elements for Person identification
- Generic data elements for Land Region Codification
- Data elements to describe Address of a Premises, where a Person resides

c) **Specifications of Code Directories like:**

- Ownership with rights to update
- Identification of attributes of the Code directories
- Standardization of values in the Code directories

d) Metadata of Generic Data Elements

- Identification of Metadata Qualifiers
- Metadata of the data elements

e) Illustration of data elements to describe:

- Person identification
- Address of a premises

This Standard would be applicable to all e-Governance applications in India as per the Government’s Policy on Open Standards (refer http://egovstandards.gov.in/policy/policy-onopen-standards-for-e-governance/)

Rerefrence Standards:

4. ISO Standard 1000:1992 for SI Units

5. MNIC Coding for Person Identification

6. ISO 693-3 for International language codes
7. RGI's coding schemes for Languages
8. Top level document provided by Working Group on Metadata and Data Standards
9. EGIF (e- Government Interoperability Framework) Standard of U.K.
10. uidai.gov.in/UID_PDF/Working_Papers/A_UID_Numbering_Scheme.pdf
11. http:// www.dolr.nic.in for conversion table of units as used by Department of Land Records
12. GoI Policy on open standards version 1.0 released in November, 2010
13. UID DDSVP Committee report, Version 1.0, Dec 09, 2009
14. ANSI92 Standard

Annex-E (Mobile Governance)

Framework for Mobile Governance (m-Governance)

Mobile Governance (m-Governance) is a strategy and its implementation to leverage available wireless and new media technology platforms, mobile phone devices and applications for delivery of public information and services to citizens and businesses.

The m-Governance framework of Government of India aims to utilize the massive reach of mobile phones and harness the potential of mobile applications to enable easy and round the-clock access to public services, especially in the rural areas**.** The framework aims to create unique infrastructure as well as application development ecosystem for m-Governance in the country.

In cognizance of the vast **mobile phone subscriber base, peaked to more than 1 billion users in the country**, the Government has decided to also provision for access of public services through mobile devices, thereby establishing mobile Governance (m-Governance) as a compelling new paradigm.

Government of India will progressively adopt and deploy m-Governance in a time-bound manner to ensure inclusive delivery of public services to both the urban and rural populace in the country in accordance with this framework.

The following are the main measures laid down:

i. Web sites of all Government Departments and Agencies shall be made mobile compliant, using the “**One Web**” approach.

ii. **Open standards** shall be adopted for mobile applications for ensuring the interoperability of applications across various operating systems and devices as per the Government Policy on Open Standards for e-Governance.

iii. **Uniform/ single pre-designated numbers** (long and short codes) shall be used for mobile-based services to ensure convenience.

iv. All Government Departments and Agencies shall develop and deploy mobile applications for providing all their public services through mobile devices to extent feasible on the mobile platform. They shall also specify the service levels for such services.

The success of the proposed initiative on m-Governance will greatly depend upon the ability of the Government Departments and Agencies to provide frequently needed public services to the citizens, create infrastructure for anytime anywhere mobile-based services, adopt appropriate open standards, develop suitable technology platforms, make the cost of services affordable, and create awareness, especially for people in underserved areas.

To ensure the adoption and implementation of the framework in a time-bound manner, following actions will be taken:

1. Creation of Mobile Services Delivery Gateway (MSDG)

MSDG is the core infrastructure for enabling the availability of public services through mobile devices. This will be developed and maintained by an appropriate agency within DIT. MSDG is proposed to be used as a shared infrastructure by the Central and State Government Departments and Agencies at nominal costs for delivering public services through mobile devices.

Various channels, such as voice, text (e-mail and SMS), GPRS, USSD, SIM Toolkit (STK), Cell Broadcast (CBC), and multimedia (MMS) will be incorporated to ensure that all users are able to access and use the mobile based services. The various delivery channels are expected to entail innovative ways of providing existing services as well as development of new services.

To ensure successful implementation of the platform with requisite levels of security and redundancy, following actions will be taken:

a) **End User Interface:** End-user devices include landline phones, mobile phones, smart phones, personal digital assistants (PDAs), tablets, and laptops with wireless infrastructure. Mobile applications developed shall take into consideration appropriately the wireless-device interface issues, such as bandwidth limitations, micro-browser and micro-screen restrictions, memory and storage capacities, usability, etc.

b) **Content for Mobile Services:** Due to lower-bandwidth and smaller-screen characteristics of mobile devices, successful development and deployment of m-Governance will require development of separate mobile-ready content. Similarly, to meet the needs of all the potential users, the applications will need to be developed in the relevant local languages for the various channels of delivery. Open standards and open source software, to the extent possible, will be used to ensure interoperability and affordability of the content and applications developed.

c) Mobile Applications (Apps) Store: A mobile applications (m-apps) store will be created to facilitate the process of development and deployment of suitable applications for delivery of public services through mobile devices. The m-apps store shall be integrated with the MSDG and it shall use the MSDG infrastructure for deployment of such applications. It is proposed that the store will be based upon service oriented architecture and cloud based technologies using open standards as far as practicable. The open platform will be developed and deployed in conjunction with the MSDG for making the additional value added services available to the users irrespective of the device or network operator used by them

d) Application Programming Interfaces (APIs) for Value-Added Services (VAS) providers: MSDG shall offer suitable APIs to VAS providers with appropriate terms and conditions to ensure interoperability and compliance with standards for development of applications for delivery of public services.

e) **Mobile-Based Electronic Authentication of Users**: For electronic authentication of users for mobile-based public services, MSDG shall incorporate suitable mechanisms including Aadhaar-based authentication. This will also help in ensuring appropriate privacy and confidentiality of data and transactions.

f) **Payment Gateway**: MSDG shall also incorporate an integrated mobile payment gateway to enable users to pay for the public services electronically.

g) **Participation of Departments**: The Government Departments and Agencies both at the Central and State levels will be encouraged to offer their mobile-based public services through the MSDG to avoid duplication of infrastructure.

