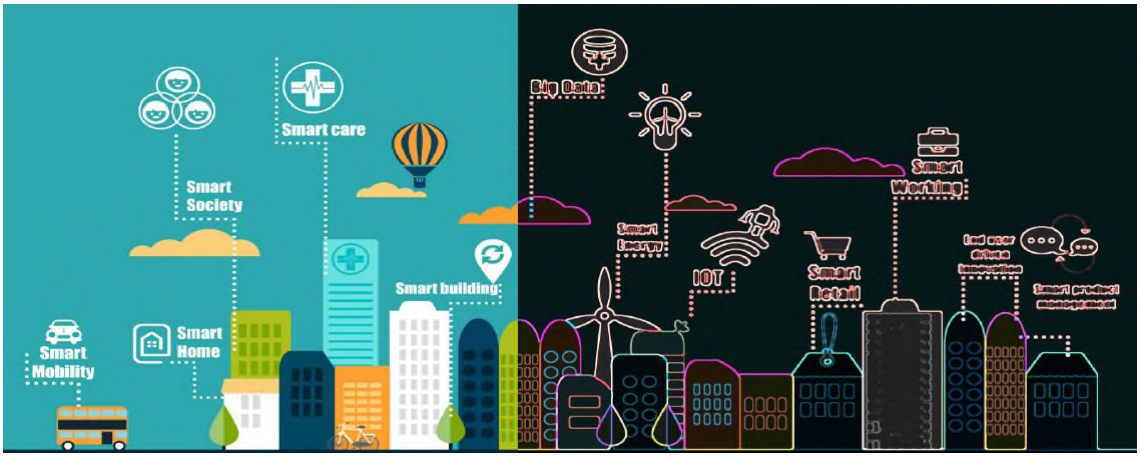
Dehradun Smart City Limited
Request for Proposal

for

Selection of Master System Integrator for establishment of Doon Integrated Command & Control Center (DICCC) and Other Integrated Smart Solutions at Dehradun



DEHRADUN
SMART CITY LTD.

RFP Ref No.: 01/DSCL/18-19/DICCC

Volume II: Scope of Work

Disclaimer

Dehradun Smart City Proposal (SCP) has been selected to implement the Area Based Development (ABD) and Pan-City proposals by Government of India (GoI) under Smart City Mission (SCM). DSCL SCP proposes served smart solution in ADB and cross pan-city providing various Smart feature/infrastructure.

To implement Smart City projects in DSCL, Dehradun Municipal Corporation and Uttarakhand Government has formed a SPV called Dehradun Smart City Ltd. (DSCL).

The DSCL has prepared this Request for Proposals (RFP) for **Selection of Master System Integrator for establishment of Doon Integrated Command & Control Center (DICCC) and Other Integrated Smart Solutions at Dehradun"**. The RFP is a detailed document with specifies terms and conditions on which the bidder is expected to work. These terms and conditions are designed keeping in view the overall aim and objectives of the Command and Control Centre. DSCL has taken due care in preparation of information contained herein and believes it to be accurate. However, neither DSCL or any of its authorities or agencies nor any of their respective officers employees, agents, or advisors gives any warranty or make any representations, express, or implied as to the completeness or accuracy of the information contained in this document or any information which may be provided in association with it.

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

DSCL reserves the right not to proceed with the project, to alter the timetable reflected in this document, or to change the process or procedure to be applied. It also reserves the right to decline to discuss the Project further with any party submitting a proposal. No reimbursement of cost of any type will be paid to persons, entities, or consortiums submitting a Proposal.

Definitions/Acronyms

Terms	Meanings
ABD	Area Based Development
AMC	Annual Maintenance Contract
ANPR	Automatic Number Plate Recognition
ATCS	Adaptive Traffic Control System
BOM	Bill of Material
CCTV	Closed Circuit Television
COTS	Commercial Off-The-Shelf
CSP	Cloud Service Provider
DC	Data Centre
DMS	Document Management System
DRC	Disaster Recovery Centre
ECB	Emergency Call Box
EMD	Earnest Money Deposit
FMS	Facility Management Services
GIS	Geographical Information System
GPS	Global Positioning System
GSM	Global System for Mobile Communication
GST	Goods and Services Tax
DICCC	Doon Integrated Command and Control Centre
ICT	Information and Communication Technology
IP	Internet Protocol
IPF	Information Processing Facility
ISO	International Organization for Standardization
ISWM	Integrated Solid Waste Management
IT	Information Technology
ITDP	Institute for Transportation and Development Policy
ITMS	Intelligent Traffic Management System
KPI	Key Performance Indicator
LOA	Letter of Acceptance
MIS	Management Information System
MSI	Master System Integrator
NIT	Notice Inviting Tender

Terms	Meanings
OEM	Original Equipment Manufacture
OFC	Optical Fiber Cable
PA	Public Address
PoP	Point of Presence
PTZ	Pan Tilt Zoom
RFP	Request for Proposal
RACI	Responsible, Accountable, Confirm, Inform
RLVD	Red Light Violation Detection
DSCL	Dehradun Smart City Ltd.
SCM	Smart City Mission
SCP	Smart City Proposal
SDC	State Data Centre
SLA	Service Level Agreement
SOP	Standard Operating Procedures
SPV	Special Purpose Vehicle
SVD	Speed Violation Detection
TCV	Total Contract Value
TDS	Tax Deducted at Source
TPA	Third Party Auditor
UAT	User Acceptance Testing
UPS	Uninterrupted Power Supply
VAT	Value Added Tax
VM	Virtual Machine
VMS	Variable Message Sign
VA	Video Analytics

Table of Contents

1 Introduction

1.2 Project Objectives

The key objective of this project is to establish a collaborative framework where input from different smart solutions implemented by DSCL, and other stakeholders can be assimilated and analysed on a single platform; consequently, resulting in aggregated city level information. Further this aggregated city level information can be converted to actionable intelligence, which would be propagated to relevant stakeholders and citizens in coordinated and collaborative manner.

The Dehradun City administration intends to use Command and Control Center (Smart City Platform) applications for monitoring and/or operating the Smart city services terminating onto these applications. While each agency delivering, their respective solutions will have their own operations applications individually, the true value of Smart City is delivered when there is a consolidated and integrated view of all these operations for the administrators. Also, when one agency application can use the data and intelligence gathered from operations of other agency, not necessarily controlling other agencies operations; Civic Services are delivered with lot more efficiency and in an informed fashion.

An example is that when police department comes to know about the real-time status of outdoor lighting, then they will be better informed on where to concentrate their patrolling on. Or when citizens come to know where there is good possibility of getting a parking in the city centre, they don't spend time looking for parking without any knowledge. This way traffic on the roads is reduced. This DICCC applications is expected to enable such transformation of the city operations.

Expectation from MSI is to provide, deploy and configure an integrated operations and dashboard application that integrated various Smart City use cases on this common Smart City Platform.

DICCC will be established for Dehradun smart city to run city operations. Citizens will be using ICT as backbone and seamless integration must be completed with all the required & existing ICT systems / Smart components of Dehradun smart city initiatives.

DICCC will be a place where information from various departmental command centres and data related to various applications will be collected and analysed for better planning of the city. DICCC will have Analytical Intelligence engine which will process all the information and generate insights. These insights will be helpful in managing incidents across the city and do a better planning for the development. DICCC will also play a role of decision support system.

Doon Integrated Command & Control Centre (DICCC) along with the Smart City Data Center shall be set-up in ITDA Building, Department of Information Technology (Government of Uttarakhand). **The O&M for the Data Centre shall be taken care by the ITDA Department from the first day after the successful establishment of Data Centre by the MSI. The MSI has to quote the prices of OPEX in the price bid BOQ exclusive of the O&M prices for the data centre.**

Benefit envisaged from DICCC to City Administration and Citizens are as under:

City Administration	• The implementation of Pan City interventions will ensure efficient traffic management, as well as safety and crowd surveillance. • The central command and control will ensure efficient continued working of the field equipment • Continuous surveillance would help in main lead to reduction in number of criminal and unlawful activities, number of traffic rule violations, illegal parking, encroachments etc. • Prompt emergency response in cases of accidents, fires, disasters, epidemics, etc. due to availability of real time data and response mechanisms • Reduction in unscheduled outage of street lights, citizen amenities etc. due to remote monitoring system • To lower the costs by adopting a centralized architecture, enabling the platform to be administered and supported from one location • Instant MIS reports for planning, budgeting, monitoring & evaluation • Instant identification of delay points has enabled prompt administrative action • Holistic citizen engagement and interaction platform that will bring the citizens to the forefront of the development process while engaging citizens through the use of social media, online communities and discussion forums. • Facilitate cross-department collaboration with the help of online systems in compliance with various standard operating procedures will bring transparency in city administration

Citizens	• Better city planning and development • Services delivered to citizens, faster, and at a lower operating expense • Local economic development • Citizens will also be able to have access to efficient, safe & reliable Urban Transport System with adequate provisions for NMT modes • Single window experience for citizens to apply for various citizen services Birth, Death, Marriage, Income, Caste, Domicile etc. and get them from a single window • Improve communication between government administrators and citizens by building an interactive Web portal to disseminate information and submit grievances

DICCC should be scalable to host more applications and services in future for managing city more effectively. DICCC will manage utilities for ABD area, and in future capable of managing utilities of the entire city.

Following are the key outcomes expected to be achieved by the proposed interventions:

a. Improved visualization of ambient or emergency in the city and facilitation of data driven decision making
b. Efficient traffic management
c. Enhanced safety and security
d. Better management of utilities and quantification of services
e. Asset Management
f. Disaster Management and Emergency Response
g. Efficiency improvement in public service delivery
h. Interdepartmental coordination and collaboration for faster execution of services
i. Implementation and Integration with all existing and all future services as identified by Dehradun Smart City limited (DSCL) in the city including but not limited to (with provision for future scalability):

- CCTV Surveillance System
- Smart Lighting
- Data Centre
- Disaster Recovery Centre
- Doon Integrated Command and Control Centre
- ICT Enabled Solid Waste Management
- Intelligent Traffic Management System
- E-Challan System
- Public Bike Sharing
- Smart Water Supply System

- Smart Education
- Smart Health Management System
- Intelligent public transport Management
- Smart pole
- Smart Energy Management system
- Pot hole management

1.3 Purpose of this RFP

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

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

This RFP is designed to provide interested bidders with sufficient basic information to submit proposals meeting minimum requirements but is not intended to limit a proposal's content or exclude any relevant or essential data.

Bidders are at liberty and are encouraged to expand upon the specifications to evidence superior bid understanding and service capability.

2 Project Overview and Components

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

S. No.	Component	Geographical Scope
1.	Network Backbone	As per requirement for field equipment's
2.	Command & Control Centre	Located centrally at one location
3.	Data Centre and DR Site	▪ Smart and energy efficient Data Centre located centrally with Command & Control Centre ▪ Cloud DR set-up
4.	ITMS	
5.	City Wi-Fi	
6.	City Surveillance	
7.	Transit Management System	
8.	Environmental Monitoring System	
9.	Enterprise GIS	
10.	Solid Waste Management	
11.	Web Portal & Mobile App	City portal and mobile app to disseminate information, info graphics and service delivery through integration with stakeholder departments
12.	Variable Message Sign Board	
13.	Emergency Helpdesk	
14.	Video Conference Solution	
15.	Citizen Centric Services	

2.1 Components & Services Scope Overview

The selected MSI shall ensure the successful implementation of the proposed DICCC solutions as well as provide capacity building support to city authorities as per the scope of services described below. Any functionality not expressly stated in this document but required to meet the needs of the DSCL to ensure successful operations of the system shall essentially be under the scope of MSI and for that no extra charges shall be admissible. MSI shall implement and deliver the systems and components which are described in this RFP. MSI's scope of work shall include but will not be limited to the following broad areas. Details of each of these broad areas have also been outlined in Annexures:

1. **Assessment, Scoping and Survey Study**: Conduct a detailed assessment, survey, gap analysis, scoping study and develop a comprehensive project plan, including:

a) Assess existing ICT systems, Network connectivity within the city and the greenfield site for the scope items mentioned in this Volume of the RFP

b) Conduct site survey for finalization of detailed technical architecture, g a p analysis, final Bill of Quantities and project implementation plan

c) Conduct site surveys to identify the need for site preparation activities

d) Obtain site clearance obligations & other relevant permissions with the support of DSCL

2. Design, Supply, Configuration, Installation, Implementation, Testing and Commissioning of the following primary components:

a) Doon Integrated Command and Control Centre

b) Smart Data Centre within DICCC Building

c) Disaster Recovery Centre (Hosted on cloud data centre of any MEITY empanelled Cloud Service Provider). All H/W and S/W on cloud should meet the specification in RFP. The cloud provider should be MEITY empanelled as well as STQC certified Govt. community cloud (GCC).

d) City Surveillance

e) Intelligent Traffic Management System

- Adaptive Traffic Control System (ATCS)
- Automatic Number Plate Recognition (ANPR) System
- Red Light Violation Detection (RLVD) System
- Speed Violation Detection (SVD) System
- Traffic Violation Cameras
- Traffic monitoring and control sensors
- Centralized Traffic suit
- Variable Message Sign boards
- Public Address (PA)
- Emergency Call Box (ECB) System

f) Environmental Monitoring Sensors

g) City Web Portal & Mobile App

h) Enterprise GIS Portal

i) Public Wi-Fi Hotspots

j) Work Flow and DMS

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

3. Integration with existing and proposed system ICT systems within DSCL ICT landscape

4. **Data Centre:** Provisioning of Hardware, Network and Software Infrastructure, which includes design, supply, installation and commissioning of ICT Infrastructure at the Command and Control Centre; Smart Data Centre. This scope consist of:

a) Site preparation services

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

c) Command Centre infrastructure including operator Video Walls, workstations, IP phones, joystick controller etc.

d) Establishment of LAN and WAN connectivity at command centre and DC limited to scope of infrastructure procured for the project
e) Application integration services with the above identified applications

5. Provisioning of City-wide Network backbone within the city and the greenfield site

a) Assessment of ISP service provider available in city
b) Connectivity between field device and DC and DICCC
c) Connectivity between DC & proposed DR
d) Internet Connectivity at DC
e) Network shall be sized with sufficient capacity to support the redundancy and future traffic growth in order to complete traffic rerouting on the network in event of failure without affecting overall network performance.

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

a) Training of city authorities, operators and other stakeholders on operationalization of the system
b) Support during execution of acceptance testing
c) Preparation and implementation of the information security policy, including policies on backup and redundancy plan
d) Preparation of revised KPIs for performance monitoring of various urban utilities monitored through the system envisaged to be implemented.
e) To improve the operations and accountability of the proposed solutions they will be mapped with their KPIs.
f) Developing standard operating procedures for operations management and other services to be rendered by DICCC
g) Preparation of system documents, user manuals, performance manuals, Operation manual etc.

7. Operations and Maintenance

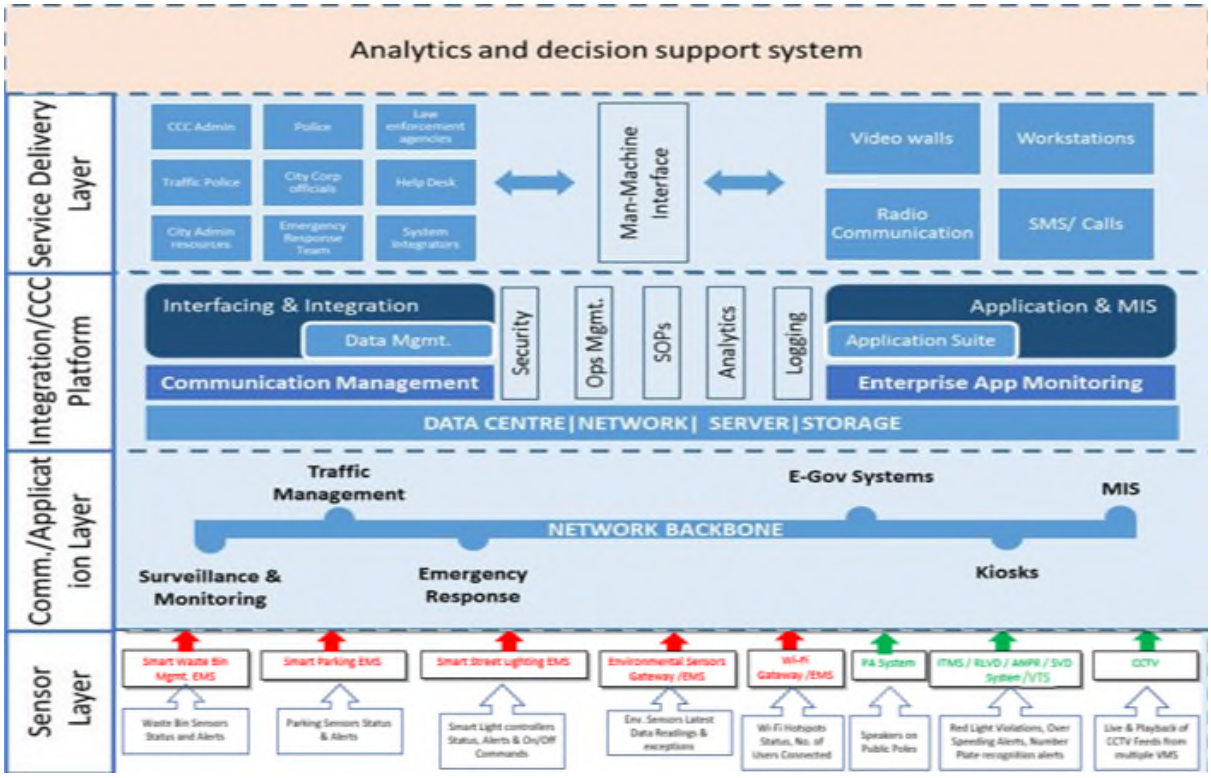
The O&M shall be for a period of 5 years from the Go-Live date of implemented solutions in an efficient and effective manner.

The O&M for the Data Centre shall be taken care by the ITDA Department from the first day after the successful establishment of Data Centre by the MSI. The MSI has to quote the prices of OPEX in the price bid BOQ exclusive of the O&M prices for the data centre.

2.2 Component Architecture

Indicative Framework of the solution envisaged under the ““Doon Integrated Command and Control Centre” is as given below.

Please note that this Framework is indicative in nature and is given in the RFP to bring clarity to prospective bidders on the overall scope of project and its intended use. MSI shall carry out the detail requirement analysis and finalize technical architecture in consultation with authority and its consultants.



The architecture layers of the complete network of smart elements is as follows:

a) Sensor or Field instrument layer

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

b) Data Collection and Transmitting Layer

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

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

c) Network/Communication Layer

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

d) Data Centre Layer

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

e) Security Layer

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

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

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

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

f) Smart Application and Integration Layer

The smart applications layer will contain data aggregation and management systems (rules engines, alerting systems, diagnostics systems, control systems, messaging system, events

handling system), and reporting / dashboard system to provide actionable information to city administrators and citizens. It will be an evolving layer with applications added and integrated as and when new applications are developed at DSCL. While aspects of ambient conditions within the city will be gathered through various sensors deployed, some city specific data will come from other government and non-government agencies. It is through the integration layer – that data will be exchanged to and from the underlying architecture components and other data from system developed by government (such as police department, meteorological department, street lights department, water department, irrigation department, transport organizations within DSCL , etc.) and non-government agencies.

g) Service delivery and Publishing Layer

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

h) Command and Control Centre.

The unified Command & Control Centre need to be developed as per the ISO standard 11064 and shall serve as a shared space to host backend systems of various Pan City ICT components listed in this DPR. It will be a common facility from where various smart components shall be operated and monitored such as smart signals, smart vehicles, intelligent street lights, smart parking, bicycle pods, etc.

The key objectives of establishing the Command & Control Centre are as below:

- Integrated Platform for control monitored managing traffic flows on the roads in the city and various other systems related to traffic management.
- Platform for monitoring operational and performance aspects related to public transport, parking, information dissemination, citizen service delivery, etc.
- Aggregation of various data feeds received from sensors/systems and further process information out of these data feeds to provide interface /dashboards for generating alerts and notifications in real time.
- Equip city administration to respond quickly and effectively to any incidents/ crisis situation in city in collaborative and coordinated manner in response to incidents/emergencies/crisis situations.
- CCC shall house various smart components feed and information, which shall use the data and intelligence gathered from operations of other to enable the data and analytics platform for batter decision management system.

Functional Layout of DDICCC

DC is proposed to have following provisions within the CCC:

- Command and Control Centre room with video wall and workstations for viewing man-power. Data center, IT team room, ups room.

- Meeting rooms, Conference Room, War room facilities
- Changing and locker room (for Gents and Ladies)
- Sitting space for helpdesk support from the MSI & space for technical staff to carry out repairs/ troubleshooting
- MSI will do load bearing capacity test of data center floor and he will do the floor strengthening if required.
- MSI has to provision space for min 15 person in DICCC for viewing Dashboard. He has to plan 5 person of MSI for viewing DICCC and rest may join from other department.

A broad level indicative representation of above requirements is specified in the suggestive layout below. This layout is indicative and subject to change as per the actual feasibility and construction norms.

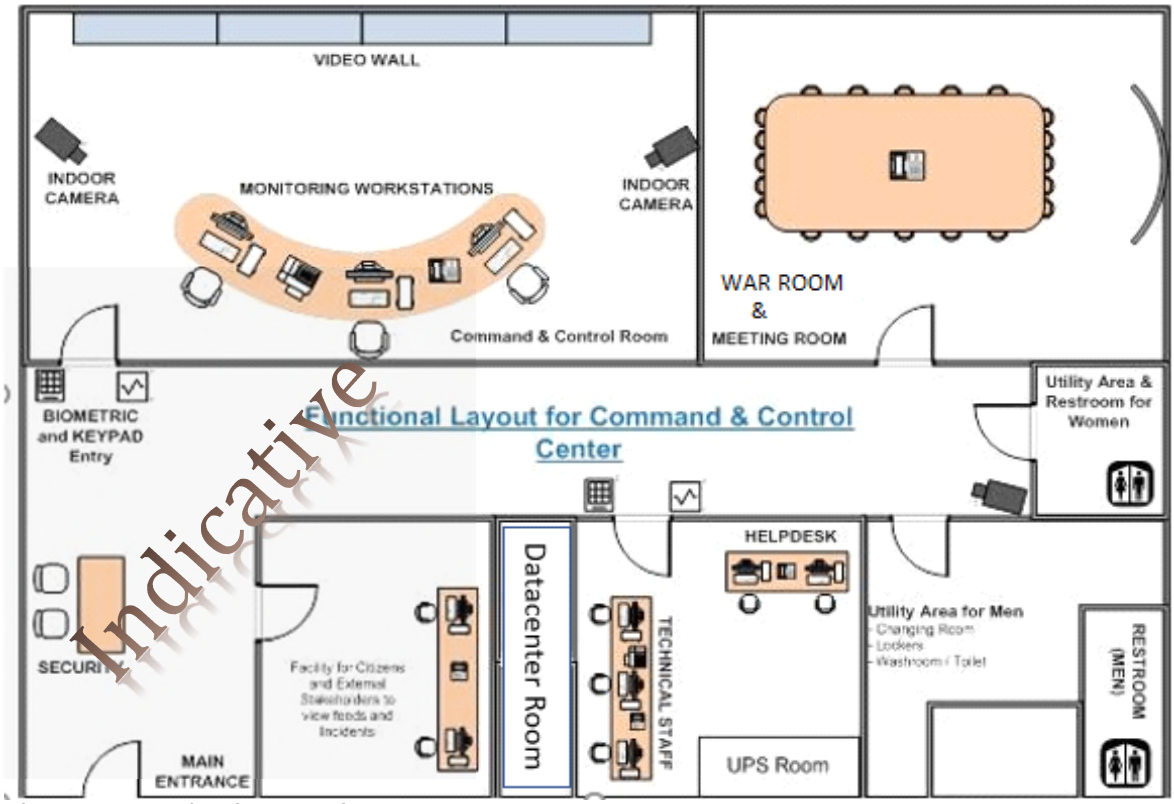


Figure 2-1: Functional Layout of CCC

2.3 Survey, Deign Consideration for finalization of detailed technical architecture and project plan.

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

1. Names of the Project Team members, their roles & responsibilities and deliverables.

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

3. Responsibility assignment matrix for all stakeholders.

4. Risks that MSI anticipates and the plans they have towards their mitigation.

5. Detailed project plan specifying dependencies between various project activities / sub-activities and their timelines.

6. Installation locations for field devices geo mapped to visually identify the geographical area.

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

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

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

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

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

2. Application component design including component deployment views, control flows, etc.

3. Low Level Design (including but not limited to) Application flows and logic including pseudo code, GUI design (screen design, navigation, etc.), Database architecture, including defining data structure, data dictionary as per standards laid-down by Government of India.

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

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

6. Location of Junction Boxes, Wi-Fi Access Points.

7. Electrical power provisioning.

MSI shall also identify the customizations/ workaround that would be required for successful implementation and operation of the project. The report should take into consideration following guiding principles:

- **Transformational Nature of Smart City applications** - Applications should look to fully embrace mobile adoption, online authentication, etc. to transform the processes completely and offer wider choice and no/low touch point for residents to interact

directly. It is critical that project design are aligned to larger trends and designed for next decade rather than past.

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

- **Distributed, PKI based Authentication and Authorization** - The solution shall support PKI based Authentication and Authorization, in accordance with IT Act 2008, using the Digital Certificates issued by the Certifying Authorities (CA). In particular, 3 factor authentications (login id & password, biometric and digital signature) shall be implemented by the MSI for officials/employees involved in processing citizen services.

- **Security and privacy of data** – The security services will cover the user profile management, authentication and authorization aspects of security control. This service run across all the layers since service components from different layers will interact with the security components. All public contents should be made available to all users without authentication. The service will authenticate users and allows access to other features of the envisaged application for which the user is entitled to. The system should be designed to provide the appropriate security levels commiserate with the domain of operation. Also the system will ensure data confidentiality and data integrity. The architecture must adopt an end-to-end security model that protects data and the infrastructure from malicious attacks, theft, natural disasters etc. SI must make provisions for security of field equipment as well as protection of the software system from hackers and other threats. Using Firewalls and Intrusion Prevention Systems such attacks and theft should be controlled and well supported (and implemented) with the security policy. The virus and worm attacks should be well defended with gateway level Anti-virus system, along with workstation level Anti-virus mechanism. There should also be an 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. Bidder's solution shall adhere to the model framework of cyber security requirements set for Smart City (K-15016/61/2016-SC-1, Government of India, and Ministry of Urban Development).

Field equipment installed through 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 equipment's 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.
- The security services used to protect the solution shall include: Identification, Authentication, Access Control, Administration and Audit and support for industry standard protocols.
- The solution shall support advanced user authentication mechanisms including digital certificates and biometric authentication.
- 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.
- 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.
- The overarching requirement is the need to comply with ISO 27001 standards of security.
- The application design and development should comply with OWASP top 10 principles
- A secure solution should be provided at the hardware infrastructure level, software level, and access level.
- Authentication, Authorization & Access Control: 3 factors (User ID & Password, Biometric, and Digital Signature) security mechanisms should be implemented to enable secure login and authorized access to portal information and services.
- Encryption Confidentiality of sensitive information and data of users and portal information should be ensured.
- Appropriate mechanisms, protocols, and algorithms necessary to protect sensitive and confirmation data and information both during communication and storage should be implemented.
- Data security policies and standards to be used as per government of India guideline.
- In order to adequately provide access to secured information, security needs must be identified and developed at the data level. Database design must consider and incorporate data integrity requirements.
- Role based access for all the stake holders to be implemented to access and use the system
- Ability to adopt other authentication mechanism such as Electronic Signature Certificates
- Authorization validity to be ensured for the users providing the Data to the system. Data should be accepted only from the entity authorized
- Audit trails and Audit logging mechanism to be built in the system to ensure that user action can be established and can investigated if any can be aided(e.g. Logging of IP Address etc.)
- Data alterations etc. through unauthorized channel should be prevented.