2. Creation of Mobile Governance Innovation Fund

Department of Information Technology (DIT) shall create a Mobile Governance Innovation Fund to support the development of suitable applications by Government Departments and Agencies and also by third-party developers including start-ups. The fund shall be created and managed by DIT for a minimum period of 3 years. The objective of this fund will be to accelerate the development and deployment of the mobile applications across the entire spectrum of public services.

3. Creation of Knowledge Portal and Knowledge Management Framework on Mobile Governance

DIT shall develop and deploy a state-of-the-art knowledge portal and knowledge management framework that acts as a platform for awareness generation and dissemination for various Central Government Ministries and the State Governments. This will enhance the absorptive as well as the service provision capabilities of various stakeholders in m-Governance. Since m-Governance is in its nascent stage both in India and globally, the knowledge portal will act as a reference and guide for Government Departments and Agencies in India.

4. Creation of Facilitating Mechanism

An appropriate facilitating mechanism will be created to ensure compliance with the standards for mobile applications and ensure seamless interoperability of services and implementation of short and long codes for public services across multiple service providers. The proposed mechanism shall be established and managed by the Department of Information Technology, Government of India.

Guidelines for Delivery Channels for Provision of Public Services through Mobile Devices

The Objective is to provide:

a. **Guidelines to deliver public services round-the-clock to the users using m-Governance**

b. **Guidelines to develop standard based mobile solutions**

c. **Guidelines to integrate the mobile applications with the common e-Governance infrastructure**

As part of the initiative a shared technical infrastructure **Mobile Services Delivery Gateway (MOBILE SEVA)** has been created to enable integration of mobile applications with the common e-Governance infrastructure and delivery of public services to the users.

The objective of creating the MOBILE SEVA is to put in place government-wide shared infrastructure and services to enable rapid development, mainstreaming and deployment of m-Governance services. It will enhance interoperability across various public services as well as reduce the total cost of operation of m-Governance services by providing a common pool of resources aggregating the demand for communication and e-Governance services, and act as a platform for various Government Departments and Agencies to test, rapidly deploy, and easily maintain m-Governance services across the country.

MSDP (Mobile e-governance Services Delivery Platform) provides an integrated platform for delivery of government services to citizen over mobile devices using Mobile Service Delivery Gateway (MSDG), SMS Gateway, m-App Store, m-Payment Services, Location Based Services (LBS), Unstructured Supplementary Services Data (USSD), Unstructured Supplementary Service Notify (USSN), Unstructured Supplementary Service Request (USSR), MMS, Cell Broadcasting Service (CBS), SIM Toolkit (STK), IVRS etc.

MSDG is a messaging middleware to facilitate e-Governance services delivery based on e-Governance Standard protocols which are IIP (Interoperability Interface Protocol), IIS (Interoperability Interface Specifications), IGIS (Inter-Gateway Interconnect Specifications) and Gateway Common Services Specifications (GCSS).

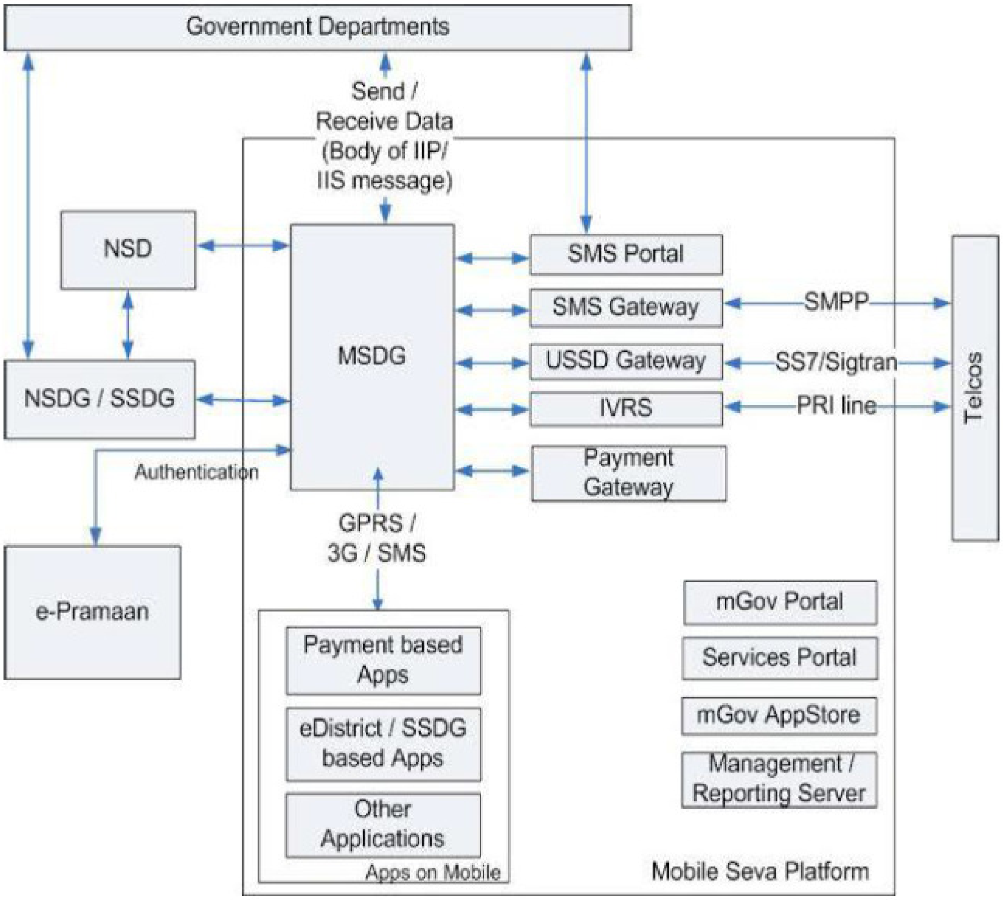


Figure 1: Mobile e-governance Services Delivery Platform (MSDP)