- Industry good practice for coding of application so as to ensure sustenance to the Application Vulnerability Assessment
- Build a complete audit trail of all activities and operations using log reports, so that errors in system – intentional or otherwise – can be traced and corrected.
- Access controls must be provided to ensure that the system is not tampered or modified by the system operators.
- The security of the field devices must be ensured with system architecture designed in a way to secure the field devices in terms of physical damage & unauthorized access.
- The message exchange between various applications in the smart city should be fully encrypted and authenticated. Any application outside the Data Centre (DC) should talk to the applications hosted in the data center through predefined APIs only.
- APIs should be published and the IT systems be running on standard protocols like JSON / XML or REST etc.
- From a network security perspective all information that flows on the network should be encrypted to ensure safety and privacy of confidential data. The devices at each endpoint of the network should be authenticated (using mechanisms based on attributes one of which could use passwords). The authentication system so used on these endpoint devices should ensure that only authorized users are sending data over the network, and there is no rogue data that is sent to the control systems to generate false alarms or sabotage the systems.
- All IoT sensors deployed as part of Smart cities system should talk only to the authorized wireless network, and do not hook on to the rogue networks. The guidelines to secure Wi-Fi networks as published by Department of Telecom must be followed.
- Wireless layer of the Smart City Network should be segmented for public and utility networks by using Virtual Private Networks (VPNS) or separate networks in the wired core, so that any traffic from the internet users is not routed into the sensor networks and vice-versa.
- All traffic from the sensors in the Smart city to the application servers should be encrypted Secure Socket Layer (SSL) and authenticated prior to sending any information. The data at rest and in transit must be encrypted.
- Authentication of sensors in the Smart city should happen at the time of provisioning the sensors, and adding them into the system, and should be based on physical characteristics of the sensors like MAC ID, Device ID etc.
- Sensors deployed in solutions to set up Smart city should be hardened devices with the ability to be upgraded remotely for firmware through encrypted image files.
- The Sensors or edge device deployed in Smart city should not have any physical interface for administration. Monitoring of systems and networks should be undertaken remotely.
- All the sensors in the Smart city should connect to a completely separate network.
- As various sensors use multiple protocols to communicate with the underlying network with varied security capability, the system should allow provisioning necessary authentication and encryption at the gateway or the nearest data aggregation level if the sensor is not able to do the same.

- Secured Information and Event Management system monitoring all Smart City networks, devices and sensors to identify malicious traffic.
- Block chain solution should be implemented by MSI for website monitoring.
- Data should be encrypted at database and application level. Hardware based encryption which has the capacity of working in layer 3 and it should be doing the encryption key mgt as well. The proposed solution should be able to encrypt everything at a min 1024 bit.

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

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

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

Document Management System which has at least one live implementation site in India in Govt/PSU with more than 10 crores document archived in document management repository with more than 5000 users using this Document Management System.

Document Management System (DMS)

- The system should be platform independent and should support both Linux and Windows platform. It should support both these platforms with or without virtualization.
- The system shall support separate Document/Image server for better management of documents and store only metadata information in database.
- Support open, scalable, Multi-tier architecture with each tier fully independent with support for clustering.
- Compliance to workflow standards: BPMN, BPEL and WFMC.
- Inter-operability - The systems must seamlessly integrate with any or all of the existing legacy and Core applications and shall support interface with other open-standard systems.
- The system shall support multiple databases i.e. MS SQL, Oracle and PostgreSQL
- DAK Management and File Management should be licensed module and should be compliant with Manual of office procedure published by DARPG. They should be available in OEM price list.
- DMS, Work flow, DAK/Correspondence Management and File Management and Scanning component should be from a single OEM only.

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

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

- Deployment of multiple application instances should be possible.

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

- Network, DC, DR should be available 99.95 % time.

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

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

- **Manageability -** Ease of configuration, ongoing health monitoring, and failure detection are vital to the goals of scalability, availability, and security and must be able to match the scalability of the system.

- **Interoperability** - Keeping in view the evolving needs of interoperability, especially the possibility that the solution shall become the focal point of delivery of services, and may also involve cross-functionality with the e-Government projects of other departments / businesses in future, the solution should be built on Open Standards. The SI shall ensure that the application developed is easily integrated with the existing applications. The code does not

build a dependency on any proprietary software, particularly, through the use of proprietary 'stored procedures' belonging to a specific database product. The standards should:

(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).

(b) Be of leading industry standards and as per standards.

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 centres & 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 MSI. The MSI shall be held responsible for any delay/error/non-compliance/penalties etc. of its sub-contracted vendor. The details of the sub-contracting agreements (if any) between both the parties would be required to be submitted to city and approved by the Authority before resource mobilisation.

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

Sub-contracting /Outsourcing shall be allowed only for the work which is mentioned in the relevant clauses of Volume I of this RFP with prior written approval of DSCL. However, even if the work is sub-contracted/outsourced, the sole responsibility of the work shall lie with MSI. MSI shall be held responsible for any delay/error/non-compliance etc. of its sub-contracted vendor. The details of the sub-contracting agreements (if any) between both the parties would be required to be submitted to DSCL.

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

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

Application Architecture

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

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.

MSI 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 In-script 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.

i. Of compliance to citizen charter on delivery of services.
ii. Delay reports.

V. The standards should: 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

VI. 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/e-Authentication (AADHHAR Based) to authenticate approvals of service requests etc.

VII. 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.

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

IX. Complete mobile enablement of the Smart City System.

2.4 Commencement of Works

Site Clearance obligations & other relevant permissions –

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

2.5 Existing Traffic Signal system

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

2.6 Road signs

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

2.7 Electrical works and power supply

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

2.8 Lightning-proof measures

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

2.9 Earthing System

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

1. Earthing should be done for the entire power system and provisioning should be there to earth UPS systems, Power distribution units, AC units, etc. so as to avoid a ground differential. DSCL shall provide the necessary space required to prepare the earthing pits.

2. All metallic objects on the premises that are likely to be energized by electric currents should be effectively grounded.

3. There should be enough space between data and power cabling and there should not be any cross wiring of the two, in order to avoid any interference, or corruption of data.

4. The earth connections shall be properly made.

5. A complete copper mesh earthing grid needs to be installed for the server farm area, every rack need to be connected to this earthing grid. A separate earthing pit needs to be in place for this copper mesh.

6. Provide separate Earthing pits for Servers, & UPS as per the standards.

7. The metallic housing of electronic equipment/junction box/panel shall be connected to the earthing system.

8. The active electronic parts of an electronic equipment system shall be connected to the earthing system.

2.10 Junction Box, Poles and Cantilever

1. MSI shall provide the Junction Boxes, posts and cantilever to mount the field sensors like the cameras, traffic sensors, traffic light aspects, active network components, controller and power backup (UPS/Alternate energy sources) at all field locations, as per the specifications given in the RFP.

2. Junction Box needs to be appropriately sized in-order to accommodate the systems envisaged at the Junctions, and MSI should design the Junction box for 1.5 times the actual size MSI requires for utilization under the ITMS project.

3. Additional 50% space in the Junction Box shall be utilized by DSCL to accommodate any future requirements under other projects.

4. Junction Box for UPS with Battery bank needs to be considered separately. Bidder may propose solar based solutions to power the equipment. In this case, raw power can be used as backup supply whenever solar power is not able to meet the requirement.

5. It should be noted that MSI would have designed the Junction box keeping in mind the scalability requirements of ITMS project, and the additional 50% volume needs to considered over and above such requirement.

6. The junction box should be designed in a way that, separate compartment will be available for separate system (i.e. ITMS Controller, Mini server, Active component, etc.). Each compartment shall have lock & key facility. There should be provision made to integrate the systems if required.

2.11 Cabling Infrastructure

1. MSI shall provide standardized cabling for all devices and subsystems.

2. MSI shall ensure the installation of all necessary cables and connectors between the field sensors /devices assembly, outstation junction box, for pole mounted field sensors/devices the cables shall be routed down the inside of the pole and through underground duct to the outstation cabinet.

3. All cables shall be clearly labeled with indelible indications that can clearly be identified by maintenance personnel. The proposed cables shall meet the valid directives and standards.

4. Cabling must be carried out per relevant BIS standards. All cabling shall be documented in a cable plan by MSI.

2.12 Doon Integrated Command & Control Centre (DICCC)

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

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

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

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

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

High Availability / Up Time Targets for DICCC operations are identified as follows:

- Availability Target (24Hr operation): 99.582%.
- Maximum Downtime Tolerated per Day: 6 minutes.
- Maximum Downtime Tolerated per Week: 42 minutes.
- Devices are expected to give 99.99% uptime for application. MTBF for devices are expected to be greater than 95%.

Integrated city operation platform should be able to carter to following requirements;

1. Urban Services and Data APIs:

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

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

i. For example Lighting APIs: Vendor agnostic APIs to control Lighting functionality.

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

2. Platform functionality:

a. API management and gateway: Provides secure API lifecycle, monitoring mechanism for available APIs.

b. User and subscription management: Provides different tier of user categorization, authentication, authorization, and services based on the subscriptions.

c. Application management: Provides role-based access view to applications.

d. Enabling analytics: Time shifted and real-time data available for big data and analytics.

e. Domain and/or Insight reports

i. Parking occupancy, energy reports, AQI report (environmental pollution).

Use cases of DICCC- MSI has to do to the implementation as per detailed specification given in the RFP.

Departments/ Systems	Relevant DICCC Use Cases	Information to be displayed in DICCC
Solid Waste Management	Show position of Fleet on the city map	Real-time/Near real- time location of the Fleet
	Display type of fleet vehicle	Categorized information of various fleet types available in the city
	Show status of Garbage collection by ward	Real-time/Near real- time status of Garbage collection in each ward
Transit Management System	Show position of Buses on the bus route	Documentation of Bus Routes
		Real-time/Near real- time location of the Buses
ITMS & City Surveillance	Show location of traffic lights	Location coordinates of traffic light installations at junctions
	Show Status of Traffic Lights	Real-time/Near real- time status of traffic lights downtime
	Show location of CCTV Cameras	Location coordinates of CCTV Cameras installations at junctions
	Show Status of CCTV Cameras	Real-time/Near real- time status of CCTV Cameras downtime
	Show location of Enforcement System	Location coordinates of Enforcement System installations at junctions
	Show Status of Enforcement System	Real-time/Near real- time status of Enforcement System downtime

	Show location of VMD Boards	Location coordinates of VMD Boards installations at junctions
	Show Status of VMD Boards	Real-time/Near real- time status of VMD Boards downtime
Electrical/Power SCADA	Identify location of Energy Assets	Location coordinates of Energy Assets
	Show the Energy Network on GIS map	Location of Energy network (pipelines) across the city
	Identify status of Energy Assets (Sub-stations, Transmission network etc.)	Real-time/Near real- time status of energy assets downtime
Smart Parking System	Identify location and number of Parking Slots	Location coordinates and Information of Parking facilities
	Show availability status of Parking Slots	Real-time/Near real- time status of Parking Occupancy (2-wheeler and 4- wheeler)
	Show Revenue Collections by each Parking Facility	Real-time/Near real- time status of Parking Fee Collections (2-wheeler and 4-wheeler)
Street Lights	Identify location of Street Lights	Location coordinates of Street Lights
	Control Street Lights status	Real-time/Near real- time status of street lights functioning
	Show Status of Street Lights	Real-time/Near real- time status of street lights functioning
Property Tax	Show the Properties on GIS map	Location geo-fenced coordinates of Properties
	Display heat map of tax collections by each ward	Tax collections data by each ward
E-Governance	Show Population by each ward	Base Population data based on latest census
		Birth and Death data at a regular frequency
	Transmit information to citizens	Data/Information that has to be broadcast to citizens
	Show status of Grievances by Ward	Details of Grievances received
	Show location of Public Advertisement Boards	Location coordinates of Public Advertisements
	Show Public Advertisements availability status	Booking status of Public Advertisements
	Display heat map of advertisement tax collections by each ward	Tax collections data by each ward

Emergency Management	Identify Location of Fire Hydrants	Location coordinates of Fire Hydrants
	Show position of Fleet on the city map	Real-time/Near real- time location of the Fleet
	Display type of fleet vehicle	Categorized information of various fleet types available in the city
	Respond to Emergency Situation	Documented Standard Operating Procedures
Water	Identify location of Water Assets	Location coordinates of Water Assets
	Show the Water Network on GIS map	Location of water network (pipelines) across the city
	Identify status of Water Assets (Overhead Tanks, Pumps etc.)	Real-time/Near real- time status of Water assets downtime
	Display heat map of high water usage areas	Meter Readings from various Commercial and Residential installations with their location details
	Identification of Non-Revenue water	Water inflow details across the water network
Smart Poles	Identify location of Smart Poles	Location coordinates of Smart Poles
	Show Status of Smart Poles – Wi-Fi Hotspots	Real-time/Near real- time status of Wi-Fi Hotspots functioning
	Show Status of Smart Poles - Panic Button/Emergency Call Box	Real-time/Near real- time status of Panic Button/Emergency Call Box functioning
	Show Status of Smart Poles - Public Address System	Real-time/Near real- time status of PAS functioning
	Show Status of Smart Poles - Environmental sensors	Real-time/Near real- time status of Environmental Sensors functioning
	Show Status of Smart Poles - Smart Billboards	Real-time/Near real- time status of Smart Billboards functioning
	Show Status of Smart Poles - Surveillance	Real-time/Near real- time status of Surveillance Cameras functioning
	Show Status of Smart Poles - LED Lights	Real-time/Near real- time status of LED Lights functioning
	Show Status of Smart Poles - Solar Panel	Real-time/Near real- time status of Solar Panel functioning
	Receive and Display Surveillance Feed	Real-time/Near real- time feed of Surveillance Cameras

	Receive and Display Environmental Sensor Feed	Real-time/Near real- time feed of Environmental Sensors
	Broadcast message on PAS	Message to be broadcast on PAS
	Play music on PAS	Music tracks to be played on PAS
	Receive and Send messages through Panic Button/ Emergency Call Box	Verbal communication will happen.
Pot hole management	should be integrated with Pot hole mgt solution	Citizen can send picture to department and it should be viewed on DICCC

2.13 Data Centre and Disaster Recovery Centre

- The DR for the data centre shall be on cloud on empanelled service providers by MeiTY. The cloud provider should be MEITY empanelled as well as STQC certified Govt. community cloud (GCC).
- Various ICT equipment to be provisioned and maintained by MSI at the Data Centre is given below.
- Only the minimum specifications for the active and passive ICT and Non-ICT components are specified.
- Surveillance Data should be stored for 30 days with 10 Frames per Second and maximum resolution.
- The DR should be replicated for 30 days. The backup storage should be active-active.
- Metadata for Analytics should be stored for 1 Year.
- MSI may propose Data Centre Virtualisation solution for price discovery
- MSI shall peruse the same provide the BOM/BOQ required to the meet the performance requirements as per the proposed business needs. MSI may also suggest additional components as per the solution requirements.
- The information between the Smart DC and the DR cloud shall be synchronised over the network such that that the smart city solutions are high available on the network.
- Operational and Uptime Requirements for Data Centre.

I. Minimum Tier Rating for Data Centre: **Tier 3**
   a. Availability Target (24Hr operation): 99.741%.
   b. Maximum Downtime Tolerated per Day: 4 minutes.
   c. Maximum Downtime Tolerated per Week: 27 minutes.
   d. Maximum Downtime Tolerated per Month: 1 hours 54 minutes.
   e. Maximum Downtime Tolerated per Quarter: 5 hours 42 minutes.
   f. Maximum Downtime Tolerated per Year: 22 hours 43 minutes.

II. Operational Compliance Requirements for MSI operations:
   a. PCI-DSS
   b. ISO 27001
   c. ISO 20000
   d. Cyber Security Framework for Smart City (MoUHA)

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

3 Expectation from MSI

1. MSI 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):

i- City Wi-Fi

ii- Surveillance Infrastructure – CCTV Cameras, Data communication, Monitoring, control room and Infrastructure.

iii- Other Smart City initiatives envisaged.

3. MSI shall assess existing infrastructure's current ability to support the entire solution and integrate the same with the proposed solution wherever applicable and possible
4. MSI shall judiciously evaluate the resources and time planned for undertaking the current state assessment, given the overall timelines and milestones of the project.
5. MSI 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. MSI 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 MSI.
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. MSI shall provide the bandwidth required for operationalizing each smart city initiative till the time Authority's own fiber is laid by the MSI as part of the scope of work of this RFP. The bandwidth requirement shall be analysed and procured by the MSI at its own cost/risk.
10. MSI shall Install and commission connectivity across all designated locations.
11. MSI shall establish high availability, reliability and redundancy of the network elements to meet the Service Level requirements.
12. MSI 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. MSI shall be responsible for up gradation, enhancement and provisioning additional supplies of network (including active/passive components), hardware, software, etc. as requisitioned by Authority.
14. MSI 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. MSI shall ensure that the end of support is not reached during the concurrency of the contract and 5 years thereafter.
16. MSI shall ensure compliance to all mandatory government regulations as amended from time to time.
17. The MSI shall ensure that all the peripherals, accessories, sub-components required for the functionality and completeness of the solution, including but not limited to devices, equipment, accessories, patch cords (fiber), cables, software, licenses, tools, etc. are provided according to the requirements of the solution.
18. Authority shall not be responsible if the MSI has not provisioned some components, sub-components, assemblies, sub-assemblies as part of Bill of Materials in the RFP. The MSI 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 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 Wi-Fi, 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.

Note:

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

2) MSI has to deploy the all the solutions with disable friendly features with in it to enable the more usage and help all type of users.

3.1 Inception Phase

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

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

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

iii. Establish and measure resource assignments and responsibilities

iv. Highlight the milestones and associated risks

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

vi. Measure project deadlines and performance objectives.

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

a. Results accomplished during the period (weekly).

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

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

d. Plan for the next week.

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

f. Support needed.

g. Highlights/lowlights.

h. Issues/Concerns.

i. Risks/Show stoppers along with mitigation.

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

3.2 Requirement Phase

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

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

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

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

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

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

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

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

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

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

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

3.3 Design Phase

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

3.4 Development Phase

MSI shall carefully consider the scope of work and provide a solution that best meets the project's requirements. Considering the scope set in this RFP, MSI shall carefully consider the solutions it proposes and explicitly mention the same in the technical proposal. The implementation of the application software will follow the procedure mentioned below:

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

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

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

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

iii. As per requirement of complex solution implementation MSI has to put requirement that OEM own resource & MSI best technical resources are deployed in this project.

iv. The OEM should provide the specific Designing (OEM Low Level Design, Core Implementation) support expertise to make sure that their supplied technology & products work as per the design objectives.

v. OEM to design and implement the complete security policy and workflow as per industry best practice in consultation with Customer to meet their Business requirements.

vi. MSI should provide the overall program management and OEM to ensure that the solution which may include multiple technologies from various OEM, to work together seamlessly as per the design goals. The seamless integration with all devices would be SI responsibility for the respective products offered.

vii. For Core, Due to large no of devices only 20% of the equipment to be deployed by OEM own the MSI as per OEM provided design shall deploy technical resources and rest including Access/Remote.

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

a) Software & licenses.

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

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

- Functional Requirement Specification (FRS)

- High level design of whole system
- Low Level design for whole system / Module design level
- System Requirements Specifications (SyRS)
- Any other explanatory notes about system
- Traceability matrix
- RACI Matrix
- Technical and product related manuals
- Installation guides
- User manuals
- System administrator manuals
- Toolkit guides and troubleshooting guides
- Other documents as prescribed by DSCL
- Quality assurance procedures
- Change management histories
- Version control data
- SOPs, procedures, policies, processes, etc. developed for DSCL
- Programs :

— Entire source codes as applicable
— All programs must have explanatory notes for understanding
— Version control mechanism
— All old versions to be maintained
— Test Environment :
— Detailed Test methodology document
— Module level testing
— Overall System Testing
— Acceptance test cases

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

3.5 Integration Phase

The Command and control Centre should be integrated with feeds of all tracks/component through OPC UA (OLE Platform Communication) deployed under this DSCL Project. MSI shall provide the testing strategy including traceability matrix, test cases and shall conduct the testing of various components of the software developed/customized and the solution as a whole. The testing should be comprehensive and should be done at each stage of development and implementation.to enable city for batter decision management and planning

3.6 Go-Live Preparedness and Go-Live

- MSI shall prepare and agree with DSCL, the detailed plan for Go-Live (in-line with DSCL's implementation plan as mentioned in RFP).
- MSI shall define and agree with DSCL, the criteria for Go-Live.
- MSI shall ensure that all the data migration is done from existing systems.
- MSI shall submit signed-off UAT report (issue closure report) ensuring all issues raised during UAT are being resolved prior to Go-Live.

- MSI shall ensure that Go –Live criteria as mentioned in User acceptance testing of Project is met and MSI needs to take approval from DSCL team on the same.
- Go-live of the application shall be done as per the finalized and agreed upon Go-Live plan.

3.7 Handholding and Training

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

a) MSI shall prepare and submit detailed Training Plan and Training Manuals to DSCL for review and approval.
b) Appropriate training shall be carried out as per the User Training Plan prepared in detail stating the number of training sessions to be held per batch of trainees, course work for the training program, coursework delivery methodologies and evaluation methodologies in detail.
c) MSI shall also be responsible for full capacity building. Training and capacity building shall be provided for all individual modules along with their respective integrations.
d) MSI shall be responsible for necessary demonstration environment setup including setup of cameras, Wi-Fi, sensors and application solutions to conduct end user training. End user training shall include all the equipment including but not limited to all the applications and infrastructure at CCC, DC, field locations etc. End user training shall be conducted at a centralized location or any other location as identified by DSCL with inputs from the MSI.
e) MSI shall conduct end user training and ensure that the training module holistically covers all the details around hardware and system applications expected to be used on a daily basis to run the system.
f) MSI shall impart operational and technical training to internal users on solutions being implemented to allow them to effectively and efficiently use the DICCC system.
g) MSI shall prepare the solution specific training manuals and submit the same to DSCL for review and approval. Training Manuals, operation procedures, visual help-kit etc. shall be provided in Hindi & English language.
h) MSI shall provide training to selected officers of the purchaser covering functional, technical aspects, usage and implementation of the products and solutions.
i) MSI shall ensure that all concerned personnel receive regular training sessions, from time to time, as and when required. Refresher training sessions shall be conducted on a regular basis.
j) An annual training calendar shall be clearly chalked out and shared with the DSCL along with complete details of content of training, target audience for each year etc.
k) MSI shall update training manuals, procedures manual, deployment/Installation guides etc. on a regular basis (Quarterly/ Biannual) to reflect the latest changes to the solutions implemented and new developments.
l) MSI shall ensure that training is a continuous process for the users. Basic intermediate and advanced application usage modules shall be identified by the MSI.
m) Systematic training shall be imparted to the designated trainees that shall help them to understand the concept of solution, the day-to-day operations of overall solution and

maintenance and updating of the system to some extent. This shall be done under complete guidance of the trainers provided by the MSI.

n) Time Schedule and detailed program shall be prepared in consultation with DSCL and respective authorized entity. In addition to the above, while designing the training courses and manuals, MSI shall take care to impart training on the key system components that are best suited for enabling the personnel to start working on the system in the shortest possible time.

o) MSI is required to deploy a Master Trainer who shall be responsible for planning, designing and conducting continuous training sessions.

p) The master trainers shall demonstrate a thorough knowledge of the material covered in the courses, familiarity with the training materials used in the courses, and the ability to effectively lead the staff in a classroom setting. If at any stage of training, the DSCL feels that on-field sessions are required, the same shall be conducted by the MSI.

q) If any trainer is considered unsuitable by DSCL, either before or during the training, MSI shall provide a suitable replacement without disrupting the training plan.

r) Training sessions and workshops shall comprise of presentations, demonstrations and hands-on mandatorily for the application modules.

s) DSCL shall be responsible for identifying and nominating users for the training. However, SI shall be responsible for facilitating and coordinating this entire process.

t) MSI has to ensure that training sessions are effective and the attendees shall be able to carry on with their work efficiently. For this purpose, it is necessary that effectiveness of the training session is measured through a comprehensive feedback mechanism. MSI shall be responsible for making the feedback available for the DSCL/authorized entity to review and track the progress, In case, after feedback, more than 40% of the respondents suggest that the training provided to them was unsatisfactory or less than satisfactory then the SI shall re-conduct the same training at no extra cost.

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

I. Functional Training

- ✓ Basic IT skills
- ✓ Web portal, Mobile App, Enterprise GIS, ITMS, Wi-Fi, environmental sensors, Data Analytics, ANPR, smart solutions etc.
- ✓ Software Applications (Command and Control Centre)
- ✓ Networking, Hardware Installation
- ✓ Centralized Helpdesk
- ✓ Feed monitoring

II. Administrative Training

- ✓ System Administration Helpdesk, BMS Administration etc.
- ✓ Master trainer assistance and handling helpdesk requests etc.

III. Senior Management Training

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

IV. Post-Implementation Training

- ✓ Refresher Trainings for senior officials
- ✓ Functional/Operational training and IT basics for new operators
- ✓ Refresher courses on System Administration
- ✓ Change Management programs

3.8 Operations and Maintenance

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

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

Regular auditing is an inspection or examination of infrastructure to evaluate or improve its appropriateness, safety and efficiency. Audits usually provide a report that points out weaknesses/ vulnerabilities and proposes remedial actions.

3.9 Applications Support and Maintenance

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

a. Compliance to SLA

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

b. Annual Technology Support

MSI shall be responsible for arranging for annual technology support for the OEM products to DSCL provided by respective OEMs during the entire O&M phase.

c. Application Software Maintenance

i. MSI shall provide unlimited support through onsite team/telephone/Fax/E-mail/Video Conferencing/installation visit as required.

ii. MSI shall address all the errors/bugs/gaps in the functionality in the solution implemented by the MSI (vis-à-vis the FRS, BRS and SRS signed off) at no additional cost during the O&M phase.

iii. All patches and upgrades from OEMs shall be implemented by the MSI ensuring customization done in the solution as per the DSCL's requirements are applied. Technical upgrade of the installation to the new version, as and when required, shall be done by the MSI. Any version upgrade of the software / tool / appliance by MSI to be done after taking prior

approval of DSCL and after submitting impact assessment of such upgrade.

iv. Any changes/upgrades to the software performed during the support phase shall subject to the comprehensive and integrated testing by the MSI to ensure that the changes implemented in the system meets the specified requirements and doesn't impact any other function of the system. Release management for application software will also require DSCL's approval. A detailed process in this regard will be finalized by MSI in consultation with DSCL.

v. Issue log for the errors and bugs identified in the solution and any change done in the solution shall be maintained by the MSI and periodically submitted to the DSCL.

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

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

d. Problem identification and Resolution

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

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

e. Change and Version Control

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

i. Detailed impact analysis.

ii. Change plan with Roll back plans.

iii. Appropriate communication on change required has taken place.

iv. Proper approvals have been received.

v. Schedules have been adjusted to minimize impact on the production environment

vi. All associated documentations are updated post stabilization of the change.

vii. Version control maintained for software changes.

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

f. Maintain configuration information

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

g. Training

MSI shall provide training to DSCL personnel whenever there is any change in the functionality. Training plan has to be mutually decided with DSCL.

h. Maintain System documentation

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

i. High level design of whole system

ii. Low Level design for whole system / Module design level

iii. System requirements Specifications (SRS)

iv. Any other explanatory notes about system

v. Traceability matrix

vi. Compilation environment

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

i. Source code is documented

ii. Functional specifications are documented

iii. Application documentation is updated to reflect on-going maintenance and

iv. enhancements including FRS and SRS, in accordance with the defined standards

v. User manuals and training manuals are updated to reflect on-going

vi. changes/enhancements

vii. Standard practices are adopted and followed in respect of version control and management.

i. All the project documents need to follow version control mechanism. MSI will be required to keep all project documentation updated and should ensure in case of any change, the project documents are updated and submitted to DSCL by the end of next quarter.

j. For application support MSI shall keep dedicated software support team to be based at MSI location that will single point of contact for resolution of all application related issues. This team will receive all the application related tickets/incidents and will resolve them. In its technical proposal MSI need to provide the proposed team structure of application support including number of team members proposed to be deployed along with roles and skills of each such member. Application support team shall be employees of MSI.

k. Any software changes required due to problems/bugs in the developed software/application will not be considered under change control. The MSI will have to modify the software/application free of cost. This may lead to enhancements/customizations and the same needs to be implemented by the MSI at no extra cost.

l. Any additional changes required would follow the Change Control Procedure. DSCL may engage an independent agency to validate the estimates submitted by the MSI. The inputs of such an agency would be taken as the final estimate for efforts required. MSI to

propose the cost of such changes in terms of man month rate basis and in terms of Function point/Work Breakdown Structure (WBS) basis in the proposal.

3.9.1 ICT Infrastructure Support and Maintenance

ICT infrastructure includes servers, storages, back up, networking, load balancers, security equipment, operating systems, database, enterprise management system, help desk system and other related ICT infra required for running and operating the envisaged system. MSI shall define, develop, implement and adhere to IT Service Management (ITSM) processes aligned to ITIL framework for all the IT Services defined and managed as part of this project.

3.9.2 Warranty support

a. MSI shall provide comprehensive and on-site warranty for 5 years from the date of Go-Live for the infrastructure deployed on the project. MSI need to have OEM support for these components and documentation in this regard need to be submitted to DSCL on annual basis.

b. MSI shall provide the comprehensive & onsite manufacturer's warranty in respect of proper design, quality and workmanship of all hardware, equipment, accessories etc. covered by the RFP. MSI must warrant all hardware, equipment, accessories, spare parts, software etc. procured and implemented as per this RFP against any manufacturing defects during the warranty period.

c. MSI shall provide the performance warranty in respect of performance of the installed hardware and software to meet the performance requirements and service levels in the RFP.

d. MSI is responsible for sizing and procuring the necessary hardware and software licenses as per the performance requirements provided in the RFP. During the warranty period MSI shall replace or augment or procure higher-level new equipment or additional licenses/hardware at no additional cost to the RSCL in case the procured hardware or software is not enough or is undersized to meet the service levels and the project requirements.

e. During the warranty period MSI shall maintain the systems and repair/replace at the installed site, at no charge to DSCL, all defective components that are brought to the MSI's notice.

f. The MSI shall carry out Preventive Maintenance (PM) of all hardware and testing for virus, if any, and should maintain proper records at each site for such PM. The PM should be carried out at least once in six months as per checklist and for components agreed with DSCL.

g. The MSI shall carry out Corrective Maintenance for maintenance/troubleshooting of supplied hardware/ software and support infrastructure problem including network (active/passive) equipment, security and rectification of the same. The MSI shall also maintain complete documentation of problems, isolation, cause and rectification procedures for building knowledge base for the known problems in centralized repository, accessible to DSCL team as well.