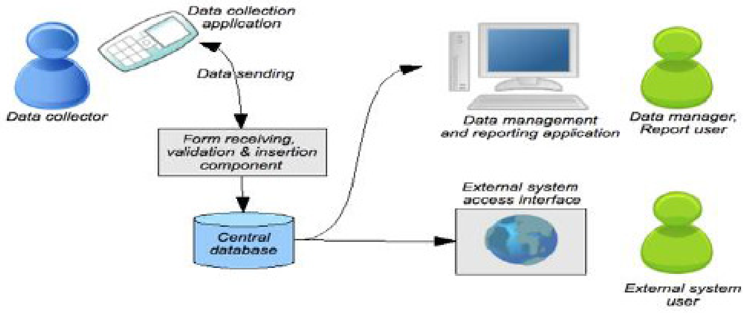
Mobile Application (m-Apps)

Mobile application software is applications software developed for handheld devices, such as mobile

phones, tablets etc. These applications can be pre-installed on phones during manufacture or downloaded by users from various mobile software distribution platforms, or delivered as web applications using server-side or client-side processing (e.g. JavaScript) to provide an application like experience within a Web browser.

1. **Mobile Application Dependency on Handset and O/S**
   Mobile Application software developers also have to consider a lengthy array of screen sizes, hardware specifications and configurations because of intense competition in mobile software and changes within each of the platforms.

2. **Data Collection: m-forms**
   Mobile Application can also make use of the various forms for data collection. Many data collection systems are built from existing commercial or open source components, or even come packaged as an end-to-end solution. The components of data collection relate to each other as shown below:


Data collection application
Data sending
Data collector
Form receiving, validation & insertion component
Central database
Data management and reporting application
Data manager, Report user
External system access interface
External system user

The data collection may be done by various methods. Following are the most common types of data collection client applications which may be used:

1. **Fixed format SMS based Forms:** The 'client application' in this case is the phone's built-in SMS functionality. The user writes and sends SMS in a predefined format, representing answers to successive questions.

2. **Java Micro Edition Platform (J2ME) Application based Forms:** A J2ME application is written in the Java programming language, and loaded onto the phone over Bluetooth or by downloading the application from the Internet. To use the client application, the data collector navigates through questions in an application on the phone, which collects the answers and submits the completed form to a server.

3. **Mobile Operating System based Forms:** Mobile Operating Systems such as Android, Windows Mobile can also be used for developing native platform-dependent applications which can have various forms for data collection.

4. **Web-based Forms:** The 'client application' for web-based forms is the phone's web browser. The user browses to a website, where the form is published in an optimized format for mobile browsers.

5. **Voice-based based Forms:** The user dials a number and then chooses from options on a menu, useful when there are low levels of literacy among data collectors, or when a system is needed that caters for both landline and mobile phones.

6. **Wireless Internet Gateway (WIG) based Forms:** WIG uses a programming language (Wireless Markup Language, or WML) that is internal to almost all SIM cards. The menu definition is easy to write, but the size limit is 1MB, making it difficult to support long menus or multiple languages.

7. **Unstructured Supplementary Service Data (USSD) based Forms:** This is a real-time question-response service, where the user initiates a session and is then able to interact with the remote server by selecting numeric menu options. The phone needs to be continuously connected during the session, which needs a good, consistent signal.

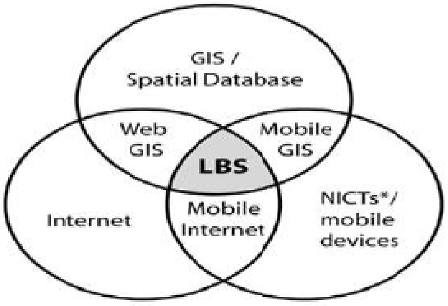
Once data has been captured on the phone, the completed form generally needs to be submitted to a central back-end server.

Other Mobile Technologies

1. Location Based Services (LBS)

Location-based services (LBS) denote services offered to mobile users according to their geographic location. LBS give the possibility of a two way communication and interaction. Therefore the user tells the service provider his actual context like the kind of information he needs, his preferences and his position. This helps the provider of such location services to deliver information tailored to the user needs. LBS enable to retrieve and share information related to their current position. For e.g. Google Latitude.

It works as an intersection of the following features in a system:



***NICT – New Information and Telecommunication technologies**

Geographical Information System (GIS) is a hardware, software and procedures designed to support the capture, management, manipulation, analysis, modelling and display of spatially referenced data for solving complex planning and management problems.

Internet is used to utilize the database dynamically so as to provide the appropriate service.
Mobile Devices as an end- device to execute the service.

2. Cell Broadcast Centre

Cell Broadcast is a mobile technology which allows text messages to be broadcasted to all mobile handsets and similar devices within a designated geographical area.
It is a one-to-many geographically focused service, in contrast to SMS which is a one-to-one or one-to-few service. It is usually used for providing location-based services, especially emergency services, as it utilizes minimum network resources for message broadcast and provides instantaneous delivery to all subscribers in a geographic area.
A Cell Broadcast message is an unconfirmed push service, meaning that the originator of the message does not know who has received the message, allowing for services based on anonymity. Mobile telephone user manuals describe how the user can switch the receiving of Cell Broadcast messages on or off.