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

i. There should not be any restriction on no. of OEM Software support incidents.

j. OEM Shall have defined product roadmap for at least five years.

k. Software OEM shall be present in India and should have Support Center also in India.

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

i. MSI shall have to stock and provide adequate onsite and offsite spare parts and spare component to ensure that the uptime commitment as per SLA is met.

ii. Any component that is reported to be down on a given date should be either fully repaired or replaced by temporary substitute (of equivalent configuration) within the time frame indicated in the Service Level Agreement (SLA).

iii. The MSI shall introduce a comprehensive Assets Management process & appropriate tool to manage the entire lifecycle of every component of DICCC system.

3.9.3 Maintenance of ICT Infrastructure at the DC and DICCC

a. Management of DC and DICCC

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

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

i. DC operations to be in compliance with industry leading ITSM frameworks like ITIL

ii. ISO 20000 & ISO 27001

iii. Ensure compliance to relevant SLA’s

iv. 24x7 monitoring & management of availability & security of the infrastructure and assets

v. Perform regular hardening, patch management, testing and installation of software updates issued by OEM/vendors from time to time after following agreed process

vi. Ensure overall security – ensure installation and management of every security component at every layer including physical security

vii. Prepare documentation/policies required for certifications included in the scope of work

viii. Preventive maintenance plan for every quarter

ix. Performance tuning of system as required

x. Design and maintain Policies and Standard Operating Procedures

xi. User access management

xii. Other activities as defined/to meet the project objectives

xiii. Updating of all Documentation.

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

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

b. System Maintenance and Management

i. MSI shall be responsible for tasks including but not limited to setting up servers, configuring and apportioning storage space, account management, performing periodic backup of data and automating reporting tasks, and executing hardware and software updates when necessary. It shall be noted that the activities performed by the MSI may also be reviewed by DSCL.

ii. MSI shall provision skilled and experienced manpower resources to administer and manage the entire system at the Data Center.

iii. On an ongoing basis, MSI shall be responsible for troubleshooting issues in the IT infrastructure solution to determine the areas where fixes are required and ensuring resolution of the same.

iv. MSI shall be responsible for identification, diagnosis and resolution of problem areas pertaining to the IT Infrastructure and maintaining the defined SLA levels.

v. MSI shall implement and maintain standard operating procedures for the maintenance of the IT infrastructure based on the policies formulated in discussion with DSCL and based on the industry best practices/frameworks. MSI shall also create and maintain adequate documentation/checklists for the same.

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

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

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

c. System Administration

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

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

iii. MSI shall be responsible for operating system administration, including but not limited

to management of users, processes, preventive maintenance and management of upgrades including updates, upgrades and patches to ensure that the system is properly updated.

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

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

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

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

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

ix. The system administrators shall provide hardening of servers in line with the defined security policies. Validation of hardening configuration will be carried out quarterly and deviations must be tracked through SLA reporting.

x. The system administrators shall provide integration and user support on all supported servers, data storage systems etc.

xi. The system administrators shall be required to trouble shoot problems with web services, application software, server relationship issues and overall aspects of a server environment like managing and monitoring server configuration, performance and activity of all servers.

xii. The system administrators should be responsible for documentation regarding configuration of all servers, IT Infrastructure etc.

xiii. The system administrators shall be responsible for managing the trouble tickets, diagnosis of the problems, reporting, managing escalation, and ensuring rectification of server problems as prescribed in Service Level Agreement.

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

d. Storage Administration

i. Compute and Storage: At least 150 Virtual machine has to be factored in DC and 75 virtual machine in DR (on Cloud). Total Storage would be 3.5 PB at least with 600TB on primary storage.

ii. MSI shall be responsible for the management of the storage solution including, but not limited to, storage management policy, configuration and management of disk array, Storage fabric/switches, tape library, etc. It should be noted that the activities performed by the MSI may be reviewed by DSCL.

iii. MSI shall be responsible for storage management, including but not limited to

management of space, SAN/NAS volumes, RAID configuration, LUN, zone, security, business continuity volumes, performance, etc.

iv. The storage administrator will be required to identify parameters including but not limited to key resources in the storage solution, interconnects between key resources in the storage solution, health of key resources, connectivity and access rights to storage volumes and the zones being enforced in the storage solution.

v. The storage administrator will be required to create/delete, enable/disable zones in the storage solution.

vi. The storage administrator will be required to create/delete/modify storage volumes in the storage solution.

vii. The storage administrator will be required to create/delete, enable/disable connectivity and access rights to storage volumes in the storage solution.

viii. To facilitate scalability of solution wherever required.

ix. The administrators will also be required to have experience in technologies such as virtualization and cloud computing so as to provision the existing and applicable infrastructure on a requirement based scenario.

e. Database Administration

i. MSI shall be responsible for monitoring database activity and performance, changing the database logical structure to embody the requirements of new and changed programs.

ii. MSI shall be responsible to perform physical administrative functions such as reorganizing the database to improve performance.

iii. MSI shall be responsible for tuning of the database, ensuring the integrity of the data and configuring the data dictionary.

iv. MSI will follow guidelines issued by DSCL in this regard from time to time including access of data base by system administrators and guidelines relating to security of data base.

v. Database administration should follow the principle of segregation of duties to ensure no single DBA can update production tables/data singularly.

vi. In addition to restrictions on any direct change in Data by any administrator, the Databases shall have Auditing features enabled to capture all activities of administrators.

f. Backup/Restore/Archival

i. MSI shall be responsible for implementation of backup & archival policies as finalized with DSCL. The MSI is responsible for getting acquainted with the storage policies of DSCL before installation and configuration. It should be noted that the activities performed by the MSI may be reviewed by DSCL.

ii. MSI shall be responsible for monitoring and enhancing the performance of scheduled backups, scheduled regular testing of backups and ensuring adherence to related retention policies.

iii. MSI shall be responsible for prompt execution of on-demand backups of volumes and files whenever required by DSCL or in case of upgrades and configuration changes to the system.

iv. MSI shall be responsible for real-time monitoring, log maintenance and reporting of backup status on a regular basis. MSI shall appoint administrators to ensure prompt problem resolution in case of failures in the backup processes.

v. MSI shall undertake media management tasks, including, but not limited to, tagging, cross-referencing, storing, logging, testing, and vaulting in fire proof cabinets (onsite and offsite as per the detailed process finalized by during project implementation phase).

vi. MSI shall also provide a 24 x 7 support for file and volume restoration requests at the Data Centre(s).

g. Network monitoring

i. MSI shall provide services for management of network environment to maintain performance at optimum levels on a 24 x 7 basis. It should be noted that the activities performed by the MSI may be reviewed by DSCL.

ii. MSI shall be responsible for creating and modifying VLAN, assignment of ports to appropriate applications and segmentation of traffic.

iii. MSI shall also be responsible for break fix maintenance of the LAN cabling within DC/DICCC etc.

iv. MSI shall also provide network related support and will coordinate with connectivity service providers of DSCL/other agencies who are terminating their network at the DC/DICCC for access of system.

h. Security Management

i. Regular hardening and patch management of components of the DICCC System as agreed with DSCL

ii. Performing security services on the components that are part of the DSCL environment as per security policy finalized with DSCL

iii. IT Security Administration – Manage and monitor safety of information/data

iv. Reporting security incidents and resolution of the same

v. Proactively monitor, manage, maintain & administer all security devices and update engine, signatures, and patterns as applicable.

vi. Managing and monitoring of anti-virus, anti-malware, phishing and malware for managed resources.

vii. Ensuring 100 percent antivirus coverage with patterns not old more than period agreed on any given system.

viii. Reporting security incidents and co-ordinate resolution.

ix. Monitoring centralized pattern distribution (live update) and scan for deficiencies.

x. Maintaining secure domain policies.

xi. Secured IPsec/SSL/TLS based virtual private network (VPN) management.

xii. Performing firewall management and review of policies on at-least quarterly basis during first year of O&M and then after at-least on half-yearly basis.

xiii. Resolution of calls for security notifications, system alerts, vulnerabilities in hardware/

software and alerting DSCL as appropriate.

xiv. Performing patch management using software distribution tool for all security applications including content management system, antivirus and VPN.

xv. Providing root cause analysis for all defined problems including hacking attempts.

xvi. Monthly reporting on security breaches and attempts plus the action taken to thwart the same and providing the same to DSCL.

xvii. Maintaining documentation of security component details including architecture diagram, policies and configurations.

xviii. Performing periodic review of security configurations for inconsistencies and redundancies against security policy.

xix. Performing periodic review of security policy and suggest improvements.

xx. Reviewing logs daily of significance such as abnormal traffic, unauthorized penetration attempts, any sign of potential vulnerability. Security alerts and responses. Proactive measures in the event a problem is detected.

xxi. Policy management (firewall users, rules, hosts, access controls, daily adaptations).

xxii. Modifying security policy, routing table and protocols.

xxiii. Performing zone management (DMZ).

xxiv. Sensitizing users to security issues through regular updates or alerts – periodic updates/ Help DSCL issuance of mailers in this regard.

xxv. Performing capacity management of security resources to meet business needs.

xxvi. Rapidly resolving every incident/problem within mutually agreed timelines.

xxvii. Testing and implementation of patches and upgrades.

xxviii. Network/device hardening procedure as per security guidelines from DSCL.

xxix. Implementing and maintaining security rules.

xxx. Performing any other day-to-day administration and support activities.

Other Activities

i. MSI shall ensure that it prepares configuration manual for OS, appliances, middleware, all tool, servers/devices and all equipment's and the same need to be submitted to DSCL, any changes in the configuration manual need to be approved by DSCL. Configuration manual to be updated periodically.

ii. MSI shall maintain data regarding entitlement for software upgrades, enhancements, refreshes, replacements and maintenance.

iii. If the Operating System or additional copies of Operating System are required to be installed/reinstalled/un-installed, the same should be done as part of O&M.

iv. MSI should carry out any requisite adjustments/changes in the configuration for implementing different versions of Application Software.

v. Updates/Upgrades/New releases/new versions: The MSI shall provide from time to time the Updates/Upgrades/new releases/new versions of the software and operating systems

as required. The MSI should provide free upgrades, updates & patches of the software and tools to DSCL as and when released by OEM.

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

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

viii. Data backup/recovery management services.

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

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

3.9.4 Compliance to SLA

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

ii. MSI shall be responsible for measurement of the SLAs at the DICCC System level as well as at the user level with the help of the enterprise monitoring tool on a periodic basis.

iii. Reports for SLA measurement must be produced DSCL officials as per the project requirements.

3.10 Compliance to Standards & Certifications

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

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

Sl. No.	Component/Application/System	Prescribed Standard
1.	Information Security	ISO 27001
2.	IT Infrastructure Management	ITIL specifications
3.	Service Management	ISO 20000 specifications
4.	Project Documentation	IEEE/ISO/CMMi (where applicable) specifications for documentation

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

- The Information Technology Act, 2000” and amendments thereof and

- Guidelines and advisories for information security published by Cert-In/MeitY (Government of India) issued till the date of publishing of tender notice. Periodic changes in these guidelines during project duration need to be complied with.

d. While writing the source code for application modules MSI should ensure high-quality documentation standards to improve the readability of the software module. An illustrative list of comments that each module contained within the source file should be preceded by is outlined below:

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

e. Apart from the above MSI needs to follow appropriate coding standards and guidelines inclusive of but not limited to the following while writing the source code.

- Proper and consistent indentation
- Inline comments
- Structured programming
- Meaningful variable names
- Appropriate spacing
- Declaration of variable names
- Meaningful error messages

f. Server Operating System shall be EAL4+ certified

g. The MeitY Policy must be adhered by the bidder.

h. No Freeware shall be proposed by bidder.

i. The bidder should not propose any limited use products/bundle. The authority shall be able to use the respective products for various applications as may be required.

j. Quality Audits

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

various sections in this RFP document.

3.11 Testing and Acceptance Criteria

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

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

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

Type of Testing	Responsibility	Scope of Work
		▪ DSCL if required, could involve third party auditors to monitor/validate the performance testing. Cost for such audits to be paid by DSCL
Security Testing (including Penetration and Vulnerability testing)	✓ MSI ✓ DSCL / Third Party Auditor (to monitor the security testing)	▪ Solution should demonstrate the compliance with security requirements as mentioned in the RFP including but not limited to security controls in the application, at the network layer, network, data center (s), security monitoring system deployed by MSI ▪ Solution shall pass vulnerability and penetration testing for rollout of each phase. The solution should pass web application security testing for the portal, mobile app and other systems and security configuration review of the infrastructure. ▪ MSI should carry out security and vulnerability testing on the developed solution. ▪ Security testing to be carried out in the exact same environment/architecture that would be set up for production. ▪ Security test report and test cases should be shared with DSCL ▪ Testing tools if required, to be provided by MSI. ▪ During O&M phase, penetration testing to be conducted on yearly basis and vulnerability assessment to be conducted on half-yearly basis. ▪ DSCL will also involve third party auditors to perform the audit/review/monitor the security testing carried out by MSI. Cost for such auditors to be paid by DSCL
User Acceptance Testing of Project	✓ DSCL or DSCL appointed third party auditor	▪ DSCL / DSCL appointed third party auditor to perform User Acceptance Testing ▪ MSI to prepare User Acceptance Testing test cases ▪ UAT to be carried out in the exact same environment/architecture that would be set up for production ▪ MSI should fix bugs and issues raised during UAT and get approval on the fixes from DSCL /third party auditor before production deployment ▪ Changes in the application as an outcome of UAT shall not be considered as Change Request. MSI has to rectify the observations.

Note:

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

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

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

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

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

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

3.12 Factory Testing

Success MSI shall have to submit Factory Test Certificate for the below mentioned materials before the actual supply of the items.MSI has to provide MAF (OEM certificate) where applicable.

3.13 Final Acceptance Testing

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

Prerequisite for Carrying out FAT activity:

1. Detailed test plan shall be developed by MSI and approved by DSCL. This shall be submitted by MSI before FAT activity to be carried out.

2. All documentation related to DSCL Project and relevant acceptance test document (including IT Components, Non IT Components etc.) should be completed & submitted before the final acceptance test to the DSCL.

3. The training requirements as mentioned should be completed before the final acceptance test.

4. Successful hosting of Application, NMS and MIS Software.

5. For both IT & Non-IT equipment's/software manuals/brochures/Data Sheets/CD/ DVD/media for all the DSCL Project supplied components.

The FAT shall include the following:

1. All hardware and software items must be installed at respective sites as per the specification.

2. Availability of all the defined services shall be verified.

3. MSI shall be required to demonstrate all the features/facilities/functionalities as mentioned in the RFP.

4. MSI shall arrange the test equipment required for performance verification, and will also provide documented test results.

5. MSI shall be responsible for the security audit of the established system to be carried out by a certified third party as agreed by DSCL.

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

4 Detailed Scope of Work

4.1 Doon Integrated Command and Control Centre

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

- Doon Integrated Command and Control Center (DICCC)
- Intelligent Traffic Management System (ITMS) Solution.
- ATCS
- Traffic Enforcement
- Public Address System and Emergency Call Box
- Transit Management System (VTMS)
- City surveillance with AI
- Environmental Sensors.
- Solid Waste Management.
- City Wi-Fi.
- Variable Message Sign Board.
- Datacenter Solutions and security.
- Web Portal and Mobile Applications
- Citizen Centric Services
- Emergency Help Desk and Contact Center
- Video Conferencing solution
- Enterprise GIS
- ICT Infrastructure – Data Center and Disaster Recovery Center.

The solution should provide option to integrate existing deployed solution by City and also need to provide scalability option to implement new use cases.

4.2 DICCC SOFTWARE compliance

DICCC Operations

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

1) Solution should have the capability to integrate with GIS
2) Solution shall integrate with GIS and map information and be able to dynamically
3) Update information on the GIS maps to show status of resources.
4) Solution should allow defining key performance indicators and visualize the
5) indicators on a configurable dashboard infrastructure
6) Solution should allow configuration and monitoring of service levels for key performance indicators and triggering of actions towards the incident management system when those service levels are breached.
7) Solution should provide current business status (snapshot) of City's facilities, departments and a holistic perspective of incidents and situations. Including incident handling time, number of false alerts, number of active and closed incident.
8) Solution should provide operators and managers with a management dashboard that provides a real-time status and is automatically updated when certain actions, incidents and resources have been assigned, pending, acknowledged, dispatched, implemented, and completed. The above attributes shall be colour coded.
9) Solution shall provide the "day to day operation", "Common Operating Picture" and situational awareness to the Centre and participating agencies during these modes of operation.
10) Shall provide complete view of sensors, facilities, e-governance/ERP, video streams and alarms in an easy-to-use and intuitive GIS-enabled graphical interface with a powerful workflow and business logic engine.
11) Shall provide a uniform, coherent, user-friendly and standardized interface.
12) Shall provide possibility to connect to workstations and visualization layer shall be accessible.
13) Dashboard content and layout shall be configurable, and information displayed on these dashboards shall be filtered by the role of the person viewing dashboard.
14) Solution should allow creation of hierarchy of incidents and be able to present the same in the form of a tree structure for analysis purposes.
15) Shall be possible to combine the different views onto a single screen or a multi-monitor workstation.
16) Solution should maintain a comprehensive and easy to understand audit trail of read and write actions performed on the system.
17) Solution should provide ability to extract data in desired formats for publishing and interfacing purposes.
18) Solution should provide ability to attach documents and other artefacts to incidents and other entities.

Integration capabilities

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

Notifications, Alerts and Alarms

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

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

2) Systems should deliver message to a set of subscribers. The Notification service should support min two types of notification methods – Email notification and Short Messaging Service (SMS) notification.

Users and roles

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

1) Platform should allow different roles to be created and assign those roles to different access control policies.

2) Platform should allow single or multiple users to view and manage alarms in defined areas/Locations. User can be part of Single or multiple Areas/Locations.

Reports

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

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

1) Incident Reports

I. Detailed incident reports shall include an incident summary, all the tasks associated with the incident, sensor related activities, relevant snapshots, and maps.
II. Periodic Reports
III. Maintenance Reports
IV. Statistical Reports

2) Ability to display report on monitor and print report.

3) Ability to capture Operators response in Text.

4) Ability to select information to be included in report at time of report generation.

5) Details of alarm including severity, time / date, description, and location.

6) Capture the operator response by text.

7) Allow operator to transfer the incident report to Mobile Device/another operator's Console.

Standard Operating Procedure

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

1) Software shall provide SOP's in text, pdf, image, word formats.

2) SOP tasks should serve as an instructional resource that allows operator to act without asking for guidance.

3) There shall be the provision to define various SOPs in Command and Control System such as alert category specific SOPs, Location Specific SOPs.

4) It shall have facility to define more than one SOP for the selected alert category or location

5) There shall be a provision to define multiple tasks under single SOP.

6) The system shall select & present the appropriate SOP automatically based on predefined policies.

7) Actions taken as part of SOP should be logged in audit trail with date time stamp and operator comments.

8) SOP shall contain the lists of tasks to be performed by operator categorized under following headings.

Task: Task to be performed by the operator in the sequential order.

Description: Task description.

Comments: Space for operator to enter the comments.

Action: Actions (like email, sms escalation) to be initiated by operator.

Done: Indication by operator that the task is completed.

User: User name of the operator for audit trail.

Date & Time: date time of the action.

Field Responder Mobile

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

1) Operator Client License min 25 with one city activation license

2) Field Responder should be able to acknowledge the incident and provide real time updates from the incident site.

3) Field Responder should be able to view the recorded stream and image of the event

4) Field Responder should be able to view live stream of the camera

5) Field Responder should be able to send ATR or action taken for the event to the command and Control application

Enterprise Service Bus:

There should be no point to point integration in the architecture. There should be a separate enterprise service bus layer for integration.

The enterprise service bus layer should be loosely coupled with any other component in the architecture.

Enterprise service bus layer should be independently scalable, modular and replaceable. It should follow scale-out architecture to handle spikes in traffic.

Enterprise service bus could be deployed on choice of environments - Bare Metal, VMs, containers, public and private cloud.

ESB layer should have out of the box support OSGi bundles.

Integration software should include out-of-the box support for Enterprise Integration Patterns and Standard Connectors without additional cost.

Integration platform should include Message Queue capability.

Should support leading industry standard protocol for interoperable reliable messaging with AMQP 1.0 and MQTT.

Integration platform should include native management console to manage ESB & Message Queue.

OEM Should have support center in India.

The OEM Software support of ESB Solution shall not restrict the number of support cases/incidents for both production and development.

The bidder shall also propose self-paced OEM online learning module for proposed ESB for at least three users for a period of one year.

API Management Platform:

The bidder shall propose a proper enterprise API Management Solution and it should not be an integrated/bundled software with any business application or CCC/DICCC Platform, it should be deployed as an independent platform.

The OEM Software support of API Management shall not restrict the number of support cases/incidents.

The API Management Solution should not restrict number of Gateways integration with the Manager.

API management solution and API gateway should provide open standards based API Management, by providing full API lifecycle management with governance and security and monitoring mechanism for the available APIs.

Bidder should Implement an API Management platform that provides Modelling, designing policies that govern API externalization (consumption) and capabilities to monitor its usage,

report with analytic, secures and governs the access to APIs and provides portal interface to facilitate partner/developer on boarding.

OEM of API Management Solution shall have presence in India and shall have its own India Support center as well.

The platform should have API Management capabilities like API Security, API Monetization for the Smart City.

API Monetization: Integration with popular payment gateways, as well as all the tools you need to define paid plans by bundling data access, rate limits, and call volume settings.

Provide documentation, example code, and other information to help API users build successfully.

Analytics: Easily see which developers and applications are most popular with built-in analytics.

API traffic control in the data flow: Protect the backend API servers with strict traffic control on incoming and outgoing traffic.

APIs Access Control & API Security.

Dashboard: The Dashboard, part of the Admin Portal, should give quick, centrally located visibility into any traffic.

API manager shall provide rate limiting, analytics capabilities along with access control mechanisms. It shall also provide developer portal for documentation of available apis, use cases, tutorials and testing of APIs.

API gateways shall work in disconnected mode (during unavailability of manager portal). API gateways shall provide instances auto scaling - scale up, scale down, auto start, auto stop basis on traffic.

Enterprise OEM System Software Requirements:

While finalizing the solution architecture for the requirement, policy of Government of India on adoption of open source software issued by DeitY vide F. No. 1(3)/2014-EG II must be adhered.

As Security shall be an important aspect, Server Operating System for all servers shall be Common Criteria EAL4+ certified.

The bidder shall be responsible for arranging annual technology support for the OEM products provided by respective OEMs during the entire O&M phase. The bidder shall provide the OEM MAF for the enterprise system software as listed below it is mandatory for the bidder to take enterprise level annual support over the entire contract duration at minimum for the software(s) mentioned below:

- Operating System
- Virtualization layers
- RDBMS
- Integration Layer
- Message Queue Layer

- Application server
- API Management Framework
- Mobile Application Framework
- All other OEM Enterprise Software products

The bidder shall provide full-use versions of the various OEM System Software which shall not be restricted for specific application use only. The client shall be able to use the proposed OEM software components for various other applications also.

Bidder shall provide ATS/AMC for the Software/solutions provided by the respective OEMs for the period specified in the RFP. The ATS/AMC should include upgrades, updates and patches to the respective Software solution for the above stated period.

All the licenses/subscription and support (updates, patches, bug fixes, etc.), if applicable, should be in the name of the client department.

The bidder shall note that free software or software which is not supported by the respective OEM shall not be accepted.

The system software proposed should be from an OEM with presence in India and the OEM shall have India Support Centre.

The Bidder shall propose an OEM Provided Training Modules in Self-paced Online Learning Mode for system software like Operating System, Virtualization Software, Application Server, ESB etc. for at least 5 users.

The OEM Software support shall not restrict the number of support cases/incidents.

The Software OEM shall have defined product life cycle and update policies.

The OEM Software license/subscription shall allow the software to be deployed on physical, virtual or cloud based servers.

The bidder shall propose full use license/subscription of various industry leading middleware software i.e. Integration Server, API management, Application Server, RDBMS etc. instead of using any restrictive bundle as part of any Platform. The proposed Platform shall support multiple choices for the middleware software instead of any vendor lock-in. The Authority shall be able to use these OEM Middleware software i.e. ESB, API Management, RDBMS, Application server even if it decides to change or discard the platform/bundle also at a later date.

The proposed Linux Operating system should support multiple architectures, including x86_64, IBM power 8 and 9, IBM z Systems, and 64-bit ARM.

The proposed Linux operating system shall be supported on various leading cloud platforms including AWS, Microsoft Azure, and Google Cloud Platform.

The proposed Linux operating system shall support security standards i.e. Common Criteria and FIPS 140-2 certifications—including the Linux Containers Framework Support to be Common Criteria-certified, NIST-certified scanner (Open SCAP).

The bidder shall provide Proper OEM Support for the proposed Linux Operating system and must not provide freeware OS, either stand-alone or bundled as part of any solution.

The DR Cloud Service Provider shall also provide MAF from the OEMs ensuring that enterprise supported software is provisioned on DR cloud.

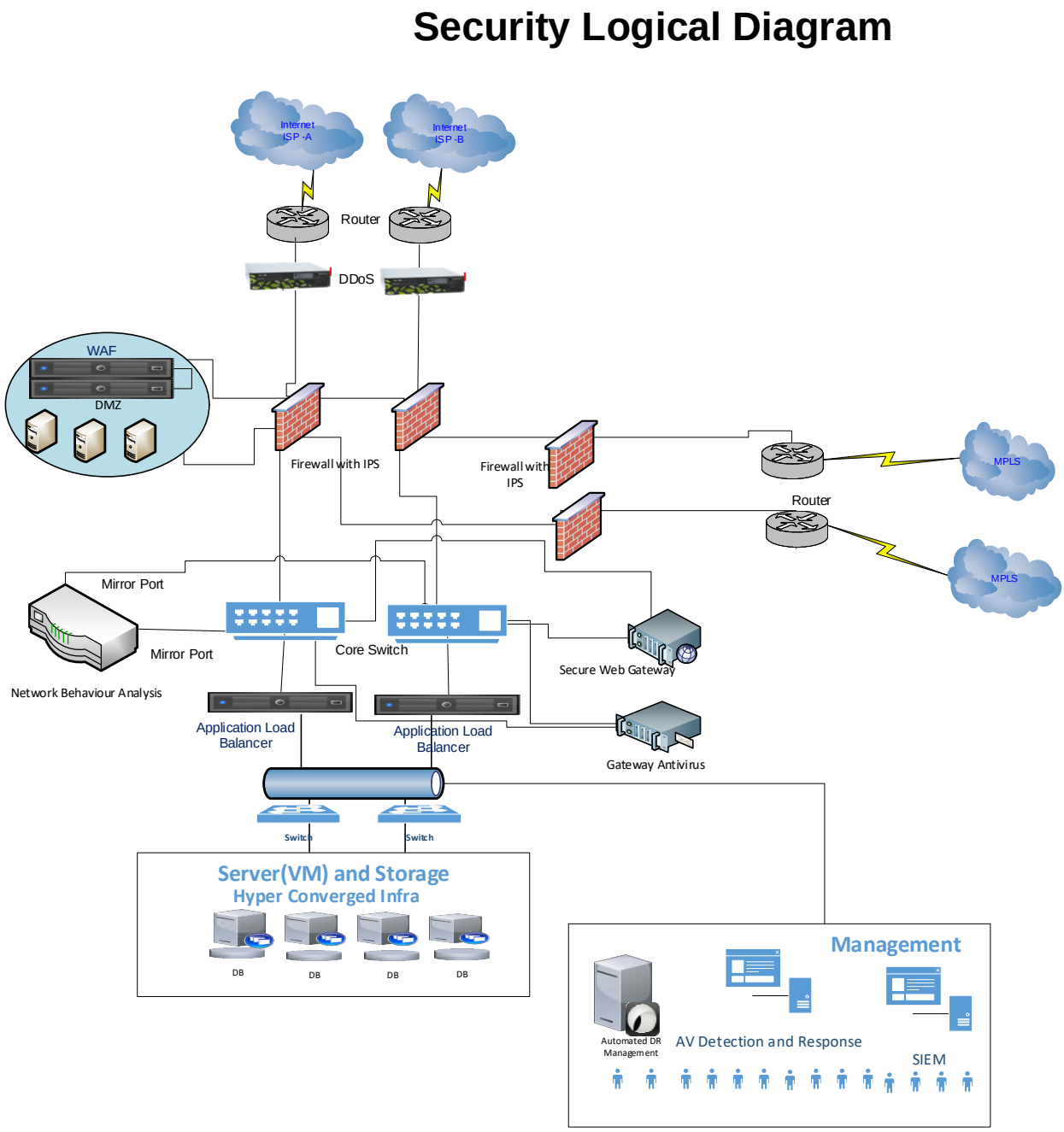
The DR Cloud Service Provider shall produce certificate for the formal cloud services agreement with the respective OEMs.

4.3 Data Centre and Disaster recovery centre

Data Centre and Disaster Recovery Centre

- The DR for the data centre shall be on cloud on empanelled service providers by MeiTY. The cloud provider should be MEITY empanelled as well as STQC certified Govt. community cloud (GCC).
- Various ICT equipment to be provisioned and maintained by MSI at the Data Centre is given below.
- The DR should be replicated for 30 days. The backup storage should be active-active.
- All equipment in DC should be in HA.
- DR should be on cloud as a service and 99.5 % uptime.

4.4 High Level Indicative Architecture (Tentative)



DC Components Specifications:

4.5 Internet Router

1 The router should be modular in architecture with minimum 3 slots and should be a single chassis solution, should support redundant Router processors/Routing engines and Redundant Power supply. All modules, fan trays & Power supplies should be hot swappable.

2 Router should have minimum 35 Gbps throughput from day 1 with minimum 50 Mpps with services on IPv4 and IPv6. Route Processors should have minimum 4GB of flash memory, 4GB of RAM/DRAM.

3 Minimum 6 x Gigabit Ethernet routing ports with copper transceivers and 4x Gigabit Ethernet Ports (Supporting long haul and short haul SFP). Should support wide variety of interfaces including 10G, OC3, OC48, DS3 WAN interfaces, should support 4 x 10G ports.

4 Features: QoS classification, policing and shaping, NAPT64, CGNAT, ACL, Router should support hardware encryption capabilities.

5 Should support 250K IPv4 and 250k IPv6 Routes, 100k MAC addresses, 1000 VRFs and should have 32K Multicast route.

6 Protocols: Should support RIPv2, OSPF, IS-1S and BGP4, LDP, BFP routing protocols & IP multicast routing protocols: PIM, IGMP, MPLS, PWE3, FRR, VPLS, NAT, PAT, RADIUS, TACACS+,

7 Security Features: should support IPv6 for IPSec encryption for data confidentiality, 3DES and AES encryption standards.

8 Management: SNMP V1 and V2, Telnet, TFTP.

9 Certification: EAL3/ NDPP or above Certified.

4.6 DC and Internet Firewall

1 The Firewall appliance should be a purpose built appliance based solution with integrated functions like Firewall, VPN and User awareness. The product licensing should be device based and not user/IP based (should support unlimited users except for VPN). The hardware platform & Firewall with integrated SSL/IPSec VPN application has to be from the same OEM. The quoted NGFW OEM must have NSS Lab's recommended rating as per latest NSS Labs NGFW Methodology testing with a minimum exploit blocking rate of 95%.

2 Throughput capacity of firewall under test conditions should not be less than 70Gbps. Throughput capacity of VPN under test conditions should not be less than 15 Gbps. Appliance should support Max 25,000,000 concurrent sessions. Appliance should support at least 1,80,000 connections per second. Solution should be based on multi core processors and not on proprietary hardware platforms like ASICs, Should have minimum 16 GB memory with option of upgradable atleast 32 GB. Hardware should have field upgradable capabilities for upgrading components like network cards, RAM, power supplies, fan etc. Solution should be field upgradable as architecture.

3 Solution should have following deployment modes mandatory: a) L3 Mode, b) L2/Transparent Mode. The solution should be deployed in High Availability. Should support

hardware fail open cards for critical interfaces. NGFW appliance should have inbuilt storage of 1 Tb SSD / HDD.

4 Interface Requirement: 8 x 10/100/1000Base-T Copper Ports, 4 x 10 GB 10G SFP ports from day 1 and support for addition of 2 x 40G SFP ports. Dedicated Management and Sync Ports

5 Firewall Feature: solution should be based on “stateful inspection” technology and must support access control for at least 500 predefined /services/protocols with capability to define custom services. Must allow security rules to be enforced within time intervals to be configured with an expiry date/time. The communication between the management servers and the security gateways must be encrypted and authenticated with PKI Certificates.

6 Authentication: schemes must be supported by the security gateway and VPN module: tokens (i.e. –Secure ID), TACACS, RADIUS and digital certificates. Should support Ethernet Bonding functionality for Full Mesh deployment architecture. Must support user, client and session authentication methods. User authentication schemes must be supported by the security gateway and VPN module: tokens (i.e. –Secure ID), TACACS, RADIUS and digital certificates. Firewall should support the system authentication with RADIUS and local authentication. Both should work simultaneously. Solution must support DCHP, server and relay. Solution must include the ability to work in Transparent/Bridge mode.

7 Solution must support gateway high availability and load sharing with state synchronization. Solution must support Configuration of dual stack gateway on a bond interface, OR on a sub-interface of a bond interface. Solution must Support 6 to 4 NAT, or 6 to 4 tunnel.

8 User Identity / Awareness: Must be able to acquire user identity from Microsoft Active Directory without any type of agent installed on the domain controllers. Must support Kerberos transparent authentication for single sign on. Must support the use of LDAP nested groups. Must be able to create rules and policies based on identity roles to be used across all security applications. The solution should have the inherent ability to detect multi-stage attacks. For the purpose of detecting multi stage attacks the solution should include static analysis technologies like antivirus, anti-malware/anti bot however in an integrate mode with the solution. The bidder or SI may use additional appliances (at max 2) for the solution but should be provided by the same OEM in the solution.

9 The solution should inspect the web sessions (HTTP and HTTPS both) to detect and notify the malicious web activity including malicious file downloads through the internet. Third Party/Separate appliance for SSL offloading will not be accepted. The proposed solution should dynamically generate real-time malware intelligence for immediate local protection via integration with the separate Automated Management and Event Correlation System. This Automated Management and Event Correlation solution must be from the same OEM. Solution should have an ability to remove all the active content and macros sending only a clean document to the end user. Solution should be able to detect & Prevent the Bot communication with C&C.

10 Solution should have a Multi-tier engine to i.e. detect & Prevent Command and Control IP/URL and DNS. Solution should be able to detect & Prevent Unique communication patterns used by BOTs i.e. Information about Botnet family. Solution should be able to detect & Prevent attack types i.e., such as spam sending click fraud or self-distribution that are associated with

Bots. Solution should be able to block traffic between infected Host and Remote Operator and not to legitimate destination. Solution should be able to provide with Forensic tools which give details like Infected Users/Device, Malware type, Malware action etc.

11 Security Management: A separate centralized management appliance/software needs to be provided for management and logging of NGFW appliance. In case other security components like APT solution etc. are from the same OEM then a single centralized management, logging (and not multiple management system) should manage all such security devices. Security management Hardware can be an OEM appliance or dedicated server with software. In case of dedicated server, Server should be rack mounted with Intel based 8 core processor with min two nos. of 64-bit processor having 64 GB RAM or OEM recommended whichever is higher for these specifications. Minimum 2 TB Hard disk and minimum dual 10/100/1000 Mbps network port. The central management console and should be able to handle 5000 log/sec.

12 Security management application must support role based administrator accounts. Management must provide functionality to automatically save current state of Policy each time when any configuration changes in Security policy is enforced, and should have option to revert back to previous state stored state. It must be capable of storing at least last 5 policies. Management Solution must include a Certificate-based encrypted secure communications channel among all vendor distributed components belonging to a single management domain. The management must provide a security rule hit counter in the security policy. Solution must include a search option to be able to easily query which network object contain a specific IP or part of it. Solution must have a security policy verification mechanism prior to policy installation.

13 The Log Viewer should have the ability view all of the security logs of all functions managed by the solution in one view pane (helpful when troubleshooting connectivity problem for one IP address).

14 The Log Viewer should have the ability in the log viewer to create filter using the predefined objects (hosts, network, groups, users...)

4.6.1 Core Router

1 The Core Router should be chassis based, Should have redundant processor and redundant power supply. All the Interfaces should be provided in line cards and no interface should be on CPU card. All interface should have wire speed performance. The back-plane capacity of Router should be minimum 700Gbps & forwarding performance of 1000 Mpps packets per sec of 64 bytes packet. The performance is considered with IPv4 & IPv6.

2 Interface Requirement: 16 X 1 Gig Base SFP interface and 4 X 10Gig interface (The optics should be populated from day one) and Chassis should have at least 3 free main slot (not daughter slots) to scale in future to support additional 8 X 10Gig interface or 60 X 1 Gig interface, should be capable to support minimum 4 X 100Gig interface in future.

3 The Router should have High Availability Features: Non Stop Routing, Graceful Restart, In Service Software Upgrade, 802.1ag, MC-LAG, BFD for IPv4 and IPv6, VRRP.

4 Protocol: DHCP, IP Multicast, PIM SM, PIM SSM, IGMP, MLD, RP, Next generation Multicast using MPLS LSP, IS-IS, HQOS, LDP, MPLS, MPLS FRR, L2 VPN, L3 VPN, VPLS,

Diff Serv TE, RIP V 2, OSPF, BGP, NAT, should support three level HQOS with minimum 32K queues.

5 Router should have IPv4, IPv6 and QoS Classification. Should have 3M IPv4 and 2M IPv6 routing entries per system. Should have support for 15 logical router.

6 Network Management: SNMP v2 and upgradable to SNMP V3, Console management access, NTP or SNTP.

7 Certification: Router should be NEBS certified and EAL 3/NDPP certified under Common Criteria.

4.6.2 Core Switch

1 The Core Switch should be Modular (Distributed Architecture with 100% passive backplane/midplane) with aggregate capacity of at least 4 Tbps. Should have at least 6 payload slots with 32 x 10/100/1000 BaseT RJ 45 and 32 SFP+ Ports. The per slot bandwidth should be at least 240 Gbps. All Interface Module should have local processing.

2 Redundancy: should have redundant switch Fabrics to support bandwidth for future Highly Scalable Ethernet Standards from Day 1. Should have Redundant CPU and redundant power supply from day 1.

3 Interface support: 40G and 100G from Day 1, Support atleast 160 Nos of 10 Gigabit Ethernet or 240 Gigabit Ethernet ports.

4 HA Features: All the main components like CPU module, switching fabric, power supplies and fans etc should be in redundant configuration. Components, like modules/power supplies/fan tray should be Hot Swappable. The switch should have redundant Switch Fabric's working in an active-active load sharing mode, Support for Hot Swap of all redundant components: Line Cards, Fabric, power supply, and fan trays.

5 Should have 4 GB DRAM and 250,000 Nos. of MAC addresses and 4K VLAN, minimum 500,000 Route entries for IPv4 and IPv6, Should support 100,000 IPv4/IPv6 multicast routes.

6 Protocols: IEEE 802.1w RSTP and IEEE 802.1s MSTP, RIP V1/v2, OSPF v1/v2, BGPv4, IS-IS, IPv6 packet switching. VRRP, Should support MPLS, GRE tunnelling, IP Multicast PIM - SSM, MSDP, IGMP v1, v2, v3, IGMP Snooping, H/W based IPv4 and IPv6 Multicasting.

7 Security Features: ACL, DHCP replay, Dynamic Arp, MAC address based filtering, RADIUS, TACACS+.

8 Monitoring: Should Support SNMP, RMON/RMON-II, SSH, telnet, web management through network management software.

9 IEEE Standards: IEEE 802.1AB, IEEE 802.1D, IEEE 802.1p, IEEE 802.1Q, IEEE 802.1s, IEEE 802.1w, IEEE 802.3ae, IEEE 802.3ba, IEEE 802.3ah, IEEE 802.3ad.

10 Certification: EAL3/ NDPP or above Certified.

4.6.3 TOR/Distribution Switch

1 The should have Non-blocking (Wire Speed) Architecture with Minimum 24 ports of 10/100/1000 base-T and 4 SFP+ uplink ports (populated with required modules). 1 U Rack mountable and should provide stacking of minimum 9 switches with 80Gbps of dedicated stacking bandwidth (All required accessories, licenses to be provided).Switch should support internal redundant power supply.

2 128Gbps or higher Backplane capacity and minimum 90 Mpps of forwarding rate, Support for at least 4000 VLANs & 16k MAC address

3 Protocol: IGMP snooping v1 & v2, static IP routing and RIP from day 1, Should be upgradable to OSPF, OSPFv3, RIPnG, PIM, MLD in future, SSH, SNMPv3, DHCP,

4 Management: Switch needs to have console port for administration & management, Management using CLI, GUI using Web interface should be supported, FTP/TFTP for upgrading the operating System, SNMP v1, v2, v3, Switch should be manageable through both IPv4 & IPv6.

5 IEEE Standards: IEEE 802.1x, IEEE 802.1D, IEEE 802.1p, class-of-service, IEEE 802.1Q, IEEE 802.3 10BASE-T, IEEE 802.3u 100BASE-TX

6 Switch should be FCC Part 15, ICES-003, VCCI Class A, EN 55022, EN 55024, EN 300386, CAN/CSA 22.2 No.60950-1, IEC60950-1, Reduction of Hazardous Substances (ROHS) 6 certified

7 Should have modular OS and should support configuration roll back to recover mis-configured switch to last known good configuration

4.6.4 Anti-APT

1 The APT appliance should be a purpose built on premise appliance based solution with integrated support for sandboxing. Cloud based solution will not be accepted.

2 The hardware-based solution should provide protection for all incoming and outgoing web and email traffic from /to Internet. Solution should also detect advance web based attacks in flash file using technologies but not limited to like push forward technology, remove exploitable content, including active content and embedded objects, should be able to Reconstruct files with known safe elements, solution should also be able to maintain flexibility with options to maintain the original file format and specify the type of content to be removed. Solution should also be able to handle evasion techniques by detecting DEP, ASLR, ROP and SEH and other exploitation techniques (e.g. privilege escalation) by monitoring the CPU flow.

3 The quoted APT OEM must have NSS Lab’s recommended rating as per breach detection system methodology2.0 and should have block rate of at least 95%.

4 The APT appliance should be able to handle min 2 Gbps incoming /outgoing traffic (throughput) and for at least 10,000 users.

5 The APT appliance should be able to process min 1,000,000 files/month (either web or mail or both). Solution should also support File Size atleast 75 Mb for sandboxing.

6 Appliance should have minimum 2 x 1 TB storage in RAID 1.

7 The APT appliance should support at least 35 virtual machines running simultaneously.

8 Min 4 Copper and 2 x 10G Fiber ports should be provided in APT appliances for achieving functionalities mentioned.

9 Minimum one number of 1G Copper ports for management.

10 The Hypervisor used by sandboxing solution must not be an OEM solution such as from VMWare, HyperV, VirtualBox, RHEV etc. however it should be a custom Hypervisor purpose built for sandboxing requirement.

11 The solution must be able to detect and report malware by using multiple images of Windows XP, 7, 8 and 10 etc.

12 The solution must support prepopulated LICENSED copies of Microsoft windows and office images through an agreement with Microsoft. There should be no requirement for the customer to buy additional Microsoft licences for sandboxing solution.

13 Anti-APT solution should be able to work independently of signature updates from OEM website.

14 The solution must be able to support scanning links inside emails/documents for zero days & unknown malware and support sandboxing of file sizes between 2 Kb and 50 MB. Solution should have an ability to remove all the active content, harmful links in email message/documents and macros sending only a clean document to the end user.

15 The solution should inspect the web sessions (HTTP and HTTPS both) to detect and notify the malicious web activity including malicious file downloads through the internet. Third Party/Separate appliance for SSL offloading will not be accepted.

16 The solution to be provided with complete endpoint detection and response (EDR) solution for at least 1000 endpoints and should work seamlessly with the same.

4.6.5 Endpoint Detection and Response.

1 The offered solution should perform the following min tasks at endpoints:

a. Endpoint Firewall

b. Endpoint Application Control

c. Media Encryption on HDD and USB

d. Prevention of C&C and BOT traffic directly at endpoint

e. Anti Ransomware Features

f. Anti-Phishing Protection

g. Compliance Monitoring capabilities

h. Endpoint Level Forensics

2 The offered solution must be from the same OEM as that of the APT and should integrate with the sandboxing device installed under APT solution. In case EDR and APT

solution are from different OEM then an on premise sandboxing solution must be provide with the EDR solution. Solution must include a Zero-hour protection mechanism for new viruses, malwares spread through email and spam without relying solely in heuristic or content inspection. Able to perform different scan Actions based on the virus type or abnormal behaviour observed (Trojan/ Worm, Hoax, Virus, other).

3 Solution must have capabilities to isolate and quarantine the endpoints from the network in scenarios where windows patches, hotfixes, services packs, virus definitions are missing or outdated on the endpoint. The solution must have capabilities to prevent against all families of ransom wares and restore encrypted files in event of a ransom ware attack.

4 The solution must have capabilities to prevent users from accessing phishing websites and URLS and prevent the users from entering corporate credentials on phishing websites. Shall provide Real-time product Performance Monitor and Built-in Debug and Diagnostic tools, and context- sensitive help.

5 The solution must support multiple remote installations. Shall provide for notification options for Virus, malwares, advanced threats, URLs, C&C call backs etc. Should be capable of providing multiple layers of defence from Known as well as unknown threats like zero days, worms, malwares, APT attacks at endpoint.

6 Shall have facility to clean, delete and quarantine and restore the virus, malware, and ransom ware affected files. Should support scanning for ZIP, RAR compressed files, and TAR archive files. Should support online update, where by most product updates and patches can be performed without affecting the normal operations. Must update itself over internet for virus definitions, program updates etc. (periodically as well as in push-updates in case of outbreaks).

7 Should support memory scanning at the endpoint and advanced threat analysis to a centralized sandboxing device on the network from the endpoints. Updates to the scan engines should be automated and should not require manual intervention.

8 All binaries from the vendor that are downloaded and distributed must be signed and the signature verified during runtime for enhanced security. Updates should be capable of being rolled back in case required.

9 Should support various types of reporting formats such as CSV, HTML and text files. Should provide native forensics capabilities for the endpoints and should be able to perform forensics even when outside the network perimeter or in offline mode.

10 Should provide in browser protection through plugin or add on mechanism to prevent and control download of malicious and unknown attacks and by blocking access to data entering on phishing websites, by removal of harmful active content in files and by converting potentially harmful files to PDF.

11 Should integrate with the sandboxing solution provided in APT solution. The solution must be provided with a centralized management console to manage at least 500 endpoints.

4.6.6 SIEM

1. SIEM and Forensics Platform is required for complete visibility to identify and investigate attacks, the ability to detect and analyse even the most advanced of attacks before they can impact critical data , and the tools to take targeted action on the most important incidents. Complete visibility across logs, packets and end point is critical. Appliance based solution for better performance is required. The solution should collect, analyse, and archive massive volumes of data at very high.
2. Speed using multiple modes of analysis. The platform should also be able to ingest threat intelligence about the latest tools, techniques and procedures in use by the attacker community to alert government on potential threats that are active.

SIEM for Logs & Packets:

1. Next generation platform should encompass log, packet and end point data with added context and threat Intelligence. Should provide complete network visibility through deep packet inspection high speed packet capture and analysis. SIEM for Logs and deep packet inspection should be from Single OEM.

2. The solution should be a physical appliance form factor with following components:

Management & Reporting

Normalization and Indexing

Correlation Engine (multi-device, multi-event and multi-site correlation)

Data Management

3. There should be no limitation on number of devices to be supported. Any addition in no. of devices should have no cost impact on department.

4. The SIEM & Log Monitoring solution should be from a different OEM than the Prevention Security solutions like F/W, IPS, HIPS, AV, DLP, and Encryption.

5. The solution should provide an integrated SOC dashboard and Incident analysis system that could provide a single view into all the analysis performed across all the different data sources including but not limited to logs and packets. The Tool should have role based access control mechanism and handle the entire security incident lifecycle.

6. Real time contextual information should be used at collection/normalization layer and also be available at correlation layer where any events are matched during correlation rule processing. In addition solution must provide contextual Hub at investigation layer for all relevant contextual awareness data regarding alerts/incidents available for any information asset like IP/Device etc.

7. All logs that are collected should be studied for completeness of information required, reporting, analysis and requisite data enhancement, normalization should be performed to meet the reporting and analysis needs.

8. A single log appliance should support minimum 30,000 EPS and packet appliance should support at least 1GBPS line rate with multiple ingress interfaces for capturing from multiple network interfaces.

9. Correlation Engine appliance should be consolidated in a purpose build appliance and should handle 100,000 EPS.

10. The solution should be storing both raw logs as well as normalized logs. The same should be made available for analysis and reporting. Solution should be sized to provide online storage for 1 year at central site. Both raw logs and normalized logs should be made available with minimum 90 TB of storage provided by OEM.

11. The solution should incorporate and correlate information that enables the Information Security Team to quickly prioritize it's response to help ensure effective incident handling.

12. The monitoring should be cross device and cross vendor and be both out of the box and scalable to cover additional devices and applications as required.

13. Appliance should have minimum 128 GB RAM to provide optimal performance and should provide at least 4 network interfaces on board.

14. Should be managed and monitored from SIEM unified console for Correlation, Alerting and Administration.

15. Should store RAW packet DATA for 7 days and normalized packet data for 30 days for forensics.

16. Should be able to provide complete packet-by-packet details pertaining to one or more session of interest including Session replay, page reconstruction, image views, artefact & raw packet and object extractions.

17. Should be able to filter the captured packets based on layer-2 to layer-7 header information.

18. Should provide comprehensive deep packet inspection (DPI) to classify protocols & application.

19. The proposed solution must be able to provide the complete platform to perform Network forensics solution.

20. The solution must be able to detect malicious payload in network traffic. Detect and reconstruct files back to its original type. Detect hidden or embedded files. Detect and flag out renamed files.

21. The solution must have the ability to capture network traffic and import PCAP files using the same infrastructure.

22. Should have customizable and configurable dashboards for users.

4.6.7 Server Load Balancer

1. The proposed Network Function Appliance should be multi-tenanted appliance and have capabilities to support multiple 3rd party and open source independent virtual instance of Network functions with dedicated Hardware resources for future requirements and scalability.
2. The appliance should have minimum 8 x10G SFP+ interfaces from day one . Should have built in 64 GB RAM, 2 TB Hard disk and capability to create at least 16 virtual Network functions from Day 1. Device to provide 50 Gbps throughput from Day1. Device should have minimum12*SSL ASICS/FGPA/cards with network virtual function support
3. The appliance should provide application delivery controllers with features like round robin, weighted round robin, least connection, Persistent IP, Hash IP, Hash Cookie, consistent hash IP, shortest response, proximity, snmp, SIP session ID, hash header etc. and support for policy nesting at layer7 and layer4, Should also have Script based functions support for

content inspection, traffic matching and monitoring of HTTP, SOAP, XML, diameter, generic TCP, TCPS. Load balancer should support ePolicies to customize new features in addition to existing feature/functions of load balancer

4. Device to have capabilities to support ADC and SSL VPN as independent Network Function and not an integrated solution to ensure required performance. Should also provide machine authentication based on combination of HDD ID, CPU info and OS related parameters like mac address to provide secure access to corporate resources.

5. It shall support built-in failover decision/health-check conditions. It shall also support failover and High Availability (HA) requirements. It shall have redundant power supplies. Shall support script based functions support for content inspection, traffic matching and monitoring of HTTP, SOAP, XML, diameter, generic TCP, TCPS.

6. Should provide comprehensive and reliable support for high availability with Active-active & active standby unit redundancy mode. Should support both device level and VA level High availability for individual Network Function

4.6.8 Link Load Balancer

1. The proposed device should be a dedicated purpose built Multi-tenanted device which can host multiple different virtual network functions. It should have capabilities to support 3rd party and open source independent virtual network functions with dedicated Hardware resources for future requirements and scalability.

2. The appliance should have minimum 8 x10G SFP+ interfaces from day one. Should have built in 64 GB RAM, 2 TB Hard disk to create virtual network functions and capability to create at least 16 virtual Network functions from Day 1. Device to provide minimum 50 Gbps throughput

3. Appliance should Support for multiple internet links in Active-Active traffic balancing and active-standby failover mode for both inbound and outbound traffic using algorithms like round robin, Weighted round robin, target proximity and dynamic detect. Appliance should also support WAN optimization with features of Network de-duplication, TCP optimization with SSL based secure WAN to avoid the repeated content across the WAN and to ensure efficient utilization WAN bandwidth.

4. Should support XML-RPC for integration with 3rd party management and monitoring. Should also support SAA, SAML, Hardware binding and AAA support along with SSO. Solution must support machine authentication based on combination of HDD ID, CPU info and OS related parameters i.e. mac address to provide secure access to corporate resources.

5. It shall support built-in failover decision/health-check conditions. It shall also support failover and High Availability (HA) requirements. It shall have redundant power supplies. Shall support script based functions support for content inspection, traffic matching and monitoring of HTTP, SOAP, XML, diameter, generic TCP, TCPS.

6. Should have IPV6 support with IPv6 to IP4 and IPv4 to IPv6 translation and full IPv6 support. Also should have IPV6 support with DNS 6 to DNS 4 & DNS 4 to DNS 6 translation based health check for intelligent traffic routing and failover.

7. Should provide comprehensive and reliable support for high availability with Active-active & active standby unit redundancy mode. Should support both device level and VA level High availability of individual virtual network function.

8. Should have capabilities to support independent Virtual Network Functions like WAN Optimization, DDoS etc.

4.6.9 DDoS

1. The Anti DDoS module should be expected to constantly monitor the behaviour of the application visitors and prevent common application layer attacks.
2. The proposed solution should detect and mitigate both traditional network- layer DDoS attacks and more advanced application layer attacks.
3. The proposed solution should have the capability to be configured in detect as well as protect mode and should prevent suspicious outbound traffic for threats and blocking malicious traffic. Solution must support the ability to blacklist a host, domain, URL.
4. The proposed solution must provide the ability to block bot-originated traffic according to system- supplied signatures. The Solution with 45 Gbps SSL Throughput. The DDoS solution should be a dedicated hardware with dual power supply. The appliance should have 8 X 10GE SFP+ ports.

4.6.10 WAF

1. Solution should be deployed in HA (High Availability) mode and protect the web applications from attacks. WAF solution should filter the HTTP/S traffic based on the rules set defined. Proposed WAF should be able to address top 10 OWASP vulnerabilities.
2. Proposed solution shall prevent the following attacks (but not limited to): Brute force, Access to predictable resource locations, Unauthorized navigation, HTTP request format and limitation violations (size, unknown method, etc.) and File upload violations
3. Solution should be able to inspect web application output and respond (allow, block, mask and/or alert) based on the active policy or rules, and log actions taken.
4. Support dynamic source IP blocking and should be able to block attacks based on IP source and automatic updates (if required) to the signature database, ensuring complete protection against the latest application threats.
5. Proposed WAF module should be from different OEM than Firewalls or Load Balancers for better security.
6. Should have positive security model with machine learning capabilities to detect and prevent anomaly in application traffic and unknown attacks. Machine learning should be based on true ML algorithms, and not just automation of dynamically learnt rules.
7. Should have 4-10Gig ports and storage capability of 2 TB. Proposed solution should have integrated Redundant power supply.

4.6.11 Key Management

Sr. No.	Particulars
Functional Capabilities	
(a)	Must support cryptographic offloading and acceleration
(b)	Should provide Authenticated multi-level access control
(c)	Must have strong separation of administration and operator roles
(d)	Capability to support hardened and hardware based client authentication mechanism with HSM

(e)	Must have secure key wrapping, backup, replication and recovery
(f)	Must support unlimited protected key storage
(g)	Must support clustering and load balancing
(h)	Should support unlimited Logical cryptographic separation of application keys
(j)	Must support —k of n multi-factor authentication
Application Program Interfaces (APIs)	
(a)	PKCS#11, Open SSL, Java (JCE), Microsoft CAPI and CNG
Host connectivity.	
(a)	Dual Gigabit Ethernet ports (to service two network segments)
Cryptography	
(a)	Asymmetric public key algorithms: RSA, Diffie-Hellman, ECMQV, DSA, El-Gamal, KCDSA, ECDSA, ECDH
(b)	Symmetric algorithms: AES, Arcfour, ARIA, Camellia, CAST, DES, MD5 HMAC, RIPEMD160 HMAC, SEED, SHA-1 HMAC, SHA-224 HMAC, SHA-256 HMAC, SHA-384 HMAC, SHA-512 HMAC, Tiger HMAC, Triple DES
(c)	Hash/message digest: MD5, SHA-1, SHA-2 (224, 256, 384, 512 bit), HAS-160, RIPEMD160
(d)	Full Suite B implementation with fully licensed ECC including Brain pool and custom curves
Security compliance	
(a)	FIPS 140-2 Level 3
Safety and environmental compliance	
(a)	Compliance to UL, CE, C-TICK, Canada ICES, FCC part 15 (for Commercial products)
(b)	Compliance to RoHS2, WEEE
(c)	IPv6 and USGv6 compliant
Management and monitoring	
(a)	Support Remote Administration —including adding applications, updating firmware, and checking the status— from NoC
(b)	Syslog diagnostics support
(c)	Command line interface (CLI)/graphical user interface (GUI)

(d)	Support SNMP monitoring agent
Physical characteristics	
(a)	Standard 1U 19in. rack mount with integrated Smart Card Reader
Performance	
(a)	RSA 2048 Signing performance - at least 3000 RSA 2048 Key generation performance - 10
Custom Application	
(a)	Should enable secure execution of custom security-critical application code within the tamper resistant hardware boundary
Key Generation and Protection	
(a)	Ability to generate RSA keys (2048 and 4096) on board on demand and shall be secured by high security module in accordance with FIPS 140-2 level 3 recommendations for Cryptographic Modules Validation. RSA 2048 key generation performance min 05 keys/second
Key back up and restoration	
(a)	The proposed solution must include the software/hardware to - securely store the keys at DC, at DR and at one remote location and restore them in case of necessity
No. of Keys to be protected	
(a)	The HSM must secure a minimum of 1 lakh keys in accordance with FIPS 140-2 level 3 standards. The licensing and HSM hardware must have no restriction on the number of keys to be protected
Performance upgrade of HSM	
(a)	The performance of HSM should be upgradable on field.
Instant Key reflection	
(a)	Multiple HSMs to be supportable for DR, key backup, key update, and key processes, load balancing and failover. Should support automatic and instant key reflection to all the HSMs in the system.
Logical partitions	
(a)	Unlimited logical/cryptographic separation of application keys.