Also known as Short message service-Cell Broadcast (SMS-CB), CB messaging is a mobile technology feature defined by the ETSI's GSM committee and is part of the GSM standard. It is also supported by UMTS, as defined by 3GPP.

a) Localization

Given that only a miniscule segment population in India can read and write English, it is important to deploy local/ regional languages to ensure all-round success of m-Governance initiatives. For detailed guidelines please refer to the Mobile Localization Guidelines.

b) Indian Language SMS

Currently, Indian language SMS services are offered by some operators but unlike the English SMS service, the language service is not necessarily interoperable across networks and cannot be availed on all types of handsets. The lack of a standard for Indian SMS comes in the way of providing scalable, interoperable and affordable SMS services in Indian languages. **To realise the goal of interoperable and affordable Indian language SMS, the following are the priority areas:**

i. **Text entry standards (i.e. keypad)**
ii. **Encoding standards to support all the major Indian languages**
iii. **Font support standardization for handsets to send and receive Indian language SMS**

i. Text entry methods

The two methods in vogue are:

a. **Mapping the Indian language characters on the handset keypad**
b. **Screen-assisted text inputting mechanisms available from a few OEMs and vendors**

The keypad for the English language has been standardized by ITU. Althoughefforts on supporting the Indian languages on handheld devices are on, acceptable standards are yet to be evolved. In the absence of any national standards specifying mapping of the Hindi (and other Indian Languages) alphabets to the 12-key mobile devices, the handset vendors keen on penetrating the large Indian market are using their own mappings (which can differ across vendors).

ii. Encoding standard

The Unicode standard supports the 22 major Indian languages but uses more bandwidth (2 octets for each character) and hence the maximum size of SMS that can be sent using Unicode (70 characters) would be less than half of that of an English language SMS (170 characters).

iii. Font Support

Solutions for aesthetic display of Indian language scripts on small handset screens are being worked out. Similarly, solutions are tried out for handsets already in use so that they can receive and display messages in Indian languages, even if they cannot be used to send such messages.

3. Mobile Payment (M-Payment)

Mobile payment is an alternative payment method. Instead of paying with cash, check, or credit cards, a consumer can use a mobile phone to pay for a wide range of services; after having authenticated the user using AADHAR or any other means. The basic aim of mobile payments is to enable micropayments on low-end mobile devices which support only voice and text, in addition to higher end phones which could support web-browsing or Java application capabilities.

a. Mobile banking (M-Banking or mBanking)

M-Banking is a term used for performing balance checks, account transactions, payments, credit applications and other banking transactions through a mobile device. The earlier mobile banking services were offered over SMS, a service known as SMS banking. With the introduction of smart phones with WAP support the mobile web is also being used for M-Banking. Latter with the advancements of web technologies such as HTML5, CSS3 and JavaScript it became feasible to launch mobile web based services to compliment native applications.

b. Immediate Mobile Payment Services (IMPS)

The Immediate Mobile Payment System (IMPS) has been developed by the National Payments Corporation of India (NPCI) to expand the scope of mobile payments to all sectors of the population. IMPS offer an instant, 24X7, interbank electronic fund transfer service through mobile phones.

An IMP provides an inter-operable infrastructure to the banks for enabling interbank real time funds transfer transactions. IMPS rides on the existing NFS Interbank ATM transaction switch infrastructure and message format making it easy for banks to adopt.

To enable the transfer of money, both the sender and the receiver of payment have to link their bank accounts with their phone numbers through their respective banks. The sender has to register for mobile banking service with her/his bank. Upon registration, the bank will provide a link to the Mobile banking software which needs to be installed in the mobile phone to enable payments.

Both the sender and the receiver will receive a Mobile Money Identifier (MMID) while the sender will also receive a Mobile PIN (MPIN) for authentication of transactions. While transacting, the sender has to input the MPIN, receiver’s mobile number and MMID, and the amount of funds to transfer.

IMPS will authenticate the sender, check the receiver’s mobile number and MMID, and transfer the funds to the receiver’s account in real-time. Both the sender and the receiver receive messages notifying them about the success or failure of the transaction.

c. Contactless cards and Mobile Phones

These cards are based upon a technology known as NFC (Near Field Communication) that allows NFC enabled cards to be ready by taping them on or by passing them by, a card reader than swiping them through or inserting into, the POS terminal. They are now being integrated into mobile phone handset for m-Payments.

NFC enabled phones are expected to become more widely available. The NFC chip inside the phone will be connected to the secure element within the SIM card, allowing information stored in an m-wallet to be accessed by the NFC card reader. Authorization for payments involves entering a PIN.

d. Airtime balance for payment

Airtime as balance for payment was realized because of the need for the unbanked majority to easily and cheaply transfer funds around the country. The facility required is the most basic of mobile phones, an account, which can be opened at any one of vendors to start transferring and receiving money.

Since the system uses either SIM toolkit or USSD technology depending on the country, the network charges are minimal to nonexistent. It has lowest entry barriers, since it works on more than 95 percent of handsets and has low transaction costs and no bank account or credit card required.

e. Mobile Wallet

A Mobile Wallet is functionality on a mobile device that can securely interact with digitized valuables thereby making payments using the mobile phone. Mobile wallet may reside on a phone or on a remote network / secure servers. It is controlled by the user of the wallet. Using a mobile wallet to make a payment is incredibly simple. When it is time to pay, the user turns on his or her phone's screen (if the screen is off, when the phone is dormant for instance, the NFC chip will not work), opens the wallet application, enters their pin number, and passes the phone within a few inches of the contactless payment symbol. The payment transaction is then processed just like a conventional card transaction. In addition, relevant offers, discounts, and coupons can be passed from the wallet along with the payment in that same tap of the phone.

4. SIM Application Toolkit

The SIM Application Toolkit is a standard set of commands, under GSM, which defines how the card should interact with the outside world and extends the communication protocol between the card and the handset. It is designed as a client server application.

With SIM Application Toolkit, the card has a proactive role in the handset, i.e., the SIM initiates commands independently of the handset and the network. This enables the SIM to build up an interactive exchange between a network application and the end user and access, or control access to, the network. The SIM also gives commands to the handset such as displaying menus and/or asking for user input.

Annexure-F (GIGW)

Guidelines for Indian Government Websites

India, the largest democracy in the world, is set to emerge as an ICT Superpower in this millennium. Realising the recognition of 'electronic governance' as an important goal by Governments world over, Indian Government has also laid a lot of emphasis on anytime, anywhere delivery of Government services. As of today, there are over five thousand Government websites in India.

Awareness about the fast changing ICT world and keenness to keep pace with the latest has ensured that almost all the State Governments in India already have their websites up and running. In fact each state has multiple websites belonging to different Departments.