4.6.12 Data Security at Rest

Data-At-Rest Security (Data Security Manager)
Separation of Duty and Privileged User Access Control

The solution must be able to protect data-at-rest against root/system privileged user account access. It should also protect file level encryption. The DSM should be a hardware device with FIPS level 3 HSM .The solution should be able to support file level encryption in transparent manner. No downtime is expected while data is transformed into encrypted data
Proposed data protection solution must support fine-grained policy to enable administrator to perform activity like file archive and backup, without access to the data content itself. The
The proposed solution must support a separation of duties (SoD) to meet rigorous compliance rules including PCI DSS, HIPAA/HITECH and government data breach policy. The vendor must provide compliance whitepaper to prove such support capability
Proposed solution must support multi-tenancy using separate domain with configurable policies, data encryption key management and audit log. Must have a seamless SIEM Integration. Must Protect the unstructured data (file-shares, files and folders) including big data.
Support Transparent Data Encryption
The proposed data protection and encryption solution must support transparent data protection on all major operating system include: • Microsoft: Windows Server, 2008, 2012 • Linux: Red Hat Enterprise Linux (RHEL), SuSE Linux Enterprise Server, Oracle RedHat Compatible Kernel and Ubuntu • UNIX: IBM AIX, HP-UX, and Solaris Database
There should not be any changes in the storage space after the encryption.
Proposed data protection solution must be able to secure both structure database information and unstructured files such as PDF, spreadsheet, scripts, images, audio/video recordings and extract-transformation-load batch files.
Proposed data security solution should have minimum performance impact to database transactions with not more than 10%.
The data transformation should not involve any downtime and live transformation is expected to achieve high Performance Encryption with 100% System Uptime. - Solution must be able to enforces access controls based on – “resources”, “processes”, and “time based access” so that only the defined resources can be accessed with the defined processes and defined users/groups at any given time - Ability to learn the effect of policies (learn mode) before actual encryption is applied is must. - Not only appliance but agent also needs to be FIPS certified
Application Encryption and Tokenization
The data protection solution must support format preserving tokenization
the proposed tokenization and masking solution must provide REST API
The data masking solution must support dynamic masking through policy based masks
The proposed solution should support Teradata V14 and V14.1 database encryption with UDF
The proposed platform should support vault less tokenization

The proposed platform should support vault based tokenization
The proposed platform should support gateway to encrypt data stored on S3 and Box
Key Management and KMIP
the proposed encryption and key management solution must be able to support KMIP client
The proposed solution should be certified to support Nutanix KMIP
The proposed solution must provide centralized key management for Oracle and MSSQL TDE master key.
The security administrator console should support 2-factor authentication with RSA.
The data protection solution must provide centralized audit for security administration access, key creation, policy changes, data access log and so on.
The proposed solution must provide application encryption support with Java, C/C++, and .Net API.
The proposed solution support LDAP and Microsoft Active Directory authentication
Support industry proven cryptograph security standard:3DES, AES128, AES256, ARIA128, and ARIA256 and asymmetric key RSA-4096/2048, SHA-256 algorithm
The Key management repository must provide virtualization option, with OVF image for deployment option - Hardened Operating System, root account must be disabled, all unnecessary software packages must be removed. A firewall in place that only opens a limited set of required ports.

Hardware Specs
Should be a FIPS 140-2 level 3 and Common Criteria Certified
Should have support for column level encryption
Should support RSA 1024, RSA 2048, RSA 4096, AES 128, AES 256, 3DES, ARIA 128, ARIA 256
Should support Clustering for high availability
Should support multi tenancy
Should have Secure Web-based GUI, secure shell (SSH), and console
Should be able to encrypt of all databases
Should be scalable at least 10000 connectors
Should have File servers support on Windows, Linux
Should be a TCP/IP based FIPS certified appliance
Should Support delegated admin, “M of N” keys. Capable of storing one million keys in hardware.
Should have support for standard libraries and protocols - PKCS#11, KMIP, REST
Should have 24/7 tel/email OEM support infrastructure based out of India
Should support live data transformation (encrypting existing data without downtime)
Should allow Key Caching, Key rotation, key Versioning, Schedule Key Rotation
Should support web Service architecture for easy integration with different application
should support 2 removable 80+certified (100VAC-240VAC/50-60Hz) 400W power supplies
Should support operating temperature 10° to 35° C (50° to 95° F)
Should support non-operating temperature -40° to 70° C (-40° to 158° F)
Should support humidity 8% to 90% (non-condensing)
Should support FCC, UL, BIS certifications
Should support two factor authentication (for administrator to login to Key manager web console)
Should support SNMP, NTP, Syslog-TCP
Should support syslog formats CEF, LEEF, RFC 5424

High Performance
The proposed data protection solution must support hardware cryptographic acceleration including •Intel and AMDAES-NI SPARC encryption • IBM P8 cryptographic coprocessor
Data Access Audit and Report
The proposed data protection solution must provide fine-grained auditing records that show system accounts and processes accessing data based on security policy.
The proposed data protection solution must support integration with SIEM solution include: Archsight, Splunk, IBM Qradar, and deliver centralized access audit and monitoring report
Certification & Validations
The encryption key manager must be Common Criteria (ESM PP PM V2.1) certified
The encryption key manager should have option with FIPS 140-2 Level 3 HSM in the box.

4.6.13 Secure Email Gateway

1 The proposed system should be a dedicated appliance based solution or Virtual Application image for email security. The Solution should have feature of virus scanning engine strip the infected attachments and the Solution should detect known or suspect secure-risk URLs embedded in the email, which are reliable indicators of spyware, malware or phishing attacks.

2 The Solution should have feature of virus scanning engine strip the infected attachments and The Solution should detect known or suspect secure-risk URLs embedded in the email, which are reliable indicators of spyware, malware or phishing attacks. The solution should support dictionaries scanning and dictionaries are built-in the product and allow customer to create his own dictionary. The solution should have at least 1500+ predefined content rules inbuilt with Email Security & embedded in the product.

3 The Solution should have close to 100% virus detection rate for known viruses. The Solution should have multiple AV engines for anti-virus and malware scanning. The Solution should provide proactive virus detection methods for new email-borne virus. The Solution should have feature of virus scanning engine strip the infected attachments.

4 The Solution should support URL classification of the embedded links and it contributes for SPAM detection. The solution should support image based spam detection capability, such as the pornography images within the email and it allow customer to adjust the sensitivity level.

5 The solution should perform image based filtering. It’s should use sophisticated analytical algorithm to analyse image to determine attributes that indicate the image may be of a pornographic or non-pornographic nature in known and unknown spams emails. The solution should have capability to analyse text inside image going through email. The solution should monitor and control sensitive email download to mobile devices through active sync.

6 The solution should provide the capability of connection control and message rates control for inbound and outbound respectively. The solution should support policy based TLS encryption between mail domains. The solution should have directory harvesting and DoS prevention capabilities. The solution should support internal sender authentication. The solution should provide real time IP reputation system. The solution should allow the administrator to specify the re-try time for a delivery failure.

7 The solution should have centralized management, including policy configuration, quarantines and logs/reporting. The solution should support the real-time graphical and chart-based dashboard for the summary of email filtering activities. The solution should be able to manage the complete solution - DLP, Email and web security through same centralized management.

8 The Solution should have option for end user notification for email quarantining letter to be customized and click boxes that enable the user to release e-mail, report false positives, add senders to allow-or block lists and direct links to personal email management portal. The solution should allow where Administrator can specify which queues can be accessed by end user.

9 The solution should have True Source IP Detection and Connection Blocking feature should work even if Email Security is deployed behind Corporate Email Relay Server/Firewall SMTP. The solution should able to provide the complete forensics of the sensitive outbound data based on the policy defined and should be able to quarantine and release as per automated workflow.

10 The solution must be from same OEM for optimum operation and manageability and the OEM should have own TAC center in India.

11 The solution should support Domain-based Message Authentication, Reporting, and Conformance (DMARC) validation integration. It should also support Domain Keys (DKIM) Identified Mail integration S/MIME encryption.

12 Anti-Spam/Content Level Detection: The propose system shall minimally integrated following spam detection technologies with unlimited users license for Inbound and Outbound Email Filtering, Extensive Heuristic Spam Filters, Dynamic Heuristic Rule Updates, Attachment Content filtering, Deep Email Header Inspection, Spam Image Analysis Scanning, PDF Scanning / PDF Image Scanning, Global and User Customized Black/White List Filtering, 3rd Party RBL and DNSBL support & Forged IP Checking.

13 Antivirus/Spyware Protection: The proposed system should have integrated Antivirus with unlimited users license and provides the following services:

14 AV engine and signatures, including legacy virus detection, Automatic update of antivirus and attack signatures global network - Push, Scheduled & Manual update, SMTP Messages Virus Scanning, Compressed Attachment and Nested Archive Support, Quarantine Infected files, Replacement Message Notification, Block by File Type, Attachment Filtering.

15 Anti-Malware Protection.

15.1. The solution should combine multiple static with dynamic technologies including signature, heuristic and behavioural techniques.

15.2 The solution should provide virus outbreak prevention through on premise sandboxing solution to protect against a wide range of constantly evolving threats such as ransomware and targeted attacks.

4.6.14 Secure Web Gateway

1 The solution should provide proxy, caching, content filtering, SSL inspection, protocol filtering, inline AV and content inspection in block mode on the same Appliance. The solution should support behavioural sandboxing to enhance advanced threat detection for Malware detection.

2 The solution should be capable of dynamically blocking a legitimate website which has become infected and unblock the site in real time when the threat has been removed for below mentioned security categories and vulnerabilities. The solution should have real time content classification and security scanning with automatic database updates for security categories- Advanced malware command and control, advanced malware payloads, Bot networks, Compromised websites, key loggers, Phishing and other frauds, Spywares

3 The solution should inspect the sensitive content through 1500 pre-defined templates, textual content inside image, cumulative content control and inspection through web channel to prevent the content from being sent over outbound web channel. The solution should have ability to provide geo-location awareness for security incidents. The solution should have ability to protect the sensitive data exfiltration based on geo-location.

4 The solution should have at least 20+ million websites in its URL filtering database and' should have pre-defined URL categories and application protocols along with YouTube, Facebook and linked-in controls. Solution vendor should ensure that 100 predefined categories & 100+ pre-defined protocols.

5 The solution should support same policy enforcement in real time policy sync for users even when they access Internet outside the corporate network, this should be enforced through an agent deployment on roaming endpoints ((MAC and Windows - MAC OS X 10.10 and MS Windows 10) . And this solution should be on premises and not with the help of SDSCL/MSIS i.e. mobile user traffic should redirect to on premise solution for policy checks.

6 The solution should have ability to block anonymizer sites or proxy avoidance tools. Should be provided in default protocol database Ghost surf, Google web accelerator, Hopster, Jap, Real tunnel, Socks online, Tongtongtong, Toonel, Tor, Your freedom. The solution must provide mentioned categories -Facebook Posting: Facebook function that enables a user to share a post, status or link, Facebook Commenting, Facebook Friends, Facebook Photo Upload, Facebook Mail, Facebook Events, Facebook Apps, Facebook Chat, Facebook Questions, Facebook Video Upload, Facebook Groups etc.

7 The solution should apply security policy to more than 100 protocols in multiple categories more than 15. This includes the ability to allow, block, log, and assign quota time for IM, P2P, and streaming media and solution should provide at least below mentioned security categories as below RIGHT FROM FIRST DAY:

7.1) Advanced Malware Command and Control category

7.2) Advanced Malware payload detection category

7.3) Malicious embedded links and iframe detection category

7.4) Mobile malware category

7.5) Key logger and Spyware category

7.6) P2P software database from day 1 to control/block the below P2P protocols

8 The solution should have granular control over popular social web applications like Facebook, LinkedIn, Twitter, YouTube, and others. The solution should have social control Video UPLOADS to Facebook and YouTube applications. The solution should have built-in or custom policies for identifying and segregate You Tube traffic for Education only and other irrelevant non-compliance video, it should simplify design and implementation of policy to ensure user compliance

9 The solution should provide geo-location awareness for security incidents. The solution should provide inbuilt capability malicious content of password and unknown encryption files. The solution should support to have capability to differentiate between YouTube educational and entertainment videos through default categories and should have separate default categories for the same.

10 The solution should have visibility and blocking for cloud applications and shadow IT application usage for enhanced security.

11 The OEM should have own TAC center in India.

4.6.15 Web

This solution should ensures that tempering of any website or any script file can be automatically detected and reverted back to the original state within a minute or two. In case any attempt is made for defacement of these website, the website and file monitoring solution, will able to detect it revert back the website/ scripts files to their original state.

Technical Specification:

1 The on premise application should protect both web content and script files from defacement
2 It should protect data integrity and create an immutable audit trail of activities log
3 It should have fast monitoring in both File level and URL level.
4 The monitoring speed should be atleast 500k files in 10 seconds at File level.
5 It should monitor 100 URLs in every 5 minutes at URL level.
6 If tampered file is detected, it must be recovered automatically within 1 min
7 The application should have the following features:
a. KSI Block Chain
b. Data Protection
c. URL Content Protection
d. Data Recovery
e. Auto Recovery
f. Manual Recovery
g. High Speed Monitoring
h. Alert System
i. Role based permission

j. Reporting

18 The technology should work on “keyless” signature to any type of data.

19 The signature should store with the data, as an attribute which can be used to verify the time of creation, identity of creator and integrity of the data, independently from insiders, keys, secrets and certificates, and without the data leaving the premises.

20 This Technology must have implemented at least in two places anywhere in the world and proof should be submitted like Purchase order copy or Project completion letter from the end customer.

4.6.16 EMS Enterprise Management System (EMS):

General:

1 For effective operations and management of IT Operations, there is a need for an industry-standard Enterprise Management System (EMS). Given the expanse and scope of the project, EMS becomes very critical for IT Operations and SLA Measurement. Some of the critical aspects that need to be considered for operations of IT setup of are:

a) Network Fault Management

b) Network Performance Management

c) Network Flow Traffic Monitoring

d) Application Performance Management

e) Server Performance Monitoring

f) Centralized Log Management

g) Centralized and Unified Dashboard

h) Centralized and Customizable Service Level Reporting

I) Help Desk for Incident Management

2 The Monitoring Solution should provide Unified Architectural design offering seamless common functions including but not limited to:

• Event and Alarm management,

• Auto-discovery of the IT environment,

• Performance and availability management

• Correlation and root cause analysis

• Service Level Management, notifications

• Reporting and analytics

• Automation and Customization

3 There should be a tight integration between infrastructure metrics and logs to have the single consolidated console of Infrastructure & security events.

4 Consolidate IT event management activities into a single operations bridge that allows operator quickly identify the cause of the IT incident, reduces duplication of effort and decreases the time it takes to rectify IT issues.

5 The Operator should be able to pull up security events related to a given Configuration Item, from a single console which also has NOC events, and use the security events to triage the problem. This way the Operator gets consolidated system/network event details and security events (current and historical) from the same console and save time in troubleshooting/isolating the issue.

6 The operator should be able to build correlation rules in a simple GUI based environment where the Operator should be able to correlate cross domain events.

7 Scalability – The system should be capable of supporting at least 100 thousand network flow per second on single server with capability to capture each unique traffic conversations.

8 Scalability – The solution must be scalable, it should be able to support at least 25000 log events per second and also be able to support beyond 25000 EPS by linearly adding more servers of either reference system type, depending on the size of the expected load.

9 The solution shall provide future scalability of the whole system without major architectural changes.

10 The Solution shall be distributed, scalable, and multi-platform and open to third party integration such as Cloud, Virtualization, Database, Web Server, Application Server platforms etc.

11 All the required modules should be from same OEM and should be tightly integrated for single pane of glass view of enterprise monitoring.

12 The solution must provide single integrated dashboard to provide line of business views and drill down capabilities to navigate technical operator's right from services to last infrastructure components.

13 Consolidated dashboard of the proposed EMS solution must be able to do dynamic service modelling of all business critical production services & use near-real time Service Model for efficient cross domain topology based event correlation.

DETAILED SPECIFICATIONS: EMS

Consolidated Dashboard

1 The platform must provide complete cross-domain visibility of IT infrastructure issues.
2 The platform must consolidate monitoring events from across layers such as Network, Server, Application, Database etc.
3 The solution should support dynamic discovery to maintains Run-time Service Model accuracy e.g. virtualization and cloud.
4 The solution must support custom dashboards for different role users such as Management, admin and report users.
5 The solution must allow creating custom data widget to visualize data with user preferences.

6 The solution must support multiple visualization methods such as gauge, grid, charts, Top N etc.

7 The proposed solution must support capacity views to find most consumed resources.

8 The solution should provide superior view of infrastructure health across system, networks, application and other IT Infrastructure components into a consolidated, central console.

9 The solution should allow for customizable operator perspectives.

Network Performance Management:

1 The proposed solution platform shall provide a single integrated solution for comprehensive management of the wired/wireless access, and rich visibility into connectivity and performance assurance issues.

2 The design functionality shall facilitate creation of templates used for monitoring key network resources, devices, and attributes. Default templates and best practice designs are provided for quick out-of-the- box implementation automating the work required to use OEM validated designs and best practices.

3 The proposed solution must provide comprehensive and integrated management of IT infrastructure components to maximize the availability of IT services and SLA performance.

4 The proposed solution must provide the complete view of the Topology and network elements. The NMS shall have the ability to include the network elements and the links in the visual/graphical map of the department. The visual maps shall display the elements in different colour depending upon the status of the element. It is preferable that green color for healthy and amber/yellow colour for degraded condition and red for unhealthy condition is used.

5 The proposed solution must have suitable system level backup mechanism for taking backup of NM data manually of at least one month.

6 The proposed solution must provide the visual presentation of the Network Element's status and the alarms. It shall also present the complete map of the network domain with suitable icons and in suitable color like green for healthy, red for non-operational, yellow for degraded mode of operation etc.

7 The proposed solution must provide Health Monitoring reports of the network with settable periodicity -@24 Hrs, 1 week, 1 month.

8 The proposed solution must provide the graphical layout of the network element with modules drawn using different colors to indicate their status

9 The proposed solution must provide calendar view which allows the operator all the schedule activities such as Reports, Inventory scans etc. It shall also allow to define scheduled report for uptime, link status etc.

10 The proposed solution should have multiple alerting feature to get the notification via email, sms and third party systems

11 The proposed solution must support listening to traps and syslog events from the network devices with retention period at least 6 months.

12 The proposed solution must support defining the data retention period to control storage.

13 The solution must support custom device template to support Generic SNMP devices.

14 The solution must provide discovery & inventory of heterogeneous physical network devices like Layer-2 & Layer-3 switches, Routers and other IP devices and do mapping of LAN & WAN connectivity with granular visibility up to individual ports level.

15 It shall provide Real time network monitoring and Measurement offend-to-end Network performance & availability to define service levels and further improve upon them.

System and Application Monitoring:

1 The solution should offer service driven operations management of the IT environment to manage distributed, heterogeneous systems - Windows, UNIX & LINUX from a single management station.

2 The solution should carry out automated probable cause analysis by picking up feeds from every infrastructure component being monitored and automating the correlation of these alarms Or events to point out the probable cause using remedy actions - E.g. pull the top 5 processes consuming most of the CPU when CPU alarm triggers.

3 The solution should provide a centralized point of control with out-of-the-box policy-based management intelligence for easy deployment for the servers, operating systems, applications and services for correlating and managing all the IT infrastructure components of a business service

4 The solution shall be able to monitor Hypervisor host hardware status e.g. fans, disk, memory, CPU etc.

5 The solution must support SNMP v1-3, PowerShell, SSH, JDBC, HTTP, JMX, collected agents for monitoring various type of devices and systems.

6 It should also be able to monitor various operating system parameters depending on the operating system being monitored and setting thresholds.

7 The solution should support Virtual platforms - VMware and Microsoft Hyper-V, Citrix Xen, AWS, Azure and provide capability to monitor both Microsoft. NET and J2EE applications from the same platform.

8 The solution should provide support for maintenance window and scheduled downtimes.

9 The solution should measure the end users' experiences based on transactions without the need to install agents on user desktops.

10 The solution must be able to provide user usage analysis and show how user's success rate, average time and transaction count has changed over a specific period of time such as current week versus previous week.

11 The solution must be able to provide the ability to detect and alert when users experience HTTP error codes such as 404 errors or errors coming from the web application.

12 Solution shall be able to monitor customer transaction by end-user name, and thus able to understand exactly which customers were impacted, their location, type of browser used etc.

13 The solution must simplify complex app topologies through task–relevant views based on attributes such as location, business unit, application component etc.

14 The solution must proactively monitor 100% of real user transactions; detect failed transactions; gather problems that affect user experiences and prevent completion of critical business processes.

15 The solution must determine if the root cause of performance issues is inside the monitored application, in connected back-end systems or at the network layer from a single console view.

16 The solution must provide proactive real-time insights into real user behaviour, trends, log analytics and performance to enhance customer experience across various channels.

Fault Management:

1 The proposed solution must should provide out of the box root cause analysis with multiple root cause algorithms inbuilt for root cause analysis. It should also have a strong event correlation engine which can correlate the events on the basis of event pairing, event sequencing etc.

2 The Platform must include an event correlation automatically fed with events originating from managed elements, monitoring tools or data sources external to the platform. This correlation must perform:

• Event filtering

• Event Deduplication

• Event aggregation

• Event masking

3 The proposed solution must support creating and monitoring of rising or falling thresholds with respect to basic key performance indicators for network, system and application infrastructures.

4 The solution should have predictive analytics and intelligence in-built into it so as to detect any anomaly before it could potentially hit the threshold thereby giving enough lead time to users to resolve the issues before the threshold is breached.

5 The proposed solution should provide out of the box root cause analysis with multiple root cause algorithms inbuilt for root cause analysis. It should also have a strong event correlation engine which can correlate the events on the basis of event pairing, event sequencing etc.

6 Powerful correlation capabilities to reduce number of actionable events. Topology based and event stream based correlation should be made available.

7 The solution must offer relevant remedy tools, graphs in context of a selected fault alarm/event.

8 The proposed monitoring solution should have capability to configure actions based rules for set of pre-defined alarms/alerts enabling automation of set tasks.

9 The Platform must support Event or Alarm Correlation integrations with service desk to trigger automated creation of incidents, problems management.

10 The solution should classify events based on business impact.

11 The solution should allow creation of correlation or analytics rules for administrators.

12 The proposed solution must provide default event dashboard to identify, accept and assign generated alarms.

Log Management:-

1 The proposed solution must provide a common classification of event irrespective of the log format.

2 The proposed solution must provide the ability to store/retain both.

Normalized and the original raw format of the event log as for forensic purposes.

3 The log data generated should be stored in a centralized server. The period at least which the data must be available should be customizable.

4 The proposed solution must support logs collected from commercial and proprietary applications i.e. Microsoft, Cisco, Brocade, HP, Security System, Firewall, Access Points etc.

5 The proposed solution must support log collection for Directories (i.e. AD, LDAP), hosted applications such as database, web server etc. using agents.

6 The proposed solution must support log collection from Network infrastructure (i.e. switches, routers, etc.). Please describe the level of support for this type of product.

7 The system shall support the following log formats for log collection:

- Windows Event Log
- Syslog
- Access Log Data
- Application Log data
- Any Custom Log data
- Text Log (flat file)

8 The solution should be able to collect raw logs in real-time to a Central log database from any IP device including:

- Networking devices (router/switches/voice gateways)
- Security devices (IDS/IPS, AV, Patch Mgmt., Firewall/DB Security solutions)
- Operating systems(Windows 2003/2008,Unix,linux,AIX)
- Virtualization Platforms(Microsoft HyperV, VMware Vcenter/VSphere 4.X, vDirector, Citrix)
- Databases(Oracle/SQL/MYSQL/DB2)

9 The collection devices should support collection of logs through Syslog, syslogNG and also provide native Windows Agents as well as Agentless (PowerShell) connectors.

10 The proposed solution must provide alerting based upon established policy.

11 The proposed solution must provide SDK/API to write custom connectors and collectors to pull log and monitoring data from third party system.

12 The proposed solution must provide UI based wizard and capabilities to minimize false positives and deliver accurate results.

13 The proposed solution must collect, index the log messages and support full-text searching for forensic investigation.

14 The proposed solution must support the ability to take action upon receiving an alert. For example, the solution should support the ability to initiate a script or send an email message.

15 The solution must provide pre-defined log correlation rules to detect suspicious behaviour.

16 The solution must support real-time and scheduled alerting time-line while creating a log policy to catch specific log pattern.

17 The solution should support applying regex pattern in real-time to extract vendor specific log data for reporting and alerting purpose.

18 The system shall have the capability to drag and drop building of custom queries & reports.

19 The system shall be capable of operating at a sustained 10000 EPS per collection device. The system shall provide the ability to scale to higher event rates by adding multiple collection devices.

Network Flow-based Traffic Analysis:

1 The proposed traffic monitoring system must be able to track all flow of traffic on the network and identify malicious behaviour with all IP conversations.

2 The proposed system must provide details of applications, hosts, and conversations consuming WAN bandwidth to isolate and resolve problems.

3 The proposed system must provide eight-hour, daily, weekly, monthly, yearly, or customizable reporting time periods.

4 The proposed solution must be able to monitor and report on a variety of unique protocols (used in the overall deployed solutions) per day and display utilization data for each protocol individually. This capability must be available for each monitored interface uniquely.

5 The proposed solution must keep historical rate and IP to IP, IP to Protocol, Protocol to Protocol conversation data for a minimum of 12 months (most recent) in its current long term operating database. All data in that database must have a maximum 15 minute window granularity.

6 The proposed solution must keep historical rate and protocol data for a minimum of 60 days (most recent) in its short term operating database. All data in that database must have a maximum 1 minute window granularity.

7 Flow collection systems must support a minimum of 6 million flows per minute and be capable of storing gathered information in a common database where all long term reporting information is held.

8 The system must support the ability to create reports that allow the user to search all IP traffic over a specified historical period, for a variety of conditions.

o Search for any traffic using a specific configurable destination port, or port range.
o Search for any protocol in use by a specific host, interface or list of hosts or interfaces.

Helpdesk - Incident Management:

1 The proposed helpdesk system shall provide flexibility of logging, viewing, updating and closing incident manually via web interface.

2 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.

3 Each incident shall be able to associate multiple activity logs entries via manual update or automatic update from other enterprise management tools.

4 The proposed helpdesk system shall be able to provide flexibility of incident assignment based on the workload, category, location etc.

5 The proposed solution should automatically provide suggested knowledge base articles based on Incident properties.

6 The proposed solution should automatically suggest available technicians based on workload while assigning tickets

7 The proposed solution should tightly integrate with monitoring system to provide two way integration - E.g. when system down alarm created, it should automatically create ticket and assign it to technician, in case system comes up before ticket is resolved by technician, it should automatically close the ticket to minimize human efforts.

8 The proposed system must not create more than ticket for same recurring alarm to avoid ticket flooding from Monitoring system.

9 Each escalation policy shall allow easy definition on multiple escalation levels and notification to different personnel via web based console with no programming.

10 The proposed helpdesk system shall be capable of assigning call requests to technical staff manually as well as automatically based on predefined rules, and shall support notification and escalation over email.

11 The proposed solution should allow administrator to define ticket dispatcher workflow which automatically assign incoming tickets based on rules defined in workflow. E.g. Network fault keyword tickets gets assigned to network technician automatically within NOC team.

12 The proposed helpdesk system shall provide grouping access on different security knowledge articles for different group of users.

13 The proposed helpdesk system shall have an updateable knowledge base for technical analysis and further help end-users to search solutions for previously solved issues.

14 The proposed solution should allow Technician to relate Incidents to Problem, Change and vice versa to have better context while working on any of ticket type.

15 The proposed helpdesk system shall support tracking of SLA (service level agreements) for call requests within the help desk through service types.

16 The proposed helpdesk system shall integrate tightly with the Knowledge tools and CMDB and shall be accessible from the same login window.

17 A configuration management database shall be established which stores unique information about each type Configuration Item CI or group of CI.

18 The proposed solution allow scheduling periodic report to check current software and hardware inventory.

Service Level Reporting:

1 The solution must provide Out of the box reporting templates for performance, availability, operation, virtualization and capacity and audit.

2 The solution should provide reports that can prove IT service quality levels, such as application response times and server resource consumption.

3 The system reports should be accessible via web browser and Reports can be published in PDF and csv format.

4 The solution must provide Reports that can be scheduled to publish automatically or they can be produced on demand.

5 The solution should be able to report in the context of the business services that the infrastructure elements support—clearly showing how the infrastructure impacts business service levels.

6 The solution should provide Business Service Management functionality to track Service quality by logically grouping Network, Server and Application components. The solution should provide correlation between Network, Server and Application to identify the business impact from the specific event or alarm.

7 The solution must provide way to define key performance indicators (KPIs) within the Service Quality report.

8 The solution must provide SLA measurement to track service quality from both Availability and Performance perspective.

Role-Based access control: -

1 The solution should have inbuilt role-based access module to enable multiple users with different groups to create dashboards specific to their department.

2 The Solution should have way to control and define permission such as read/write for set of devices rather than all the devices for the ease of use.

EMS Other Key Requirements: -

1 The Solution should provide all the modules as a single monitoring engine to correlate events in real-time from Networks, Servers and Applications

2 The solution should be deployable on Linux operating systems to reduce the overall TCO

3 The solution should run without any propriety database license for data store Data store must be bundled within EMS (E.g. popular time-series, no-sql, hbase based monitoring systems) to reduce the TCO

4 The solution must provide way to define key performance indicators (KPIs) within the Business Service Management module.

4.6.17 Endpoint Security and HIPS

Sr. No	Functional Requirement for Server Security (HIPS)
1	Solution should support stateful Inspection Firewall, Anti-Malware, Deep Packet Inspection with HIPS, Integrity Monitoring, Application Control, and Recommended scan in single module with agentless and agent capabilities and Firewall should have the capability to define different rules to different network interfaces with stateful inspection.
2	Firewall rules should filter traffic based on source and destination IP address, port, MAC address, etc. and should detect reconnaissance activities such as port scans and Solution should be capable of blocking and detecting IPv6 attacks and Product should support CVE cross referencing when applicable for vulnerabilities.
3	Solution should have Security Profiles allows Firewall rules to be configured for groups of systems, or individual systems. For example, all Windows 2012 servers use the same operating system rules which are configured in a single Security Profile which is used by several servers.
4	The solution should protect against Distributed DoS attack and Solution should have the ability to lock down a computer (prevent all communication) except with management server.
5	Host based IPS should support virtual patching both known and unknown vulnerabilities until the next scheduled maintenance window. Solution should have capability to submit unknown files to sandboxing for simulation and create IOC's on real time basis as per sandboxing analysis and revert back to server security solution and sandboxing should have at least virtual instance of server class OS - Win 2008, win 2012.
6	HIPS should have signatures for known & unknown vulnerabilities and exploits. It should also allow for creation of custom signatures to secure home grown legacy applications. Detailed events data to provide valuable information, including the source of the attack, the time, and what the potential intruder was attempting to exploit, should be logged.
7	Virtual Patching should be achieved by using a high-performance HIPS engine to intelligently examine the content of network traffic entering and leaving hosts.

8	Should provide automatic recommendations against existing vulnerabilities, Dynamically tuning IDS/IPS sensors (Eg. Selecting rules, configuring policies, updating policies, etc...) And provide automatic recommendation of removing assigned policies if a vulnerability no longer exists - For Example - If a patch is deployed unwanted signatures should be un-assigned.
9	The solution should have Application Control rules provide increased visibility into, or control over, the applications that are accessing the network. These rules will be used to identify malicious software accessing the network and provide insight into suspicious activities.
10	Solution should have Security Profiles allows rules to be configured for groups of systems, or individual systems. For example, all Windows 2012 servers use the same operating system rules which are configured in a single Security Profile which is used by several servers
11	Solution should have Security Profiles allows Integrity Monitoring rules to be configured for groups of systems, or individual systems. For example, all Windows 2012 servers use the same operating system rules which are configured in a single Security Profile which is used by several servers. However, each server has unique requirements which are addressed at the individual Host configuration level.
12	Solution should have an intuitive rule creation and modification interface includes the ability to include or exclude files using wildcards filenames, control over inspection of sub-directories, and other features and Solution Should have pre and post execution machine Learning and should have Ransom ware Protection in Behaviour Monitoring.
13	Solution should support any pre-defined lists of critical system files for various operating systems and/or applications (web servers, dns, etc.) and support custom rules as well.
14	Solution should have feature to take backup of ransom ware infected files and restoring the same and Management Server should support Active Passive high availability configuration. Should have central management console for server security and Anti-APT with sandboxing for central visibility and control.
15	Host IPS should be capable of recommending rules based on vulnerabilities with the help of virtual patching and should have capabilities to schedule recommendation scan and entire features of solution should be agentless.
16	HIPS Solution Should not have the need to provision HIPS Rules from the Policy Server as the Rules should be automatically Provisioned.
17	Virtual Appliance should be able to build scan cache of VM which is scanned to compare the same file attributes while scanning other VM's thereby reducing the scan time and Should have the ability to identify resource usage of VM's during scheduled scans to avoid scan storms.

Sr No	Functional Requirement for Endpoint Protection & Storage protection
1	Endpoint solution should have capability of AV, Vulnerability protection, HIPS, Firewall, Device control, virtual Patching and integrated DLP and pre and post machine learning execution.
2	Endpoint vulnerability protection should scan the machine and provide CVE number visibility and accordingly create rule for virtual patch against vulnerability.
3	Endpoint solution should have pre and post execution machine learning and behaviour monitoring along with ransom ware protection engine, ransom ware engine should have feature to take backup of ransom ware encrypted files and restoring the same.

4	Endpoint solution should have integrated DLP with pre-defined templates for HIPAA, PCI-DSS, GLBA etc. for compliance requirements and should have capability to create policies on basis of regular expression, key word and dictionary based for data loss prevention
5	Solution should have capability to submit unknown files to sandboxing for simulation and create IOC's on real time basis as per sandboxing analysis and revert back to Endpoint security solution to block and clean threats and sandboxing solution should support customizable Windows 7/8/10 and Microsoft 2008/12 operating environments for Sandboxing with at least 60 virtual instances running in single sandboxing box.
6	Endpoint solution should be in OEM
7	Host IPS should be capable of recommending rules based on vulnerabilities on endpoint and Host IPS should have dynamic rules based on System posture and endpoint posture
8	Solution should deprovision corresponding HIPS rules id System upgraded or patched and Should support Detecting and Blocking Reconnaissance on the endpoint
9	Solution should be APT ready, capable of submitting to Sandbox for analysis without additional License on Endpoint
10	Server protection for storage solution should provide alerts to administrators for virus outbreaks and emergencies to help reduce response time
11	Server protection for storage solution should support at least ICAP, EMCCAVA, and RPC protocols.
12	Server protection for storage solution should supports EMC Celerra, Isilon, and VNX/VNXe storage servers, NetApp ONTAP filers and IBMN Series running Data ONTAP and Hitachi Data Systems NAS
13	Server protect for storage solution should provide automatic, incremental security updates and centralized management of servers via a web-based console.
14	Server protection for storage solution should provide real-time server protection against viruses, worms, spyware, and Trojan attacks.
15	Server protect for storage should Integrates tightly with NetApp Filers or Hitachi NAS Platform and enables multiple or single-scan server malware protection for multiple layers

4.6.18 Hyper Converged Infrastructure

Sl.	HCI
1	HCI Cluster with a mix of SSD and HDD disks.
2	Processor (Minimum 2.1 GHz processor)
3	The solution shall come with 700 Cores, 5 TB RAM/Memory and with min 3 PB of storage.
4	Storage - Hybrid HCI cluster with at least 10% SSD disks. Boot disks or dedicated caching disks (if required) is separate.
5	Network (4 x 10G Ethernet NICs per node)
6	The proposed solution should support at least two or more leading Virtualization Software's, VMware ESXi, Microsoft Hyper-V & Open KVM, XenServer. HCI solution must support industry leading protocols NFS, iSCSI & SMB.

7	The proposed solution should provide hyper-converged software that allows delivery of enterprise-class storage services across any type of disks (SSD/SAS/NLSAS) using latest x86 server infrastructures without dependence on a separate Storage Area Network & associated components such as SAN Switches & HBAs.
8	The proposed HCI solution should be 100% software defined and should not leverage any specialized hardware(proprietary) other than x86 Hardware to run virtualization layer with virtual storage appliance.
9	The proposed HCI solution must natively support Container based Application like Docker and Open stack integration.
10	The proposed HCI solution should be 100% software defined and should not be dependent on any hardware (RAID Controller etc.) for Compression or De-duplication across each and every nodes in cluster.
11	The proposed solution should run on industry standard x86 servers and it should leverage Virtual Storage Appliance to build true Software defined Storage.
12	The proposed solution independently scale storage and compute as and when needed without any downtime. HCI should support storage expansion without any virtualization license implication for only storage expansion.
13	The proposed HCI solution must have metadata distributed on all nodes in a cluster i.e. each node in the cluster should carry information about data lying across every node in the cluster and capacity utilization/distribution across all nodes has to be uniform at all times.
14	The proposed HCI solution should be able to create multiple logical unit (LUN's) for storage with multiple policy for deduplication and compression across storage logical unit.
15	The proposed HCI solution must support Hybrid and All flash nodes in same cluster without impacting any functionality.
16	The Proposed HCI solution should support Erasure Coding for archival data storage.
17	The proposed HCI solution should be able to leverage SSD for not only for caching but for capacity also to optimized read IOS and there should not be any limitation on SSD overall caching on software defined storage.
18	The proposed solution must have capability to support HCI nodes with different models (same OEM)/different CPU & Memory/Disks configurations in the same cluster without any impact on enterprise-class storage services/functionalities.
19	The proposed solution should support hybrid and all flash nodes in same cluster for future scalability.
20	Shall support minimum 32 nodes in a same cluster without any federation.
21	The proposed solution should have options to create multiple data store for diversified application requirements on deduplication/compression across all storage tier (Hybrid/All Flash).

22	Proposed HCI solution should support fault tolerance of at least two nodes failure within a cluster.
23	Required Hypervisor License and Hypervisor Management should be included into the solution.
24	The proposed solution support thin provisioning for storage.
25	The solution support for automated upgrades of storage controllers through management GUI with no downtime and major impact on production.
26	The proposed solution should take native storage level snapshots with no impact to guest performance.
27	The proposed solution should be capable of creating instant snapshots of virtual machines (hypervisor agnostic) and maintained multiple copies of snapshots & clones.
28	The platform should have capability to leverage SSD for IOPS hungry workload should be running from SSD only.
29	The proposed solution should support multi-site (One to Many & Many to One) replication.
30	Support for layer-2 VLAN for networking and integrated VM IP's Management capabilities.
31	Proposed solution should support Virtual Network visibility with application-centric protection from network threats and automation of common networking operations.
32	Proposed solution should support VM's life cycle policy based firewall rules for east west traffic across VM's through one management console without any third party software.
33	Proposed solution should integrate with third party network function software like virtual load balancers, virtual firewall etc.
34	Proposed solution should integrate with L2/L3 network device with API call function for all required network configuration (L2/L3) with VM Life cycle.
35	The platform should have support for rack /chassis awareness to support redundant data should go to different rack/chassis nodes.
36	The proposed HCI must support connectivity (HCI Storage extension) to 3rd party bare metal servers along with load balanced and distributed architecture across all available nodes in cluster (for optimized DB licensing on physical servers) to HCI storage cluster & use the cluster capacity like a iSCSI, NFS target.
37	The proposed HCI should support native (without any third party software) File Services over NFS, CIFS & SMB and file replication across clusters and data centers.
38	The Platform must provide management through a web based HTML 5 console. Must provide storage, compute & hypervisor metrics on as per VM level as well as health and monitoring of entire platform. Platform should support LDAP Active Directory integration

39	The Platform must support multiple individual clusters (from multiple OEM/Hypervisors) management from a Single Console.
40	The Platform must support monitoring via SNMPv3 and email alerting via SMTP.
41	The Solution should have capability for managing multiple sites/clusters from one HTML5 based browser with single sign on.
42	The Solution should support rest API for third party integration.
43	The solution should have call home capability for remote log collection and proactive support for predictive failure hardware component.
44	The proposed HCI solution should support data at rest encryption without any specialized hardware.
45	The solution should support out of the box security compliance for proposed HCI solution to ensure highly secure HCI environment. Solution should have at list industry three or more certifications. (e.g. NIST, FIPS140-2, EAL2 CCC-Common Criteria Certified, DISA- approved STIG).
46	Shall include 24x7x365 infrastructure maintenance and support for all hardware and software components of the proposed solution, including updates and patches as well as technical support available via telephone, email, and web during all hours (24 hours per day, 365 days per year).
47	The storage solution shall support the single global name space
48	The storage solution shall be s3 Compatible and WORM support
49	The solution shall allow object versioning and tagging
50	The storage solution shall support self-healing and TTFB shall be under 10 MS

4.6.19 10G Switch for HCI Nodes

Sl. No.	Detailed Technical Specifications
	Architecture
1.	Switch capacity - 1.4 Tbps or higher
2.	Switch forwarding rates – 1Bpps or higher
3.	10G SFP+- 24 ports populated with SFP module, scalable to 40 x 1/10G fiber ports
	40 Gig interface for uplink Populated with module – 4 Nos.
4.	Non-blocking switch architecture and modular operating system
	Switching features
5.	802.3ad based standard port/link aggregation, Jumbo frames, storm control
6.	Support at least 4000 VLAN and 150,000 MAC Address
7.	FIP snooping , Datacenter bridging exchange (DCBX) and IEEE 802.1Qbb (PFC) from day1
	Security
8.	802.1X Network Security and Radius/TACACS AAA authentication

9.	MAC Address filtering based on source and destination address
10.	support for various ACLs like port based, vlan based and L2- L4 ACL's
11.	Should have Control plane (DoS) protection
12.	The switch should support MACsec, SSH v1 & v2 and Dynamic ARP inspection
	Network Protocols
13.	Layer3 routing protocols like Static, RIP, OSPF, RIPnG, OSPFv3 from day 1 for the solution.
14.	The switch should support MPLS, L2 and L3 VPN and IPv6 Tunneling
	Quality of Service
15.	8 number of hardware queues per port
16.	DSCP, 802.1p
	Multicast
17.	IGMP v1,v2,v3, IGMP snooping, PIM SM and MSDP
	High Availability
18.	The switch should support ISSU and BFD
	Management
19.	SNMP v1, v2, v3, RMON/RMON-II enabled, SSH, telnet, GUI, Web management and should have dedicated Management port
20.	The switch should support CLI via console, telnet, or SSH and should have image rollback option.
21.	Switch should support port mirroring feature for monitoring network traffic of a particular port/VLAN.
22.	Switch should support Link Aggregation on two different switches
23.	Built-in real-time performance monitoring capabilities
24.	Power Supply: Switch should have internal Hot Swappable Redundant Power supply
25.	Cooling Fans: Should have redundant cooling FANS
26.	The switch should support NEBS
27.	Switch should be stackable/VPC/Equivalent (All accessories to be provided from day 1)
28.	The Switch should be EAL3/ NDPP certified

4.6.20 Video Wall, Video wall Management software and Controller

Video Display Wall

1 Size: 70” or more with complete configuration of (5 cubes x 2 cubes) with covered base. All cubes have to be of the exactly same size, configuration.

2 Resolution: Full high definition (1920 x 1080); aspect ratio of 16:9 Widescreen with LED light source.

3 Contrast Ratio: Dynamic contrast should be min 1,000,000:1 or better.

4 Colour & Brightness: Minimum 250 nits and should be adjustable for lower or even higher brightness requirements Uniformity: >=95% or better. Uniform brightness and colour. The colour calibration should be automatic and continuous operations for 24x7 operation.

5 LED Life: The light source lifetime of the LED in eco mode shall be 80,000 hours. This should be certified by the OEM.

6 Placement: The inter screen gap (bezel gap) should be <0.4 mm or batter and viewing angle should be 178 degree/178 degree (H/V)

7 Dust Prevention: Should be designed to avoid dust / Dust tight and resistant / Follow standards as prescribed by Government

8 Input & Control: Analog D-sub/Ethernet/Digital DVI/Digital HDMI with On Screen Display (OSD) and control by IP.

9 Display: shall provide image uniformity across the whole display area, real-time clear luminous view to share information between operators and decision makers, flicker free image on the Large Screen for seamless display. Remote viewing, the video wall content will be able to show live on any remote display. Mobile with IE (no apps). The display solution as well as the complete control ware including Display Controller, Central management SW & Web-streaming hardware as well as software should be of same Make/OEM

10 Capability: Ability of Cubes to display 4K, high definition (HD) and standard definition (SD) content, Low maintenance

11 Remote management through IP Remote management through IP for parameter adjustment. Each cube should have built-in web server

12 Access Rear only

13 Pixel clock Min 300 Mhz or higher

14 Heat Dissipation (Eco Mode) - Less Than450 btu/Hr Eco Mode

Video Wall Controller

1 Display controller: Controller to be able to control min 10 cubes and Controller to control Video wall in a matrix arrangement as per design and redundant for high availability and support Minimum1920 x 1080 or higher.

2 Platform: Pre-loaded 64-bit Operating System Windows / Linux / Equivalent, with recovery.

3 CPU:Min 16 GB RAM with Quad/Octa Core processor (3.4 Ghz) or higher and Redundant Hot Swappable HDD in RAID 1 Configuration.

4 Chassis Type: 19" Rack mount industrial chassis with adequate cooling fans and power supply on higher availability in hot swappable.

5 Network: Min 2 Network Ports and more.

6 RSS Feed: The controller should be able to show the RSS feed as required.

7 Scalability: The system should be able to add additional inputs as required in the future.

8 Keyboard & Mouse Extension: Keyboard and Mouse along with extendable mechanism up to display.

9 24 x 7 operation: The controller shall be designed for 24 x 7 operation and high availability.

10 The Video Wall and the Controller should be of the same make to ensure better performance and compatibility.

Video Wall Management Software

1 Display & Scaling: Display multiple sources anywhere on display up to any size

2 Input Management : All input sources can be displayed on the video wall in freely resizable and movable windows 3Ability to input, manage, and distribute visual content, including digital CCTV Video, web pages, CATV, workstation applications, and active screens from any networked/remote workstation.

3 Multi View Option: Multiple view of portions or regions of Desktop, Multiple application can view from single desktop. Ability to display multiple sources anywhere on video wall in any size. Ability to stretch, re-position, and resize any video source on any display device. Ability to treat the VDW as a single display. It shall act as a single canvas with no pixel separation.

4 Other features: SMTP support, Remote Control over LAN or VPN. Ability include an administrator role that shall be able to manage system configuration, sources, user groups, and user authentication. Alarm Alerts, Remote and Multiple concurrent client.

Ability to commands on wall level or cube level or a selection of cubes. Switching the entire display wall on or off. Setting all projection modules to a common brightness target, which can be either static (fixed) or dynamic to always achieve maximum (or minimum) common brightness between projection modules. Fine-tune colour of each cube. KVM Support and GUI.

4.6.21 Video Conferencing Solution

4.6.21.1 Multiparty Conference Unit

Sl. No	Minimum Requirements	Compliance (YES/NO)/Page NO
1	The MCU should be running on dedicated Hardware appliance with capacity of 25 ports and escapable to 50 Ports 1080p 30fps on IP in continuous presence mode and AES encryption in a single chassis without cascading/clustering from Day one.	
2	The MCU should be licensed for 25 ports HD 1080p 30fps and it should be capable to support minimum 25 session’s day one.	
3	All necessary hardware to support the above capacity needs to be supplied from day one in DC-DR.	
4	All the ports must be able to connect different sites at different bandwidths and protocols.	

5	H.264 AVC standard must be supported at the minimum to connect all the sites.	
6	The MCU should support room-based video end points, users joining from clients equal to number of ports of MCU. In case additional components are required for this functionality, all additional components required to have this functionality has to be included in the solution.	
7	The MCU should have the capability to host meetings with internal and external participants in a secure way such that it should co-exist with the enterprise security policies.	
8	The MCU should have components such as Scheduler as part of the offering from day one.	
9	Should support H.263/H.263+/H.263++, H.264AVC, H.264 SVC & H.264 High Profile.	
10	Should support video resolution from SD to Full HD to join into a conference.	
11	Along with the Support for basic algorithms like G.711 and G.722.1 the bridge should also support wideband Audio protocols like MPEG 4 AAC - LC/ MPEG 4 AAC –LD/equivalent.	
12	Must support the ability to allow Video conferencing devices, Clients on Mobile phones, Smart phones and Laptops to join into conference. These clients can be inside the WAN network or even on the Internet without a VPN.	
13	The bridge should support transcoding of different Audio/video Protocols.	
14	The bridge should have H.239/BFCP protocol for sending and receiving dual video streams (Presenter + Presentation).	
15	The bridge must also support advanced continuous presence such that the site that is "on-air" to be seen on a larger window and the other sites are seen in smaller quadrants.	
16	The bridge must be a secure Non-PC Hardware with a strong operating system. All the individual components of the centralized infrastructure should be quoted with a dedicated hardware to remove single point of failure.	
17	The bridge should support 128 Bit strong AES encryption for calls and H.235 for authentication.	
18	It should be possible for outside agencies (for state government, central government, police department, etc.) to join the bridge for multi-party video conference call securely over internet.	

19	They should be able to join the MCU using standards based VC endpoints using internet (as long as these endpoints are exposed to internet) securely.	
20	It should be possible to connect 50 such external endpoints/ locations concurrently at any given point of time.	
21	It should use secure firewall traversal technology.	
22	It should support any standards-compliant SIP or H.323 video conferencing endpoints.	
23	It should support for H.323 SIP Interworking.	
24	It should use standards based firewall traversal methods - H.460.18/19.	
25	The Complete Video Conference Infrastructure and room based Endpoints are from same OEM.	

4.6.21.2 Integrated Endpoint DICCC

Sl. No	Parameters	Minimum Specifications	COMPLIANCE (YES/NO)
1	Protocols	The system should be able to call any H.323 and SIP endpoint directly or indirectly. It should be possible to share content via BFCP and H.239. Endpoint should support the latest video coding standard either H.263, H.264SVC & H.264 High Profile. It should support Audio Coding G.722, G.722.1, G.711.	
2	Network	Endpoint should support bit rate atleast 6 Mbps or more on IP (H.323and SIP). Minimum 1 X Gigabit Ethernet: Should support 10/100/1000 BASET	
3	Main Video Resolution	Shall work in high definition video resolution of 1080p 60fps for live video for both Transmit and receive	
4	Camera	System equipped with 2 cameras so as to automatically zoom and focus on to the person speaking in the room. Codec & speaker track camera should be from same OEM. Zoom: Minimum 10x (optical) PTZ or better with PAN of +/- 100 Degrees and proposed Endpoint should support internal multipoint of 1+5 HD 720p through software license in future. Camera Pre-Sets should be minimum 10+.	

5	Video Inputs	System must have HD input/s for connecting 2 FHD cameras, as per the specifications, for speaker tracking. In addition, it should also have HDMI & VGA port for connecting PC/Laptop.	
6	Video Outputs	Minimum 2 x HDMI or similar or better to connect two displays. Additional Outputs are desirable.	
7	Audio Inputs	It should support 4 Omnidirectional Microphones. 3 microphones to be supplied from day one with the system.	
8	Encryption	AES 128 bit or more, TLS, SRTP, HTTPS or similar or better	
9	User Interface	Intuitive touch panel to operate the entire system	

4.6.21.3 Endpoint Other Location (Optional)

Sl. No.	Parameters	Minimum Specifications	COMPLIANCE (YES/NO)
1	Protocols	The system should be able to call any H.323 and SIP endpoint directly or indirectly. It should be possible to share content via BFCP and H.239. Endpoint should support the latest video coding standard either H.263, H.264SVC & H.264 High Profile. It should support Audio Coding G.722, G.722.1, G.711.	
2	Network	Endpoint should support bit rate atleast 6 Mbps or more on IP (H.323and SIP). Minimum 1 X Gigabit Ethernet: Should support 10/100/1000 BASET	
3	Main Video Resolution	Shall work in high definition video resolution of 1080p 60fps for live video for both Transmit and receive	
4	Camera	System support automatically zoom and focus on to the person speaking in the room. Codec & speaker track camera should be from same OEM. Zoom: Minimum 10x (optical) or better with PAN of +/- 100 Degrees and proposed Endpoint should support internal multipoint of 1+5 HD 720p through software license in future. Camera Pre-sets should be minimum 10+	
5	Video Inputs	System must have HD input/s for connecting 2 FHD cameras, as per the specifications, for speaker tracking.	

		In addition, it should also have HDMI & VGA port for connecting PC/Laptop.	
6	Video Outputs	Minimum 2 x HDMI or similar or better to connect two displays. Additional Outputs are desirable.	
7	Audio Inputs	It should support 4 Omnidirectional Microphones.	
8	Encryption	AES 128 bit or more, TLS, SRTP, HTTPS or similar or better	

4.6.22 IP Telephony

4.6.22.1 Contact Centre/Helpdesk for Integration with Emergency Services

Contact Centre/Helpdesk for Integration with Emergency Services		
S.N.	**Minimum Requirements**	**Compliance (Yes/No)**
1	The contact center solution shall include VoIP based EPBAX, IVRS, Automatic Call Distribution (ACD), Voice Logger Server among other hardware and software. Using the contact center solution, citizens can contact city administrator through the emergency communications system or through the contact center helpline number.	
2	Solution should be designed for atleast 30 agents	
3	IVRS should be modular and scalable in nature for easy expansion without requiring any change in the software.	
4	The contact center solution should be able to route voice/ VOIP calls from centralized Interactive Voice Response System (IVRS) to respective call center (s) along with interaction history of the calling party.	
5	The callers should be able to access the various services through state-of-art centralized integrated Interactive Voice Response System (IVRS).	
6	IVRS should support various means of Alarm indications in case of system failures, e.g. Functional error, missing voice message prompt, etc., and shall generate error Logs.	
7	IVRS shall be able to get information /text/data from databases, convert to voice, and speaks it back to the caller in relevant/desired language. TTS required from Day-1 for English and Hindi. (TTS will be used for text to speech along with IVR application.	

8	Solution should provide pre-integration with industry standard IVRS servers and enhance routing & screen pop by passing forward the information. Interactive Voice Response System (IVRS) should -	
	a. play welcome messages to callers Prompts to press and collect DTMF digits	
	b. be able to integrate with backend database for self-service, as and when required	
	c. Offer GUI based tool to be provided for designing the IVR and ACD call flow.	
	d. support Voice XML for TTS, and DTMF call flows	
	e. be able to Read data from HTTP and XML Pages be able to run outbound campaigns.	
9	**Automatic call distribution (ACD) solution should -**	
	a. be able to route the call to any remote call center agent using IP phones	
	b. have an ability to queue or hold the call for an agent if none is immediately available	
	c. have an ability to keep the callers informed as to the status of the call and providing information to callers while they wait in queue	
	d. be able to perform prioritized call routing	
	e. be highly available with active standby and seamless failover in case of main server failure	
	f. support skill-based routing and it should be possible to put all the agents in to a single skill group and different skill groups	
	g. support routing of incoming calls based upon caller input to menus, real-time queue statistics, time of day, day of week, ANI, dialled number etc.	
	h. support call routing based on longest available agent, circular agent selection algorithms	
	i. maintain log of all services offered which can be used for audit and analysis purpose.	
	j. Support the playing of customizable queuing announcements based upon the skill group that the call is being queued to, including announcements related to position in queue and expected delay	

	k. Allow agents to chat with other Agents or supervisor from the Agent desktop software	
	l. Allow supervisor to see the real-time status of agents, supervisors should be able to make agent ready or logout from the supervisor desktop	
	m. Support Queuing of calls and playing different prompts depending on the type of call and time in the queue	
10	System shall provide for 100% recording of calls using a call logger. The recording shall contain detailed call information and the solution must provide advanced searching capabilities.	
11	Solution should have automatic identification of incoming number based on landline and mobile number mapping	
12	Solution should support call recording mapped to incident tickets	
13	Solution should offer customizable agent and supervisor desktop layout	
14	Solution should offer Inbound and outbound capability	
15	Solution should provide facilities for outbound calling list management, and software based predictive or preview dialling. Call routing should be supported basis on skill-based routing.	
16	The agent's desktop shall have an application which shall fulfil the following functionalities:	
	It should provide consistent agent interface across multiple media types like fax, SMS, telephone, email, and web call back.	
	The agent's desktop should have a "soft-phone" – an application that enables standard telephony functions through a GUI.	
	It should provide the agents with a help-desk functionality to guide the agents to answer a specific query intelligently.	
	It should also provide an easy access to agents to previous similar query which was answered successfully.	
	It should also be possible to identify a request to be a similar request made earlier.	
	It should be possible for agents to mark a query as complex/typical and put in to database for future reference by other agents.	
	It should be possible for agents to escalate the query.	