However, these websites follow different Technology Standards, Design Layouts, Navigation Architecture, or, in simple terms, different look and feel as well as functionality.

The need for standardisation and uniformity in websites belonging to the Government cannot be stressed enough, in today's scenario.

As a first step, it is suggested that the Indian Government websites adhere to certain common minimum standards which have been derived, in the form of guidelines discussed in this document, as prerequisites for a Government website to fulfil its primary objective of being a citizen centric source of information & service delivery. These guidelines could eventually form the basis for establishment of the desired standards.

Compliance to these guidelines will ensure a high degree of consistency and uniformity in the content coverage and presentation and further promote excellence in Indian Government Web space.

These Guidelines have been framed with an objective to make the Indian Government Websites conform to the essential pre-requisites of UUU trilogy i.e. Usable, User-Centric and Universally Accessible. They also form the basis for obtaining Website Quality Certification from STQC (Standardisation Testing Quality Certification) an organisation of Department of Information Technology, Government of India.

These Guidelines are based on International Standards including ISO 23026, W3C's Web Content Accessibility Guidelines, Disability Act of India as well as Information Technology Act of India.

A. Indian Government Entity

All websites and Portals belonging to the Indian Government Domain at any hierarchical level (Apex Offices, Constitutional Bodies, Ministries, Departments, Organisations, States/UTs, District Administrations, and Village Panchayats et al) must prominently display a strong Indian Identity and ownership of Indian Government.

The above objective can be achieved through the following:

1. The National Emblem of India MUST be displayed on the Homepage of the websites of Central Government Ministries/Departments. The usage of National Emblem on an Indian Government website must comply with the directives as per the 'State Emblem of India (Prohibition of improper use) Act, 2005'.

   Further, the State Governments should also display the State Emblem (or the National Emblem in case the State has adopted the National Emblem as its official State Emblem) as per the Code provided in the above Act. The Public Sector organisations and autonomous bodies should display their official logo on the Homepage of the website to re-enforce their identity.

2. The Homepage and all important entry pages of the website MUST display the ownership information, either in the header or footer.

3. The lineage of the Department should also be indicated at the bottom of the Homepage and all important entry pages of the website. For instance, at the bottom of the Homepage, the footer may state the lineage information, in the following manner:

   i. This Website belongs to Department of Heavy Industries, Ministry of Heavy Industries and Public Enterprises, Government of India' (for a Central Government Department).

   ii. This Website belongs to Department of Industries, State Government of Himachal Pradesh, India' (for a State Government Department).

   iii. This is the official Website of Gas Authority of India Limited (GAIL), a Public Sector Undertaking of the Government of India under the Ministry of Petroleum and Natural Gas (for a Public Sector Undertaking).

   iv. This is the official Website of the District Administration of Thanjavur, State Government of Tamil Nadu (India)' (for a District of India).

4. All subsequent pages of the website should also display the ownership information in a summarised form. Further, the searchengines often index individual pages of a website and therefore, it is important that each webpage belonging to a site displays the relevant ownership information.

5. In case of those websites which belong to Inter-Departmental initiatives involving multiple Government Departments which are difficult to list on the Homepage, the Government ownership should still be reflected clearly at the bottom of the page with detailed information provided in the 'About the Portal/Website' section.

6. The page title of the Homepage (the title which appears on the top bar of the browser) MUST be complete with the name of the country included, for instance, instead of the title being just Ministry of Health and Family Welfare, it should state, Government of India, Ministry of Health & Family Welfare.

   Alternatively, in case of a State Government Department, it should state 'Department of Health, Government of Karnataka, India '. This will not only facilitate an easy and unambiguous identification of the website but would also help in a more relevant and visible presence in the searchengine results. Further, it is important since the screen readers used by the visually impaired users first read the title of the page and in case the title is not explanatory enough, it may confuse or mislead them.

B. Government Domains

The URL or the Web Address of any Government website is also a strong indicator of its authenticity and status as being official. In today's era with a large proliferation of websites, which resemble Government websites and fraudulently claim to provide reliable Government information and services, the role of a designated Government domain name assumes a lot of significance.

Hence, in compliance to the Government's Domain Name Policy, all Government websites MUST use 'gov.in' or 'nic.in' domain exclusively allotted and restricted to Government websites. The military institutions and organisations in India may also use 'mil.in' domain in place of or in addition to the gov.in /.nic.in domain. The above naming policy applies to all Government websites irrespective of where they are hosted.

Those Departments and Government entities that are using and have been publicising a domain name other than the above should take appropriate early action to register official government domain names and use the existing ones as 'alias' for a period of six months. An intermediary page with a clear message notifying the visitors about the change in the URL and then auto redirecting them to the new URL after a time gap of 10 seconds should be used.

The Domain Name Conventions, as specified in the '.IN Registration' policy should be followed while registering a 'gov.in' Domain Name.

National Informatics Centre (NIC) is the exclusive Registrar for GOV.IN domain names. The use of GOV.IN Domain is restricted to the constituents of Indian Government at various levels right from Central, State/UT, District & Sub-District, block, village etc.

For detailed information and step-by-step procedure on how to register a .GOV IN Domain, one may visit http://registry.gov.in **.**

C. Link with National Portal

1) **india.gov.in:** The National Portal of India is a single window source for access to all information and services being provided by the various constituents of the Indian Government to its citizens and other stakeholders.

There are exclusive sections on Citizens, Business, Overseas, Government, Know India, Sectors etc. catering to the information needs. Sections targeting special interest groups such as Government Employees, Students, Senior Citizens, Kids etc. are also present.

a) **Since the National Portal is the official single entry Portal of the Indian Government, all Indian Government websites MUST provide a prominent link to the National Portal from the Homepage and other important pages of citizens' interest**.

b) **The pages belonging to the National Portal MUST load into a newly opened browser window of the user.** This will also help visitors find information or service they could not get on that particular website. It is quite common that citizens are not aware which information or service is provided by which Department.