17	System should be able to integrate with e–mail / SMS gateway so that appropriate messages can be sent to the relevant stakeholders after the interaction and any updates thereon.	
18	Should intelligently and automatically responds to email inquiries or routes inquires with skills-based routing discipline to agents	
19	Live data reporting gadgets	
20	Speed dial in IP phones	
21	Solution should provide CTI services such as:	
	CTI link should allow a computer application to acquire control of the agent resources on the IP EPABX & change state of the agent phone through commands on the CTI link.	
	CTI link should pass events & information of agent states & changes in agent states as well as incoming calls to the computer applications.	
	CTI link should allow a computer application to take control of the call flow inside the IP EPABX & also allow the computer application to decide the most suitable action / agent for an incoming call.	
	Automatic display (screen pop) of information concerning a user/customer on the call agent	
	Screen prior to taking the call based on ANI, DNIS or IVR data	
	Synchronized transfer of the data and the call to the call centre agent	
	Transfer of data corresponding to any query raised by any agent regarding a query raised by	
	➢ A caller whose call is being attended by the agent	
	➢ Call routing facilities such as business rule-based routing, skills-based routing etc.	
22	Supervisor Module	
	The call centre should provide a graphical console application program for the supervisor's workstation. This position shall facilitate the following features: -	
	Any supervisor shall be able to monitor or control any group in the call Centre	
	It shall show the live activity of each agent in details as well as in a summarized fashion including information like total number of calls received, calls answered, average response time etc.	

	Supervisor console shall also graphically display live status of the call session summary, number of call waiting in the queue, call traffic etc.	
	Live status of the group shall be shown, including waiting calls and calls being answered currently.	
	Access to the supervisor console shall be restricted.	
	It shall be possible for a supervisor to attend calls whenever necessary.	
23	Reporting:	
	System to provide report of IVR Application Performance Analysis, Call by Call details for all the calls, Traffic analysis reports etc.	
	Reporting platform to support Agent level reports, Agent login, logout report, report on agent state changes	
	Queue reports, Abandon call reports all the reports should be summary, tabular and detailed report format to be available for the agents.	
	Reporting platform to support custom reports using a combination of the Crystal Reports Developer's Toolkit and SQL stored procedures.	
	Developer's Toolkit and SQL stored procedures.	
	Users of the Historical Reports should be able to perform the following functions View, print, and save reports. Sort and filter reports, Send scheduled reports to a file or to a printer. Export reports in a variety of formats, including PDF, RTF, XML, and CSV.	
24	Solution should offer audit trail with the following features -	
	Solution should have a comprehensive audit trail detailing every user activity including system/security administrators with before and after image	
	Audit trails presented by the system shall be very detailed with all the related fields, such as User ID, time log, changes made before and after, Machines ID etc.	
	It shall have the facility to generate security report(s) and audit the whole process from logs reports at any future date. The system shall have complete audit trail of any changes to the system e.g. alert generated, system configuration etc.	
	System shall not allow audit log to be deleted and any attempts to delete must be logged.	

	System shall have at a minimum following standard report:	
	List of users, user privileges and status	
	User sign-off and sign-on	
	User violation – unsuccessful logon attempts	
	User additions, amendments and deletions with before & after image	
25	All contact center related components including ACD, PABX, Gateways, Recording, CTI, softphone, hard phones, Citizen Centric Services etc. must be from same OEM.	
26	Solution should support inbound (Voice, MM) & outbound (Preview) blended agents from day	
27	Solution should support Browser-based Agent Controls if required.	
28	The call center solution should have been implemented in minimum 2 projects of Emergency handling over 50,000 calls per day in India. Documentation proof should be submitted as part of the tender submission	
29	Chat Bot: -	
	a. The solution should provide conversational chat solution wherein citizens can interact with bot for simple enquires to complex form submission services as well. It should allow citizens to just type their question into the chat window and get an instant response from a virtual digital assistant and even fill up some online forms. when citizens enquire cannot be handled by bot application, the same chat can be escalated to Contact/Helpdesk Centre with previous chat history so that citizen enquiry can be handled by live agent without losing the context of the previously happened conversation. Citizen can ask transfer to an agent anytime in the conversation. Since the Citizen Centric Services needs to handle the chat or call to the live agent, the call center agent and Citizen Centric Services should be closely coupled and preference would be given to the same call center as that of Citizen Centric Services.	
	b. Chat bot should be able to automate services such as birth registration, NOC request, death registration, property tax and water tax enquiry and payments. It should begin with 10 forms and scalable to 30 forms. The same chat transcript will be emailed to the citizen after the chat completion.	
	c. Chat bot should be able to handle 100 concurrent sessions.	
	d. Chat bot should be web based (html 5) and can be invoked using SMS, IVR or mobile web URL.	

	e. Citizen Centric Services should be able to handle text-based interaction with user in Indian English and Hindi.	
	f. Chat bot should be able to push forms, widgets and files to the users.	
	g. Chat bot should be able to read data from back end applications using web services, JDBC/ODBC and REST interfaces. In case chat bot is unable to handle user query, it should transfer the session to contact center agent with the context and history of the conversation. Since the Citizen Centric Services is closely integrated with call center technology, preference will be given to the same OEM of Citizen Centric Services as that of call center. The application should be "Pre-Tested/Running" with the provided ACD platform for removing any interop related issues. The interop certification should be incorporated as part of the tender technical from both ACD and application provider.	
	Citizen Notification System (CNS):	
30	a. System must Support Voice Call Notification – Office Phone, Cell Phone, Home Phone	
	b. System must support SMS, Email, Speakers / Paging	
31	System must offer Web based self-service management	
32	It should be possible by administrator to define attributes (location, role, etc.) for users	
33	It should support CSV File Upload for contacts	
34	System should support One-way Notification & ACK	
35	System Admin must be able to define Notification Scenario for quick management	
36	System admin must be able to do Message Mgmt. (Pre-recorded, "record on the fly", Text-To-Speech)	
37	User/Group Profile Mgmt.	
38	Escalation Configuration	
39	Security Configuration	
40	Message Broadcast (Priority)	
41	Audit logs and Reports (Web and PDF formats), Data and Analytics	

42	System must be able to reach 500 people with 10 minutes for a 30 second call with a ring time of 30 seconds	
43	Audit logs and Reports (Web and PDF formats), Data and Analytics	
44	The application should be “Pre-Tested/Running” with the provided ACD platform for removing any interop related issues. The interop certification should be incorporated as part of the tender technical from both ACD and application provider	
45	System must be able to reach 500 people with 10 minutes for a 30 second call with a ring time of 30 seconds	
46	The application should be “Pre-Tested/Running” with the provided ACD platform for removing any interop related issues. The interop certification should be incorporated as part of the tender technical from both ACD and application provider	
	Citizen Complaint services:	
47	After the citizen reaches out to the call center, he registers a complain over the phone and a ticket incident is generated. For the exact location of incident an SMS can be shared with the citizen or manual entry can be done.	
48	The user can click on the SMS to share the exact location of the faulty road, fallen tree / pipe, garbage collection etc. services.	
49	The location shared by the user / citizen should be capable of being shared with any number specified or even with the dispatcher for exact location.	
50	Once the dispatcher has the location, he should be able to use google maps to navigate to the exact location or pin point it on the map.	
51	User shall have the capability to share upload a picture / video of the incident with this application.	
52	The shared file should be tagged and stored with the same incident for future reference.	
53	The call center agent who answered the call shall have the capability to send automatic mail of the incident to the respective authorities.	

54	The application should be “Pre-Tested/Running” with the provided ACD platform for removing any interop related issues. The interop certification should be incorporated as part of the tender technical from both ACD and application provider	

4.6.22.2 IP PBX (Call Control System)

Sl. No.	Minimum Specifications	Compliance (Yes/No)
1	The IP telephony system should be a converged communication System with ability to run TDM and IP on the same platform using same software load based on server and Gateway architecture	
2	The single IP PBX system should be scalable to support atleast 500 stations (any mix/percentage of Analog/IP) to achieve the future capacity	
3	Proposed Solution should support remote site survivability on local gateways and the survivable system should provide all the telephony features as of main site. Survivability features and options that allow gateways to continue operating even if the primary server fails or in the event a WAN failure affects communications between the gateway and the IP PBX.	
4	System should support High availability and seamless failover from primary server to secondary server. It should allow the administrator to make configuration changes even when primary server is down.	
5	The system should be based on server gateway architecture with external server running on Linux OS. No card-based processor systems should be quoted	
6	The voice network architecture and call control functionality should be based on SIP	
7	The call control system should be fully redundant solution with no single point of failure & should provide 1:1 redundancy.	
8	The communication server and gateway should support IP V6 from day one so as to be future proof	
9	The entire solution (IP PBX, its hardware, IP Phones, Recording, Voice Gateway) should be from a single OEM	
	Support for call-processing and call-control	
10	Should support signalling standards/Protocols – SIP, H.323, Q Sig, etc.	
11	Voice Codec support - G.711, G.729, G.729ab, g.722, etc.	

12	The System should have GUI support web-based management console Security	
13	The protection of signalling connections over IP by means of authentication, Integrity and encryption should be carried out using TLS	
14	Proposed system should support SRTP for media encryption and signalling encryption by TLS	
15	Secure HTTP support for Call Server Administration, Serviceability, User Pages, and Call Detail Record Analysis and Reporting Tool. Should support Secure Sockets Layer (SSL) for directory	
16	The administrator logging on to the call control server needs to authenticate by suitable mechanism such as User Login Information and Passwords/ Radius Server	
17	Voice gateway to be provided with 1 PRI card scalable to 3 PRI in future for PSTN (PRI) line termination.	

4.6.22.3 IP Phones

IP Phones			
Sl. No	**Parameter**	**Minimum Specifications**	**Compliance (Yes/No)**
1	Display	2-line or more, Monochrome display for viewing features like messages, directory	
2	Integral switch	10/100 Mbps for a direct connection to a 10/100BASE-T Ethernet network through an RJ-45 interface	
3	Speaker Phone	Yes	
4	Headset	Wired (Kevlar cord), Cushion Padded Dual Ear-Speaker, dual microphone mouthpiece with noise cancellation, port compatibility with IP Phone. Headset should be light in weight.	
5	VoIP Protocol	SIP V2 VoIP supported	
6	POE	IEEE 802.3af or better and AC Power Adapter (Option)	
7	Supported Protocols	SNMP, DHCP, DNS	

8	Codecs	G.711, G.722, G.729 including handset and speakerphone	
9	Speaker Phone	Full duplex speaker phone with echo cancellation	
		Speaker on/off button, microphone mute	
10	Volume control	Easy decibel level adjustment for speaker phone, handset and ringer	
11	Phonebook/ Address book	Minimum 100 contacts	
12	Call Logs	Access to missed, received, and placed calls. (Minimum 20 overall)	
13	Clock	Time and Date on display	
14	Ringer	Selectable Ringer tone	
15	Directory Access	Able to integrate with LDAP standard directory	
16	QoS	QoS mechanism through 802.1p/q	

4.6.22.4 Emergency Notification System

Sl. no.	Notification System	Complied (Yes/NO)
1	Notification Formats	
	System must Support Voice Call Notification – Office Phone, Cell Phone, Home Phone	
	System must support SMS, Email, Speakers / Paging	
2	User Contact Lists	
	System must offer Web based self-service management	
	It should be possible by administrator to define attributes (location, role, etc.) for users	
	It should support CSV File Upload for contacts	
3	Message Configurations	
	System should support One-way Notification & ACK	

	System should be able to notify and respond and Notify to Conference to all stake holders	
	System should support auto Escalation or cascading chains of notifications whenever needed	
4	Administration Portal (Web Application)	
	User/Group Mgmt.	
	Partition Mgmt for different departments	
	Conferencing Configuration	
	Security Configuration	
	Channel (Device) Configuration & Mgmt.	
	Communications Resource Mgmt.	
	Broadcast Trigger Configuration	
	Inbound Call Trigger Configuration	
	Message Inbox Configuration	
5	Operations Portal (Web Application)	
	System Admin must be able to define Notification Scenario for quick management	
	System admin must be able to do Message Mgmt. (Pre-recorded, “record on the fly”, Text-To-Speech)	
	User / Group Profile Mgmt.	
	Escalation Configuration	
	Security Configuration	
	Message Broadcast (Priority)	
	Audit logs and Reports (Web and PDF formats), Data and Analytics	
	System must be able to reach 500 people within 10 minutes to play 30 second voice announcements.	

4.6.22.5 Unified Collaboration Solution/UC Client

S no	**Minimum Specifications**	**COMPLIANCE (YES/NO)**

1	The Collaboration Client application must enable streamline communications and enhances productivity with integrated presence, IM, voice, voice messaging, desktop sharing, and conferencing capabilities.	
2	The Collaboration solution should have capability to integrate with Emergency Response/Radio Dispatch system.	
3	The UC application shall have a friendly, intuitive and easy to use graphical interface that informs in real time the multiple states of presence using the user-defined list.	
4	On the UC Client The presence shall use icons and colors and shall include at least: On-Line Telephony	
5	The solution must be able to support one-to-one and multi-party messaging	
6	It must support ability to send Multimedia (Text, Voice and photo) messages between users	
7	It should support multiple devices like Windows Desktop, Android and IOS on iPhones and iPads.	

4.6.23 Unified Management

Sr. No	Parameter	Minimum Specification
1.	**Automation**	Solution should provide automation and orchestration solution for automated delivery of IaaS, PaaS, XaaS/ SaaS services for Smart City applications so that when VM/app is created it should automatically get the required virtualized compute, storage, switching, routing, firewall, load balancing services without any manual intervention. All compute, network, storage, security, load balancing policies must follow the life cycle of VM and movement within and across DC & DR.
2.	**Policy defined Infrastructure**	Solution should be built using programmable & policy defined infrastructure components which should be independent of underlying hardware components and use standard x86 servers, storage, switches from any OEM make and model.
3.	**Auto-scale**	Solution must provide auto scale so that in case of increase in load/connections/users. Additional VMs should be automatically created with all network, security and load balancing policies. Integration required from cloud portal, orchestration, virtualization, virtual network, security and load balancing should be done to achieve this functionality.

4.	**Operations & Management**	Solution must provide cloud operations layer integrated with automation layer which provides proactive monitoring, alerts, management, capacity planning, performance management.
5.	**Monitoring**	• Solution should monitor utilization of running VMs and should reclaim resources from idle VMs and allocate to other VMs in automated fashion. • The solution capacity analytics should provide "What If" scenarios to eliminate the need for spreadsheets, scripts and rules of thumb to eliminate time-consuming problem resolution processes through automated root cause analysis • Solution should provide automated workflow triggers which would let admins associate workflows created in Orchestrator layer with Operations alerts. For example, these workflows can automatically delete old VM snapshots when available capacity falls below a critical threshold or add resources when workload demands are rising above normal. Automated workflows help reduce Mean time to incident (MTTI) and mean time to resolution (MTTR)
6.	**Dashboard & Reporting**	Solution should provide monitoring and management of complete virtualized infrastructure with prebuilt and configurable operations dashboards to provide real-time insight into infrastructure behavior, upcoming problems, and opportunities for efficiency improvements.

Server Virtualization

Sl. no	Parameter	Minimum Specification
1.	**Bare Metal Solution**	Sits directly on the bare metal server hardware with no dependence on a general-purpose OS for greater reliability & security and should be Leaders in OEM
2.	**Guest OS Support**	Windows client, Windows Server, Linux (at least Red Hat, SUSE, Ubuntu and CentOS, Solaris x86) etc.
3.	**VM Live Migration**	Live Virtual Machine migration between different generations of CPUs in the same cluster and without the need for shared storage option and long distances from one site to another (atleast 150 milliseconds round trip time) with no disruption to users or loss of services, eliminating the need to schedule application downtime or business downtime.
4.	**Storage Live Migration**	Live migration of VM disk from one storage array to another without any VM downtime. Support this migration from one storage protocol to another eg: FC, NFS, iSCSI, DAS.

5.	**High Availability**	• Proactive High availability capability that utilizes server health information and migrates VMs from degraded hosts before problem occurs • Migration of VMs in case one server fails all the Virtual machines running on that server shall be able to migrate to another physical server running same virtualization software. • The solution should have single reboot to dramatically reduce the upgrade times by skipping a host reset and also help to reduce patching and upgrade times by rebooting the hypervisor without rebooting the physical host, skipping time-consuming hardware initialization
6.	**Always Available**	Zero downtime, Zero data loss and continuous availability for the applications running in virtual machines in the event of physical host failure, without the cost and complexity of traditional hardware or software clustering solutions.
7.	**Resource Addition**	Add CPU, Memory & devices to virtual machines on the fly when needed, without disruption or downtime of working VMs for both windows and Linux based VMs.
8.	**Resource Scheduler**	Create a cluster out of multiple storage datastores and automate load balancing by using storage characteristics to determine the best place for a virtual machine's data to reside, both when it is created and when it is used over time.
9.	**Security**	• VM-level encryption with no modifications in guest OS to protects unauthorized data access both at-rest and in-motion and also provides secure boot for protection for both the hypervisor and guest operating system by ensuring images have not been tampered with and preventing loading of unauthorized components. • Integration of 3rd party endpoint security to secure the virtual machines with offloaded antivirus, antimalware, firewall and hips solutions without the need for agents inside the virtual machines.
10.	**Storage support**	Support boot from iSCSI, FCoE, and Fibre Channel SAN. Integration with Storage API's providing integration with supported third-party data protection, multi-pathing and disk array solutions.
11.	**Virtual Switch**	• Span across a virtual datacenter and multiple hosts should be able to connect to it. This will simplify and enhance virtual-machine networking in virtualized environments and enables those environments to use third-party distributed virtual switches. • In-built enhanced host-level packet capture tool which will provide functionalities like SPAN, RSPAN, ERSPAN and will capture traffic at uplink, virtual switch port and virtual NIC level. It

		should also be able to capture dropped packets and trace the path of a packet with time stamp details.
12.	**VM based Replication**	Efficient array-agnostic replication of virtual machine data over the LAN or WAN. This Replication should simplify management enabling replication at the virtual machine level and enabling RPOs as low as 15 minutes.
13.	**VM Backup**	Simple and cost-effective backup and recovery for virtual machines which should allow admins to back up virtual machine data to disk without the need of agents and this backup solution should have built-in variable length de-duplication capability.
	Disaster Recovery Automation	• Solution should provide DR automation solution delivered from virtualization manager console for automated failover, failback and recovery of application VMs in proper sequence to other data center with single click • Solution should provide solution to perform non-disruptive DR drill/testing of recovery plan for full and selected applications every six months without impacting production applications running in primary environment.
14.	**OEM Support**	Direct OEM 24x7x365 days with unlimited incident support and 30mins or less response time including the unlimited upgrades and updates.
15.	**Operations Management**	• It should include proactive smart alerts with self-learning performance analytics Capabilities with Prebuilt and configurable operations dashboards to provide real-time insight into infrastructure behavior, upcoming problems, and opportunities for efficiency improvements. • Capacity analytics which can identify over-provisioned resources so they can be right-sized and "What If" scenarios to eliminate the need for spreadsheets, scripts and rules of thumb, as well as Real-time, integrated dashboards of performance and capacity to enable a proactive management approach and help ensure SLAs are met • Automated workflow triggers which would let admins associate workflows created in Orchestrator layer with Operations alerts. For example, these workflows can automatically delete old VM snapshots when available capacity falls below a critical threshold or add resources when workload demands are rising above normal.

Note:- MSI has propose hybrid solution of HCI (min 70%) and Non- HCI as per their application requirement.

4.6.24 Integrated Data centre infrastructure

This specification covers intelligent integrated/inbuilt infrastructure, standalone system design, engineering, manufacture, assembly, testing at manufacturer's works, supply, delivery at site, unloading, handling, proper storage at site, erection, testing and commissioning at site of complete infrastructure for the proposed Data Centre to be installed by MSI as per detailed specification, complete with all accessories required for efficient and trouble free operations.

The detail specifications of the intelligent integrated/inbuilt infrastructure, standalone system shall be in adherence to data center guidelines thus shall be composed of dual active power and cooling distribution paths, but only one path active. Shall have redundant components.

The Intelligent Integrated Infrastructure essentially includes internal redundant or backup power supplies, environmental controls (e.g., precision air conditioning, fire suppression, smoke detection, Water leak detection, humidity sensor etc.), security devices etc. Critical systems like UPS and Precision Air-conditioning system will have N+N topology respectively

The Intelligent integrated infrastructure shall be having foot print approximately 17 Sq. Mtr which shall have min 117 U usable space (min 4 racks), to accommodate IT and network equipment & devices. This footprint should include separate panel housing fire suppression and power distribution preferably.

The Intelligent integrated infrastructure would provide many functionality and some of the key functionalities are Cold Contained Front Aisle & Rear Contained Hot Aisle, insulation, remote management and single point of service.

The Intelligent integrated Infrastructure shall have following components:-

- Precision Air conditioner with variable capacity cooling, heater and humidifier to cater IT load approximately 40 KVA and in N+N topology for total 4 racks.
- 2 x 20 KVA – 2 Sets rack mount UPS with P.F. Atleast 0.9 & efficiency more than 92% ~94% - 2 numbers. There should be 10 min battery back-up. UPS & Battery should be mounted inside the cabinet only.
- UPS, Cooling and monitoring system should be from single OEM
- Novec 1230 Gas based fire suppression system as per NFPA guidelines
- Smoke detectors, water leaks detection system, temperature & humidity sensor, door sensor, and alarm beacon.
- 42 U racks of dimension 600 mm x 1000 mm 4 numbers.
- Monitoring system – capable for Email alerts
- Biometric access control system which should be control by access control panel.
- 32A Vertical Rack mount PDU of type IEC C13 & IEC C19 combination, each rack shall have two such PDU's.
- Electrical system with essential MCB/MCCB.

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

Detailed specs of components

Uninterrupted Power Supply (UPS) System

Configuration: 2 x 20KVA – 2 Nos.

General Description:

Supply, install, test and commissioning of two numbers of true online, double conversion, high efficiency, high power factor Uninterruptible Power Systems (UPS) rated at 2 x 20 KVA – 2 Sets with battery backup support for 5 minutes on full load. The backup batteries should be supplied with the necessary arrangements to mount inside the cabinet.

Scope:

The scope shall include design, supply, installation, testing and commissioning of the complete UPS system and related accessories including:

1. All Server racks will get power feed from two independent 2 x 20 KVA UPS systems to ensure redundancy.
2. All systems should be tested in factory as per the manufactures recommended procedure for all operating parameters and the test results should be provided during the installation.
3. Delivery at site, unloading, handling, installation of complete system including interconnection from the UPS system to batteries and to input / output panels switches. All interconnections shall be done using multi-strand Flexible Copper conductor cables of appropriate sizes.
4. Scope includes battery bank connections and providing safety barriers for all bus bars and cable connection leads on battery racks.
5. Energizing of UPS and Battery bank commissioning.
6. UPS control parameters setting and complete testing of system on load.
7. Service backup by engineer till system is fully operational and subsequently training is to be provided to the concerned persons of the Institute.
8. Any upgrade of the system hardware and associated other software during the warranty period should be supplied at free of charge.
9. Acceptance tests will be carried out after installation and the systems will be taken over only after successful completion of the acceptance tests.
10. Operation and service manuals of the systems containing technical/Electronic drawings / circuit diagrams complete in all respects should be supplied.

Specification / features of the Each UPS system are as follows:

- Widest input range. -
- Double conversion and IGBT technology.
- Full IGBT Rectifier/Battery charger
- IGBT based Inverter
- Batteries to support 10minutes full load backup. (Extra backup with external batteries with charger)
- Facility for remote viewing
- Easy to expand in a cost effective way

20 KVA/ 10 KVA UPS other Technical Specification:

OUTPUT PARAMETERS	
Capacity	20kVA/18kW , 10 kVA/9kW (0-30deg C) / 16.2kW (30-35 deg C) / 14.4kW (35-40 deg C)
Power Factor	0.9 at 30Deg C
Configuration	3- ph, 3-wire,N +PE / 1 phase, L-N + PE
Voltage Regulation	(+/- 1%)

Voltage THD	<=2% - Linear load <=5% - Non linear load
Frequency	50/ 60Hz
Frequency Regulation (synchronized with bypass)	(+/- 2 Hz)
Slew Rate	0.2Hz/s
Crest Factor	3:1 max.
Recovery time	60 millisecond
Over load capacity	< 105% - continuous; 105-125% - < 5 min; 125-150% -< 1 min >150% - < 200ms (after overload shifted to bypass)
AC-AC Efficiency	>93% atleast 94%
Transfer time - Mains to battery	0 millisecond
Transfer time - Inverter to bypass - Synchronization mode	1 millisecond
Parallel Redundancy	N+N
INPUT PARAMETERS	
Configuration	3- ph, 3-wire,N +PE
Nominal Voltage	380/400/415V
Input Voltage range	3 Phase 228Vac-478Vac
Frequency	50/60 Hz
Frequency range- Hz	40 to 70 Hz at full load
Power Factor	>0.99 at full load
BYPASS	
Voltage Range	+15% -20%
Frequency	50/ 60Hz
Frequency Range	+/-20%
BATTERY PARAMETERS	
Type	SMF
No. of battery blocks	32-40
Battery Voltage	384-480Vdc
ENVIRONMENTAL PARAMETERS	

Operating temperature	0 to 40 deg. Centigrade
Storage temperature	-40 to 70 deg. Centigrade
Relative Humidity	95% RH non condensing
Altitude	2000 meters
Temperature de-rating	30-40deg de-rating
Altitude de-rating	< 2000m; derating according to GB/T3859.2 when higher than 2000m
Noise level	<58db
MECHANICAL PARAMETERS	
Ventilation	Forced - Air cooled
Cable Entry	terminal block
Color / Panel finish	EG7021
Protection	IP20
Parallel	3+1, Built in Provision
LBS	Built in
MONITORING SOFTWARE	SNMP, Dry contact card, site monitoring / shutdown for multiple servers

Installation:

1. The entire system shall be installed as per manufacturer's recommendations & instructions including all interconnections for supply & control circuits.
2. All components shall be clearly identified using labels including battery cells individually.
3. Services of authorized representative or manufacturer for supervision of installation, connections, testing, & adjustments shall be provided.

Testing & Commissioning:

1. Under supervision of manufacturer's representative all system functions, operations, protective features shall be checked & present to ensure compliance or specifications.
2. Test the system as per recommendations & test listed below using pre-calibrated instruments.

Load simulation:

1. Simulation of malfunctions to verify protective device operations.
2. Duration of supply on emergency. Low battery voltage alarm & shutdown, transfer & restoration of normal supply.

Remote status & alarm tests:

In case of test any shortfalls / faults, the same shall be rectified & test procedure shall be again repeated to establish satisfactory performance.

Cleaning:

On completion of installation, testing of the system all components, cabinets etc. shall be cleaned & unwanted material, debris shall be removed from site. Scratches dents if any shall be cleaned & touched up to match the original finish.

Drawings & Manuals for UPS:

Following drawings & manuals/information shall be submitted in at least THREE copies at appropriate stages & for handing over the system. Manufacturer's data for product, features, components & performance along with the offer Operation & maintenance manual with List of recommended spares & replacement components. Detail operating instructions covering operations in normal & abnormal conditions. Shop drawings showing detail fabrication, assembly of components, internal & interconnecting wiring, dimensions, plans & views, installation details access & clearance etc. for approval. Product certificates for Brought out items. Factory test certificates & Inspection report. Field test reports.

Precision Air Conditioning System

Configuration:

Supply, installation, testing and commissioning of DX Type Air-conditioning Units designed specifically for high sensible heat ratio with variable cooling technique to match the low latent loads of systems to be installed in the integrated cabinet for effective and uniform distribution of cooling. Cold air will be supplied to the cold aisle containment of the integrated cabinet and the hot air will be taken from the hot aisle containment of the cabinet.

GENERAL

Cooling Circuits

1. Direct expansion
2. One refrigeration circuit, incorporating a high efficiency, fully hermetic variable capacity compressor with crankcase heater, safety valve, filter drier, moisture indicating sight glass, liquid line solenoid valve and an externally equalized expansion valve.
3. Each compressor is equipped with pre-set high and low pressure switches for protection against high condensing and low evaporating temperatures. The low pressure switch features an automatic reset (with an adjustable delay for winter start-up).
4. The unit shall be provided with additional protection against high ambient temperature. When the temperature goes over the design conditions, the unit remains in operation with partial load (20% decrease against required). If such protection is not sufficient High Pressure switch shall generate an high pressure alarm and the unit shuts down - manual reset shall be required.
5. The inclined evaporator coil is manufactured from copper tubes, mechanically bonded to hydrophilic painted aluminium fins, with a stainless steel condensate drain pan. The large face area/low velocity coil allows precise control of temperature and humidity* during cooling and dehumidification*, and is designed to optimise fluid velocity and minimise pressure drop.