As per linking Policy of the National Portal, no prior permission is required to link 'india.gov.in' from any Indian Government website. However, the Department providing a link to the National Portal is required to inform the National Portal Secretariat about the various sections of the National Portal that they have linked to, so that they can be informed of any changes, updations / additions therein. Also, it is not permitted that the National Portal Pages be loaded into frames on any site. These must be loaded into a new browser window.

Special Banners in different sizes and colour schemes for providing a link to the National Portal have been given at http://india.gov.in/linktous.php

Instructions on how to provide a link have also been given. The Government websites / portals may choose any banner from the ones provided, depending upon their site design and place the same on their Homepage.

D. Content Copyright

Copyright is a form of protection provided under law to the owners of "original works of authorship" in any form or media. It is implied that the original information put up on the website by a Government Department is by default a copyright of the owner Department and may be copied, reproduced, republished, uploaded, posted, transmitted, or distributed only if the copyright policy of the concerned Department allows so.

Hence, the information, material and documents made available on an Indian Government website MUST be backed up with proper copyright policy explaining the terms and conditions of their usage and reference by others. The copyright policy of a Department could be liberal, moderate or conservative depending upon their preferences based on the kind of information available on their website. However, since it is a duty of a Government Department to provide all the information in the public domain freely to the citizens, the Departments should aim to have a liberal copyright policy.

The Departments should also be sensitive towards publishing any information having a third party copyright. The Government Departments MUST follow proper procedures to obtain the permission, prior to publishing such information on their websites.

If any published Government Document/Report is being reproduced on any website, whether as excerpts or in full, the source of the same i.e. Full Title of the Report/Document along with the name of the concerned Department and year of publication MUST be provided.

E. Content Hyper linking

Since Government websites often receive queries and requests from owners of other websites who might want to provide a hyper link to their web pages, every Indian Government website MUST have a comprehensive and clear-cut hyper linking policy defined and spelt out for those who wish to hyper link content from any of its sections. The basic hyper linking practices and rules should ideally be common across the websites of a State/Ministry.

The hyperlinking policy enumerating the detailed criteria and guidelines with respect to hyperlinks with other sites may be made available under the common heading of **'Hyperlinking Policy'** and displayed at a common point on the Homepage of all sites under the ownership a State/Ministry.

a) To create a visual distinction for links that lead off site, Cascading Style Sheets (CSS) controls or XSL or some such similar mechanism should be used. In case the link takes the user to another website of the same Department/Ministry/ State, a seamless transition should be used through appropriate CSS controls.

b) Third party content should only be linked when consideration about the copyright, terms of use, permissions, content authenticity and other legal and ethical aspects of the concerned content have been taken into account.

c) The overall quality of a website's content is also dependent, among other things on the authenticity and relevance of the 'linked' information it provides.

d) Further, it MUST be ensured that 'broken links' or those leading to 'Page Not Found' errors are checked on a regular basis and are rectified or removed from the site immediately upon discovery.

F. Privacy Policy

Government websites should follow an extremely cautious approach when it comes to collecting personal details/information about the visitors to the sites. It should be an endeavour to solicit only that information which is absolutely necessary.

In case a Department solicits or collects personal information from visitors through their websites, it MUST incorporate a prominently displayed Privacy Statement clearly stating the purpose for which information is being collected, whether the information shall be disclosed to anyone for any purpose and to whom.

Further, the privacy statement should also clarify whether any cookies shall be transferred onto the visitor's system during the process and what shall be the purpose of the same.

Whenever a Department's website allows e-commerce and collects high risk personal information from its visitors such as credit card or bank details, it MUST be done through sufficiently secure means to avoid any inconvenience. SSL (Secure Socket Layer), Digital Certificates are some of the instruments, which could be used to achieve this.

Annex-G (Open APIs)

Policy on Open Application Programming Interfaces (APIs)

Under the overarching vision of Digital India, Government of India (GoI) aims to make all Government services digitally accessible to citizens through multiple channels, such as web, mobile and common service delivery outlets.

To meet this objective, there is a need for an interoperable ecosystem of data, applications and processes which will make the right information available to the right user at the right time.

Interoperability among various e-Governance systems is an important prerequisite for upgrading the quality and effectiveness of service delivery. For promoting Open Standards for software interoperability across various Government departments and agencies, GoI has already notified the “Policy on Open Standards for e-Governance” and “Technical Standards on Interoperability Framework for e-Governance”.

Open API is the API that has been exposed to enable other systems to interact with that system. Open API may be either integrated with the host application or may be an additional piece of software that exposes any proprietary API with an Open API equivalent. The Open API, whenever possible, may be free of charge and without restrictions for reuse & modifications.

Policy on Open APIs for Government of India” (hereinafter referred to as the “Policy”) will encourage the formal use of Open APIs in Government organizations. This policy sets out the Government’s approach on the use of “Open APIs” to promote software interoperability for all e-Governance applications & systems and provide access to data & services for promoting participation of all stakeholders including citizens.

The objectives of this policy are to:

i. Ensure that APIs are published by all Government organisations for all e-Governance applications and systems.

ii. Enable quick and transparent integration with other e-Governance applications and systems.

iii. Enable safe and reliable sharing of information and data across various e-Governance applications and systems.

iv. Promote and expedite innovation through the availability of data from e-Governance applications and systems to the public.

v. Provide guidance to Government organizations in developing, publishing and implementation using these Open APIs.

Government of India shall adopt Open APIs to enable quick and transparent integration with other e-Governance applications and systems implemented by various Government organizations, thereby providing access to data & services and promoting citizen participation for the benefit of the community.

The Open APIs shall have the following characteristics for publishing and consumption:

i. The relevant information being provided by all Government organisations through their respective e-Governance applications shall be open and machine readable.

ii. All the relevant information and data of a Government organisation shall be made available by Open APIs, as per the classification given in the National Data Sharing and Accessibility Policy (NDSAP-2012), so that the public can access information and data.

iii. All Open APIs built and data provided, shall adhere to National Cyber Security Policy.

iv. The Government organizations shall make sure that the Open APIs are stable and scalable.

v. All the relevant information, data and functionalities within an e-Governance application or system of a Government organisation shall be made available to other e-Governance applications and systems through Open APIs which should be platform and language independent.

vi. A Government organisation consuming the data and information from other e-Governance applications and systems using Open APIs shall undertake information handling, authentication and authorisation through a process as defined by the API publishing Organisation.

vii. Each published API of a Government organization shall be provided free of charge whenever possible to other Government organizations and public.

viii. Each published API shall be properly documented with sample code and sufficient information for developers to make use of the API.

ix. The life-cycle of the Open API shall be made available by the API publishing Government organisation. The API shall be backward compatible with at least two earlier versions.

x. All Open API systems built and data provided shall adhere to GoI security policies and guidelines.

xi. Government organizations may use an authentication mechanism to enable service interoperability and single sign-on.

The policy shall be applicable to all Government organisations under the Central Government and those State Governments that choose to adopt this policy for the following categories of e-Governance systems:

- All new e-Governance applications and systems being considered for implementation.
- New versions of the legacy and existing systems.

Annex-H (Internet of Things)

1. Sensor & Actuators

a. IEEE 1451

IEEE 1451 is a set of smart transducer interface standards developed by the Institute of Electrical and Electronics Engineers (IEEE) Instrumentation and Measurement Society's Sensor Technology Technical Committee describing a set of open, common, network-independent communication interfaces for connecting transducers (sensors or actuators) to microprocessors, instrumentation systems, and control/field networks.

b. Identification Technology

ISO/IEC JTC 1/SC31 Automatic identification and data capture techniques

It develops and facilitates standards within the field of automatic identification technologies. These technologies include 1D and 2D barcodes, active and passive RFID for item identification and OCR.

c. Domain Specific Compliance:

Sensors/IoT Devices/Actuators should follow the compliance to respective domain specific standards, like healthcare devices HL7, automobile/bus UBS-II (ITS sensor parameter & standards), OBD-II, Electric Vehicle Charging etc.

2. Communication Technology

a. Thread:

Networking protocol called Thread that aims to create a standard for communication between connected household devices.

b. AllJoyn:

Open source AllJoyn protocol was initially developed by Qualcomm provides tools for the entire process of connecting and maintaining devices on a Wi-Fi network.

c. IEEE 802.15.4:

It offers physical and media access control layers for low-cost, low-speed, low-power Wireless Personal Area Networks (WPANs).

IEEE 802.15.4e-2012, IEEE 802.15.4-2011, IEEE 802.15.4-2003, IEEE 802.15.4-2006

d. IETF IPv6 over Low power WPAN (6LoWPAN):

It defines encapsulation and header compression mechanisms that allow IPv6 packets to be sent to and received over IEEE 802.15.4 based networks.
6LoWPAN Frame Format
Fragmentation and Reassembly
Header Compression
Support for security mechanisms

e. IETF "Routing Over Low power and Lossy (ROLL):

IPv6 Routing Protocol for Low power and Lossy Networks (LLNs) (RPL)

RPL Topology Formation (Destination Oriented Directed Acyclic Graphs - DODAGs)
RPL Control Messages

f. **IETF Constrained Application Protocol (CoAP):**
It offers simplicity and low overhead to enable the interaction and management of embedded devices.

3. **Use Case/ Application Specific:**

i. **Industrial IoT (IIoT):** Object Modeling Group (OMG) has been active in IIoT standardization efforts. OMG IIoT standards and activities include (but are not limited to):

- Data Distribution Service (DDS)
- Dependability Assurance Framework For Safety-Sensitive Consumer Devices
- Threat Modeling
- Structured Assurance Case Metamodel
- Unified Component Model for Distributed, Real-Time and Embedded Systems
- Automated Quality Characteristic Measures
- Interaction Flow Modeling Language™ (IFML™)

(Source: http://www.omg.org/hot-topics/iot-standards.htm)

ii. **eHealth:** IEEE has many standards in the eHealth technology area, from body area networks to 3D modeling of medical data and personal health device communications. IEEE 11073 standards are designed to help healthcare product vendors and integrators create devices and systems for disease management.

iii. **eLearning:** The IEEE Learning Technology Standards Committee (LTSC) is chartered by the IEEE Computer Society Standards Activity Board to develop globally recognized technical standards, recommended practices, and guides for learning technology.

iv. **Intelligent Transportation Systems (ITS):** IEEE has standards activities on many aspects of ITS, such as vehicle communications and networking (IEEE 802 series), vehicle to grid interconnectivity (IEEE P2030.1), addressing applications for electric sourced vehicles and related support infrastructure, and communication for charging (IEEE 1901).

4. **Consortia**

a. **Open Interconnect Consortium:**
OIC (Atmel, Dell, Broadcom, Samsung, and Wind River as members) is an open environment to support the billions of connected devices coming online.

b. **Industrial Internet Consortium:**

It was founded by Intel, Cisco, AT&T, GE & IBM with the goal of developing standards specifically for industrial use of the Internet of Things.

5. Architecture Technology

a. IEEE P2413: Standard for an Architectural Framework for the Internet of Things

The architectural framework for IoT provides a reference model that defines relationships among various IoT verticals (e.g., transportation, healthcare, etc.) and common architecture elements.

The standard also provides a reference architecture that builds upon the reference model. The reference architecture covers the definition of basic architectural building blocks and their ability to be integrated into multi-tiered systems.

6. Further Readings for Standards

a. ITU Standardization Roadmap

This document was released on 6 May 2016. It contains a collection of Standards/ITU-T Recommendations that fit into the scope of Joint Coordination Activity for IoT and Smart Cities. It includes Standards/ITU-T Recommendations related to Internet of Things (IoT), smart cities and communities (SC&C), network aspects of identification systems, including RFID (NID) and ubiquitous sensor networks (USN). Refer References for the link.

b. IERC Position Paper on IoT Standardization:

It presents an inventory of existing standards and provides an overview of past and current activity in relation to standardization in the area of Internet of Things, and assembles a series of examples of standardization activities in this area.

Annex-I (Smart Parking)

The following standards and certifications need to be followed:

1. **Entry Device**
   i. Communication protocol should be TCP/IP
   ii. Conform ISO 9001 Quality Assurance Standard
   iii. CE, FCC, IC, CNRTLUS certified
   iv. Degree of protection based on IEC 60529: IP43

2. **Exit Device**
   i. Conform ISO 9001 Quality Assurance Standard

3. **Entry/Exit Barrier**
   i. The Barrier unit must conform to ISO 9001 Quality Assurance standards
   ii. CE, Ukr - Sepro certified
   iii. Degree of protection: IP34D

4. **Sensors**
   i. Conform ISO 9001 Quality Assurance Standard
   ii. Protection Level: IP67

5. **Parking light aisle indicators**
   i. Conform ISO 9001 Quality Assurance Standard
   ii. Protection Level: IP55

6. **Indoor LED indicators**
   i. Conform ISO 9001 Quality Assurance Standard
   ii. Protection Level: IP33
   iii. Communications: Bus RS-485

7. **Other Technical Specifications**

Annex-J (Public WI-FI)

1. All equipment must support the following standards/capabilities:

i. 802.11n

ii. 802.11ac

iii. 802.11e Quality of Service (QoS)

iv. WMM Wireless Multimedia Extensions

v. WMM Powersave

vi. 802.11h Dynamic Frequency Selection and Transmit Power Control

vii. 802.11i Security, including AES

viii. 802.1X with dynamic VLAN policies

ix. WPA2-Enterprise certification

x. 802.11r Roaming

xi. preferred: 3X3 MIMO

xii. preferred: Polycom/SpectraLink VIEW Certification, SpectraLink Voice Priority

xiii. preferred: Wi-Fi Certified Voice-Enterprise

2. Wireless Access points specs

i. Shall be IEEE 802.11ac compliant concurrent dual radio access point.

ii. Shall feature a three spatial-stream 802.11ac (3x3 MIMO) integrated or external dual band (2.4GHz & 5GHz) antenna.

iii. Shall have 802.3af or 802.3at compliant Gigabit PoE UTP port and a console port.

iv. Shall be IEEE 802.3af PoE compliant and both the radios shall operate at full power and full performance on 802.3af PoE/Gigabit Ethernet.

v. Shall be Wi-Fi Alliance certified for interoperability with all IEEE 802.11a/b/g/n/ac client devices.

vi. Shall support up to 16 SSID/VSC profiles.

vii. Shall support simultaneous detection & prevention of wireless threats on 2.4GHz & 5GHz frequency bands.

viii. Shall support both centrally managed mode (configured and updated via a controller) and autonomous mode (standalone in the absence of a controller).

ix. Shall support auto-selection of RF channel and transmit power.

x. Shall support enforcement of client authorization based on user credentials (802.1X/EAP), and hardware identifiers (MAC address, WEP key).

xi. Shall support ACS or similar feature to reduce co-channel interference (CCI) by automatically selecting an unoccupied radio channel.

xii. Must support Proactive Key Caching and/or other methods for Fast Secure Roaming.

xiii. AP model proposed must be able to be both a client-serving AP and a monitor-only AP for Intrusion Prevention services

xiv. Must support up to 23dbm of transmit power in both 2.4 GHz and 5 GHz radios.

xv. The Wireless AP should have the technology to improve downlink performance to all mobile devices including one-, two-, and three spatial stream devices on 802.11n. The technology should use advanced signal processing techniques and multiple transmit paths to optimize the signal received by 802.11 clients in the downlink direction without requiring feedback and should work with all existing 802.11 clients.

Annex-H (Disaster Management)

The aim of the local disaster management standards and guidelines is to support local government / municipal corporations to develop a community specific disaster management system, including governance arrangements, a Local Disaster Management Plan (LDMP) using the comprehensive approach to disaster management.

This standard establishes a common set of criteria for all hazards disaster/emergency management with fundamental criteria to develop, implement, assess, and maintain the program for prevention, mitigation, preparedness, response, continuity and recovery.

International Standards used in Disaster Warning and Management

S. No.	Standards	Description
1.	ISO 22320:2011	Societal security – Emergency management – Requirements for incident response deals with overall approach for preventing and managing emergencies /disasters
2.	ISO 22322:2015	Societal security -- Emergency management -- Guidelines for Public warning deals with guidelines for developing, managing, and implementing Public warning before, during, and after incidents / disasters
3.	ISO 22324:2015	Societal security — Emergency management — Guidelines for colour-coded alerts deals with guidelines for the use of colour codes to inform people at risk as well as first response personnel about danger and to express the severity of a situation. It is applicable to all types of hazard in any location.
4.	ISO 31000:2009, *Risk management – Principles and guidelines*	It deals with principles, framework and a process for managing risk. It helps organizations / local bodies to increase the likelihood of achieving objectives, improve the identification of opportunities and threats and effectively allocate and use resources for risk treatment.
5.	IEC 31010:2009, Risk management -- Risk assessment techniques	It helps the decision makers understand the risks that could affect the achievement of objectives as well as the adequacy of the controls already in place. It focuses on risk assessment concepts, processes and the selection of risk assessment techniques.
6.	ISO 11320:2011	Nuclear criticality safety -- Emergency preparedness and response
7.	ASCE/SEI 41-06 - *Seismic Rehabilitation of Existing Buildings*	Standards for Seismic retrofitting of existing building including steps to better protect non-structural components (suspended ceilings, non-load-bearing walls and utility systems) and building contents (furnishings, supplies, inventory and equipment)
8.	ISO 19115-1:2014	Defines the schema required for describing geographic information and services by means of metadata. It provides information about the identification, the extent, the quality, the spatial and temporal aspects, the content, the spatial reference, the portrayal, distribution, and other properties of digital geographic data and services