6. The moisture indicating sight glass, liquid line solenoid valve and expansion valve for each circuit are mounted in a service compartment, isolated from the air stream, to allow checking and adjustment while the unit is in operation.

Fan section

Units is offered with two plug EC Direct Drive Fan, High efficiency, external rotor electronically commutated (EC) motor with integrated electronics, True soft start characteristics (inrush current lower than operating current), Backward curve, corrosion resistant aluminium fan wheel, Maintenance free design and construction. The fan section shall be designed for higher air flow. The fan shall be protected over temperature of motor, electronics, locked rotor protection, short circuit of motor output. Fans are IP54, Protection class F.

Cabinet and Frame

The unit shall be powder painted panels with ½" (or 10mm) insulation. A hinged control access panel opens to a second front panel which is a protection enclosure for high voltage components. The frame is painted with a powder coat finish to protect against corrosion. The unit is totally front and rear accessible including any component removal.

Air Filtration

1. The filter cells are made of two deep pleated 4" filters rated MERV8 following ASHRAE 52.2 (45% by ASHRAE 52.1) or G4 following EN779, located within the cabinet, and accessible from the rear of the unit. Frame of the filter shall be made of galvanized steel.
2. Optional filters are available: MERV11 following ASHRAE 52.2-1999 (45% by ASHRAE 52.1-1992) or F5 following EN779.
3. Clogged filter alarm is available for standard and for optional filter. It sends a visual alarm to display.

Refrigerant

All units equipped with direct expansion circuit are suitable for R410A refrigerant.

Microprocessor Controller

1. Air conditioning models should be controlled by microprocessor based controller. It can be programmed to control the function of every device within the unit via I/O.
2. The controller allows setting and monitoring of the room parameters. Unit utilizes multiple temperature sensors placed at the rack inlet, to ensure management and control of temperature by rack. Each unit should be connected atleast 10 Sensors.
3. The controller should allow setting and monitoring of the following space parameters:

a. Air inlet Temperature
b. Air supply Temperature (remote sensors at rack inlet)
c. Return Temperature set-point
d. Supply Temperature set-point
e. Return Temperature band
f. Supply Temperature band
g. Humidity (inlet)
h. Humidity set-point
i. Humidity band
j. Rack Min, Max and Average temperature

k. The example of available warnings / alarms:
l. High supply temperature
m. Low supply temperature
n. High return humidity
o. Low return humidity
p. Loss of airflow
q. Compressor Low Pressure
r. Compressor High Pressure
s. Electrical heater high temperature (When applicable)
t. Clogged filter
u. Customer input (No 4 inputs)
v. LP transducer fail
w. Call service (customer input)
x. High temperature (customer input)
y. Unit hours exceeded
z. Compressor hours exceed
aa. Humidifier hours exceed
bb. Supply sensor failure
cc. Network failure
dd. Humidifier problem
ee. Digital scroll high temperature
ff. Smoke detected
gg. Fire alarm
hh. Rack sensor failure

4. Following features should be incorporated in the controller:

a. Status Report of the latest 400 event-messages of the unit.

b. Input for remote on-off and volt-free contacts for simple remote monitoring of low and high priority alarms: high/low temperature, high/low refrigerant pressure, fan/control failure, compressor/control failure and others are available

c. LAN management: functions provided as standard include stand-by (in case of failure of the unit in operation, the second one starts automatically), and automatic rotation. At least one unit in the LAN has to be equipped with ColdFire large display.

d. Automatic restart is provided after a power failure.

Monitoring

1. There should be SNMP and HTTP/Web-management capability for enhanced communications and control of HPM systems. The cards make use of an Ethernet network (10/100Mbit) to monitor and control a wide range of operating parameters, alarms and notifications thanks to a standard web browser (Internet Explorer). The card utilizes standard Ethernet cables (different cable lengths are available for your convenience on the Connectivity price list).

2. The unit shall also include input volt-free contacts for simple remote monitoring of low and high priority alarms: high/low temperature, high/low refrigerant pressure, fan/control failure, compressor/control failure and others are available.

Condenser

The condenser should be with fan speed controller designed & set for usages of R410A refrigerant. Condenser should be worked -20 deg C to 46 deg C ambient temperature. The condenser frame shall be made up of a sturdy GI structure. The motorized fan shall be IP54, protection class F.

Additional Features - Humidifier

The unit is fitted with an canister type steam humidifier suitable for use with water of varying degrees of hardness, provided that the water is not treated or demineralised (Conductivity range 125-500μS/cm). The humidifier is complete with a water inlet valve, water outlet valve and a maximum water level sensor, disposable cylinder, steam distributor and electronic controls. Humidifier control is of the ON-OFF type, can be also disabled by remote contact (Optional - humidifier and reheat lockout). Humidifier is removable from the rear of the cabinet.

Rack & Accessories

Supply and installation of high density 42 U height, Rack with Integrated cold aisle & hot aisle containment frame, with basic rack accessories.

Rack & Accessories Technical Specification:

1. Rack Containment Frame is 42 U, 19'' mounting type with 2200 (Height) x 600 (Width) x 1800 (Depth, including Rack + Cold & Hot Aisle Containment).
2. Rack frame is, scalable and modular with safe load carrying capacity of 1000 Kg.
3. Colour shade of Rack is RAL 7021.
4. Base plinth with 100 mm height.
5. Cable entry provision from top & bottom both side of rack.
6. Cut outs with rubber grommet on top and bottom cover of rack for cable entry.
7. Vertical Cable manager on both LHS & RHS on rear side.
8. Front & Rear glass door for complete 42U height visibility.
9. Thermally insulated cold aisle chamber.
10. Blanking panels to prevent air mixing.
11. Fixed Shelf to be provided.
12. Plastic Cable duct on vertical LH & RH section of racks for cable routing.
13. Front Rack doors are provided with Biometric Access Control with 02 nos. of Electromagnetic lock per door.
14. Gas spring to be provided on front doors of racks.
15. LED light to be provided on each rack.

SAFETY and security systems

Biometric based Access Control

The IP based Access Control System shall be used to serve the objective of allowing access to authorized personnel only. The system deployed will be based on Biometric Technology. The front rack doors will be provided with magnetic locks, and will operate on fail-safe principle through one common Biometric access control system. Rear doors will be operated through mechanical lock & key mechanism.

The system would be designed and implemented to provide following functionality:

- Configurable system for user defined access

- Built-in Real Time Clock (RTC), calendar; complete Database stored locally and shall be capable of operating offline on standalone mode
- Record, report and archive each and every activity (permission granted and / or rejected) with log formats
- Fail safe operation in case of no-power condition and abnormal condition such as fire, theft, intrusion, loss of access control, etc.
- At the biometric reader, user presents the finger to the biometric reader which is unique to each employee. The pattern is read and compared with stored data to grant / deny access.

Fire Alarm System

The integrated Data Centre infrastructure is designed as a complete stand-alone unit with security, fire detection and fire suppression systems. Each of the systems is inter-operable and inter connected.

Environmentally friendly Novec 1230 agent to be used to ensure that no harm to human beings and environment is caused.

Following systems to be installed.

- Novec 1230 Clean Agent for fire suppression system
- Fire detection and alarm systems, with detectors and panel.
- Protected area: The entire enclosed volume of the integrated data centre & Utility cabinet having electrical distribution panel is protected with fire detection and fire suppression system.
- The Novec 1230 system should be designed and installed as per NFPA 2001-2012 Edition. SMPV, Petroleum and Safety Explosives Organization (PESO) approved cylinder filled with Novec 1230 is installed in specially designed utility cabinet integrated with Data centre

Monitoring

1. Supply and installation of RDU based / monitoring system with Sensors & notification system. The system shall continuously collects critical information from network connected devices such as UPS system, Cooling Units , temperature & humidity sensors, Door sensors, Water Leak sensor and other dry contact monitoring. Beacon & Buzzer-Sound and Flash Led Alarm. Based on pre-set parameters, automated email alerts are sent to the intended recipients
2. Environmental monitoring with Temperature & Humidity sensors
3. Monitoring Technical Specification:

a. Intelligent Rack environment remote monitoring.
b. Modbus 485 Communications
c. SNMP Communication.
d. Single window for monitoring all sensors.
e. Data and logs of historical information of alarms and notification.
f. Temperature & Humidity Sensor, with LCD display and RJ45 connector.
g. Door opening sensor with RJ 45 connector.
h. Water leak detection sensor with RJ45 connector.
i. Smoke detection sensor with RJ45 connector.
j. Alarm device with LED flash and sound option.

CCTV Surveillance:

1. Supply and installation of CCTV System for integrated data centre infrastructure.
2. The Critical area of the Data Centre needs to be under constant video surveillance. The primary objective of implementing a CCTV system is to ensure effective surveillance of the area and also create a record for post event analysis. Monitoring cameras should be installed in proper areas to cover all the critical areas of the data centre.
3. The CCTV system shall provide an on-line display of video images on monitor. LED/LCD monitor shall be provided by client. Cameras with suitable lenses shall be used to view all the critical areas of the Data Centre. The CCTV system shall be based on the use of fixed dome cameras with 4 Channel DVR & suitable Hard disc for storage
4. The CCTV System proposed to fulfil the overall surveillance/observation requirements and enhance the level of security necessary shall be complete in all respects.

IP Based Dome camera (Indoor)

1. The IP based domes cameras shall support power over Ethernet (IEEE802.3at)
2. The camera shall provide 3 simultaneous video streams – Dual MPEG4 both 25 fps (Pal) and scalable MJPEG.1/3" Progressive CMOS.
3. 1.3 mega-pixel (1920 x 960) resolution camera, 3.6mm lens, ICR, 0.0lux with IR, 1280x960:25fps(P)/30fps(N), H.264/MJPEG, dual-stream, DC12V & PoE, DWDR, 3D DNR, BLC, IR: Atleast 30m, IP66 Housing (PANASONIC).
4. Channel DVR with 2 CCTV (500 GB Hard Disc).

Rodent Repellent System

The proposed modular Data Centre shall also have Rodent Repellent System

Other Requirement:

1. Proposals not complying with minimum eligibility criteria, as enumerated below, will be rejected and will not be considered for evaluation of technical bid. The proposal should adhere to the following minimum eligibility criteria.
2. Cooling, UPS and monitoring system should be from single OEM.
3. (DX) in row air conditioning unit using refrigerant R407C/R410a & inbuilt Humidifier. Each unit shall be factory tested for performance rating before shipment. Test certificate shall be submitted prior to shipment. Owner may choose to witness factory test at his option.
4. The OEM must have designed and executed minimum three Data Centre projects on a turnkey basis with Tier compliance for a third party customer, adhering to Data centre standards during the last 5 years from the of bid submission date.
5. OEM Service Support for Major Equipment's/OEM or Manufacturer should have its own service centre.
6. The OEM should have at least three qualified and experienced DC certified professionals like CDCP/CDCS/CDCE/ATD on their company payroll with minimum 3 years' experience in Data Centre designing and implementation.
7. OEM or Manufacturer should be ISO 9001: 2000 and ISO 14001 certified.
8. The Project Manager proposed from bidder must have a minimum 5 years of experience in executing & managing Data centre projects. (CV along with Client reference to be provided).
9. OEM shall be present in IDC (International Data Corporation) Market Space in leader position for Data Centre Infrastructure Management.

10. OEM or Manufacturer of the offered goods/ equipment's should be a company registered under the companies Act since last 10 years. Valid company registration certificate should be submitted.

4.7 Scope of Implementation and Integration components:

4.7.1 Field Equipment:

4.7.1.1 Industrial Grade Outdoor PoE switches

S.N.	Parameter	Minimum Technical Specifications
1	General Features	The switch should be Industrial Grade ruggedized in nature that provides minimum 8 x 10/100/1000 BASETX access ports four out of which should support HPOE (60W), additional 4 x 1000 Base-X SFP & One (1) ruggedized single mode SFP should be supplied with the switch.
		The switch should have non-blocking wire-speed architecture with support for both IPv4 & IPv6 from day one with wire-rate
		Switching fabric of minimum 20 Gbps or more.
		The switch should support backup storage drives, which will store the last known configuration of the switch In the case of hardware failure and replacement reinserting the storage drive should restore the last backup configuration
2	Layer 2 Features	802. 1Q VLAN on all ports with minimum 10k MAC address
		Spanning Tree Protocol as per IEEE 802.1d, ring protection protocol like REP or equivalent
		Should support Jumbo frames atleast 9000 bytes & Link Aggregation Control Protocol (LACP) as per IEEE 802.3ad.
		The switch should support IGMP v1/v2/v3 & atleast 1000 IGMP groups as well as IGMP snooping & IGMP filtering. Should also support MLD v1/v2.
4	Quality of Service (QoS)	Switch should support classification and scheduling as per IEEE 802.1P on all ports.
5	Features	The switch should provide traffic shaping and rate limiting features for specified Host, network, Applications etc.
6	Security Features	The switch should support ACLs, Extended IP ACLs, support RADIUS and TACACS+ for access restriction and authentication.
		Should support a mechanism to shut down Spanning Tree Protocol Fast-enabled interfaces when BPDUs are received to avoid accidental topology loops.
		Switch should support static ARP, Proxy ARP, UDP forwarding and IP source guard, DHCP Snooping, DHCP Option 82, Dynamic ARP Inspection (DAI), IP Source Guard, BPDU Guard, Port-Security, DHCP Snooping, 802.1x, 802.1AE, MAC

		Authentication Bypass, 802.1x Multi-Domain Authentication, Storm Control
7	Management Features	The switch should be SNMP manageable with support for SNMP Version 1, 2 and 3.
		Support for Automatic Quality of Service or equivalent for easy configuration of QoS features for critical applications.
		Switch should support PTP, FTP/TFTP
8	Mechanical Conditions:	• -5 to +70ºC continuous operating temperature range
		• Operating relative humidity: 5% to 95% no condensing
		Protection Class -minimum IP 30, NEMA TS-2
9	Certifications	Switch should be EN 55022A Class A, VCCI Class A, certified
		The switch should support IEEE 1588 PTP/BITS/PPS
		EMC interface immunity:
		Switch should be EN55024, EN 61000-4-2 Electro Static Discharge, EN 61000-4-5 Surge, EN 61000-4-8 Power Frequency Magnetic Field, EN 61000-4-11 AC Power Voltage

4.7.1.2 Direct Current Power Supply (DCPS)

S. No.	Features	Description	
Enclosure			
1.	General	The system shall be IP 55 with wall/floor and Pole mount option. This shall withstand the high temperature operation requirement as the system is exposed to outdoor environment. The system shall be unique and equipment space should be efficiently designed and the thermal condition should be evenly managed. Material of Cabinet is GI -120 GSM, Surface treatment PP Coating 80-120 Micron and Color-RAL (7035). Size: OEM to Comment	
2.	General	It shall be SMPS based and shall communicate with controller to charge the battery and provide the output.	

		Rectifiers shall be modular and work in parallel to share the load and provide redundancy. Failure of one module shall not affect operation of another module and other module shall keep working to feed the load. Rectifier shall have all the power connection on the backplane and shall be hot plug type in prewired shelf.	
Rectifier Specification			
3	Nominal Input Voltage	90 to 300 VAC	
4	Full Power operating range	180 to 300 VAC	
5	Operating Frequency	45 to 65 Hz	
6	Rectifier Module Capacity	1000 Wattage of each module (N+1) with 1 Redundant rectifier module	
7	Maximum. input current per Rectifier.	<6 Amps each module	
8	Efficiency at nominal condition	>90	
9	Power Factor	>0.99	
10	Operating Temperature	-40 to 75 Deg C	
11	Relative Humidity	0 to 95% (Non-condensing)	
12	Parallel Operation	Yes	
13	Modular / Hot swappable	Yes	
14	Module communication with controller	CANBUS	
Controller			

15	General	The controller shall be advanced controller to take care of Lithium Ion Battery charging. The controller shall have microcontroller based functionality. The controller shall able to provide data over SNMP and shall be able to integrate with GSM modem for remote communication	
16	Controller Interface	Digital, CANBUS	
17	Rectifier interface	CAN-based	
18	Rectifier Operation	Parallelable	
19	Digital Input	8	
20	Relay Output	8	
21	Temperature Monitoring	Ambient and Battery	
22	Voltage, Current	Load, Battery	
23	Display	LCD Display	
24	Local Monitoring	LAN / WEB browser	
25	Remote Monitoring	LAN / Modem, GSM, GPRS / WEB browser/SNMP V2C/Modbus	
26	Remote alarming	Dry contacts / SNMP	
27	Data Logs	Atleast 5,000 entries with Min., Max, Average value shall be recorded for selected parameter.	
28	Languages	English	
29	Local user interface	Configurable LEDs; LCD display; Keypad	
30	WEB	Different access levels; More than 200 dynamic WEB pages; SW and setup updates locally and remotely	
31	SNMP	Remote alarms using traps	
32	Parameter Setting	Keypad on Controller	
33	Safety	EN 60950, class I; UL 60950; CAN / CSA - C22.2	

34	EMC	EN 55022/EN 61000-6/1 class B; ETSI EN 300386 compliant	
35	Cooling	Natural air flow	
36	Operating temperature	0 to +65 ºC / +32 to +140 ºF	
37	Relative humidity	95 %, non-condensing	
38	Battery management	Temperature compensated Float charge, Boost and equalize charge for VRLA/SMF	
39		Charging Current Limitation (advanced)	
40		Low voltage disconnection, State of charge supervision and display	
41		Backup time supervision / Life time prediction, Automatic capacity test	
42		Symmetry supervision for voltage and currents	
43		Block voltage supervision	
44	Rectifier management	Microcontroller based for customization and supervision and control of auxiliary devices	
45		AC measurement (internal / external)	
46		Mains failure detection and alarming	
47		Rectifier Redundancy Supervision	
48		LLVD and BLVD functions	
49		Configurable event log and data log up-to 5k Logs	
50	System Management	Individual rectifier information and control	
Lithium Ion Battery Specification			
51	Battery-Lithium-Ion	The system should be designed to work with Lithium Ion battery (20AH)	
52	Technology	LiFePO4	
53	Nominal Voltage	48V	
54	Cycles	>3000 Cycles @ 80% DOD	
55	Operating Temperature Range (Charge)	Charging: 0℃ to +55℃ Discharging: -20℃ to +60℃	

56	Discharge Ending Voltage	42V	
57	Charging Limited Voltage	54.0 V	
58	Weight	Kg. (OEM to specify)	
59	Dimensions (L*W*H) mm (inches)	440 * 340 * 89 (2U) all in mm 19Inch Mounting Provision 2U Height	

Inverter Specification			
S. No.	**Features**	**Description**	
1	Input DC Voltage Range	40 – 57.6 VDC	
2	Nominal Input Voltage	48 VDC	
4	Low Voltage Cut off	42V DC	
5	Reverse Polarity Protection	Yes	
6	Nominal system voltage	230 V + 5%	
7	Continuous Power	700W	
8	Output	Sine wave	
9	Overload Capacity	110% for 60 sec 150% for 3 sec..	
10	THD	<3% (resistive load)	
11	Output frequency	50 + 5%	
12	Short Circuit Protection	Yes	
13	Over Temperature Protection	Yes	

14	Efficiency (75-100% of full loading)	88% peak	
15	Operating temperature	-5 to +70 °C Full Power – atleast 55°C (reduced Power @ 65 °C)	
16	Communication Interface	RS 485 / Modbus / SNMP	

4.7.1.3 Field Junction Box

S.N.	Parameter	Minimum Specifications
1.	Size	Suitable size as per site requirements to house the field equipment
2.	Cabinet Material	Powder coated CRCA sheet/ Stainless steel
3.	Material Thickness	Min 1.2mm
4.	Number of Locks	Two
5.	Protection	IP66 / NEMA 4X
6.	Mounting	On Camera Pole / Ground mounted on concrete base
7.	Form Factor	Rack Mount/DIN Rail
8.	Other Features	Rain Canopy, Cable entry with glands and Fans/any other accessories as required for operation of equipment's within junction box.

4.7.1.4 Camera Poles

S.N.	Parameter	Minimum Specifications
1.	Pole type	Hot Dip Galvanized after Fabrication with Silver coating of 86 micron as per IS:2629; Fabrication in accordance with IS-2713 (1980)
2.	Height	5-10 Meters, as-per-requirements for different types of cameras & Site conditions
3.	Pole Diameter	Min. 10 cm diameter pole (bidder to choose larger diameter for higher height)
4.	Cantilevers	Based on the location requirement suitable size cantilevers to be considered with the pole
5.	Bottom base plate	Minimum base plate of size 30x30x15 cm
6.	Mounting facilities	To mount CCTV cameras, Switch, etc.
7.	Pipes, Tubes	All wiring must be hidden, through tubes/pipes. No wires shall be visible from outside.
8.	Foundation	Casting of Civil Foundation with foundation bolts, to ensure vibration free erection (basic aim is to ensure that video feed quality is not impacted due to winds in different climatic conditions).

		Expected foundation depth of min. 100cms. Please refer to earthing standards mentioned elsewhere in the RFP.
9.	Protection	Lightning arrester at select sites as per the requirements
10.	Sign-Board	A sign board describing words such as “This area under surveillance” (in English and Hindi)

4.8 Other Items

4.8.1.1 Monitoring Workstations

S.N.	Parameters	Minimum Requirements
1	Processor	Latest generation 64bit x 86 Xeon Processer with latest chipset
2	Motherboard	OEM Motherboard
3	RAM	Minimum 8 GB DDR3 RM expendable to 32 GB
4	Graphics card	Minimum Graphics card with 2 GB video memory (non- shared)
5	Monitor	Monitors of 24” TFT LED monitor, with Minimum 1920 x1080 resolution, Minimum input of 1xDP, 1x HDMI, 1xDVI, Energy star 5.0/BEE star certified
6	HDD	Min. 2 TB Hard Drive @7200 rpm
7	Other Accessories	Line/Mic IN, Line- out/Spr Out (3.5 mm), Minimum 6 USB ports (out of that 2 in front), 104 keys minimum OEM keyboard, USB Optical OEM mouse,
8	PTZ joystick controller	PTZ speed dome control for IP cameras Minimum 10 programmable buttons Multi-camera operations Compatible with all the camera models offered in the solution Compatible with VMS /Monitoring software offered
9	Operating System	64 bit pre-loaded OS with recovery disc
10	Antivirus feature	Advanced antivirus, antispyware, desktop firewall and encryption as required.

4.8.1.2 Desktops for Helpdesk

S.N.	Parameters	Minimum Technical Specifications
1.	Processor	latest & high performance (3.0 Ghz) or higher
2.	Memory	8 GB DDR3 RAM @ 1600 MHz. One DIMM Slot must be free for future upgrade
3.	Motherboard	OEM Motherboard
4.	Hard Disk Drive	Minimum 500 GB SATA III Hard Disk @7200 RPM or higher
5.	Audio	Line/Mic In, Line-out/Speaker Out (3.5 mm)
6.	Network port	10/100/1000 Mbps auto-sensing on-board integrated RJ-45 Ethernet Port
7.	Wireless Connectivity	Wireless LAN - 802.11b/g/n/
8.	USB Ports	Minimum 4 USB ports
9.	Display Port	Minimum 1 Display Port (HDMI/VGA) port

10.	Keyboard	104 keys Heavy Duty Mechanical Switch Keyboard (USB Interface) with 50 million keystrokes life per switch. Rupee Symbol to be engraved.
11.	Mouse	Optical with USB interface (same make as desktop)
12.	Monitor	Minimum 18.5" diagonal LED Monitor with 1366x768 or higher resolution. (Same make as desktop). Must be TCO05 certified.
13.	Operation System and Support	Pre-loaded Windows 10 (or latest) Professional 64 bit, licensed copy All Utilities and driver software, bundled in CD/DVD/Pen-drive media.
14.	Certification for Desktop	Energy Star 5.0 or above / BEE star certified

4.8.1.3 Ceiling Speakers

- The ceiling speakers shall have high power and high sensitivity with extended frequency responses.
- The ceiling speakers shall have wide, controlled constant directivity dispersions for optimum coverage.
- The ceiling speakers shall have output of at least 15W peak. They shall have in-built amplifiers or shall be supported by an external amplifier.
- The ceiling speakers shall have a conical coverage pattern.
- The ceiling speakers shall be in a colour to match the ceiling and surrounding interior design.
- The ceiling speaker shall have a diameter not greater than 8.5".
- MSI shall quantify and space speakers to provide full audio coverage within the command centre room and conference room.
- The ceiling speakers shall follow the manufacturer recommendation for connectivity.
- The Ceiling Speakers shall automatically adjust the output audio level based on ambient noise. This may require either in-built noise sensors with the ceiling speakers or an independent ambient noise monitoring system.

4.9 Disaster Recovery Center

Disaster Recovery Center on Cloud.

MSI should provide DR as a service on cloud with 50% capacity of DC.

Following criteria need to be complied by CSP (Cloud Service Provider)

- Data Center Service Provider (CSP) should be a company registered under Indian Companies Act 1956. The company should be providing Data Center related services in India for atleast the last FIVE financial year ending 31st March 2016.
- CSP must have annual revenue of INR 30 Crores or more for last three financial years ending 31st March 2016.
- CSP must be operating at least two Data Center Facilities operational in India with a minimum provisioning capacity of 400 Racks.
- DC/DR facility proposed should be certified by Uptime Institute for atleast TIER III certificate and should be valid at the time of bidding.

- CSP should have executed atleast TWO projects of DC/DR with Cloud deployment with an order value of minimum 5 Cr hosted out of the proposed DC/DR facility.
- CSP should have executed at least ONE project of DC/DR with proposed Cloud deployment with an order value of minimum 1 Cr from its proposed DC/DR facility and should be operational at the time of bidding.
- CSP must be having at least 1000 VM's running out of the proposed DC/DR facility at the time of bidding.
- Both DC & DR facility should be owned by the CSP and should be a separate building or in a non-commercial premises.
- DC and DR should conform to at least Tier III standard, certified under TIA 942 or Uptime Institute certifications and the certificate should be valid at the time of bidding
- Data Center and Disaster Recovery Center Facilities must be certified for the latest version of ISO 27001 / 27018 (year 2013 or above) and provide service assurance and effectiveness of Management compliant with ISO 20000 standards.
- Data Center facility must be PCI certified and should be valid at the time of bidding.
- CSP should have atleast 150+ technical staff on its payroll at the time of bidding.
- CSP should have atleast 5 ITIL v3 certified staff on its payroll at the time of bidding.
- CSP should have atleast 1 BS7799/ISO27001 lead implementation /auditor at the time of bidding.
- NOC / Operations centre should be part of data centre facility proposed.
- Proposed data center and cloud hosting infrastructure should be SAP HANA certified.
- The bidder should have experience of hosting SAP with HANA database with at least 5 clients with SAP HANA running at the time of bidding.

DR As a Service

a) MSI shall also be responsible for providing Cloud service for storing all applications at DR [minimum 50% production capacity, RTO – 60 mins, RPO – 15 mins] which will be implemented under Dehradun Smart City project for the project duration. All H/W and S/W on cloud should meet the specification in RFP. The cloud provider should be MEITY empaneled as well as STQC certified Govt. community cloud (GCC).

b) All applications need to have high performance clustering (redundancy) within the Data Centre with heartbeat, automatic fail-over, and redundant data storage is active passive or active-active configuration as per the high availability targets. The data replication should be continuous among all the servers and shared storage should not be used. All mission critical systems must be active-active configurations. Active passive configurations may be permissible for supporting applications.

c) The proposed Cloud Service Provider (CSP) must be an empaneled cloud service provider by Meity (Ministry of Electronics and Information Technology for Public cloud, Virtual Private Cloud and Community Government Cloud.

d) The Cloud Data Centre Facility must be within India and must be Tier III or above. The DR site within India should be at least 250 Km away from the DSCL Data Center and in a different seismic zone.

e) The Cloud Data Centre, where cloud hosting is proposed, must have ISO 27001 certification.

f) The cloud service provider must have billing model of pay-per-consume where it will charge for amount of computing resources being consumed by application rather than for the allocated resources. MSI shall provide the rate chart of the cloud services to DSCL.

g) Cloud services should be accessible via Internet, Point to Point / MPLS, Leased Lines,

OFC WAN etc. MSI must provide private connectivity between DSCL's network and Cloud Data Centre Facilities.

h) MSI shall be fully responsible for upgrades, technological refreshes, security patches, bug fixes and other operational aspects of the infrastructure that is in the scope or purview of MSI.

i) MSI shall provide interoperability support with regards to available APIs, data portability etc. for DSCL to utilize in case of Change of cloud service provider, migration back to Local Data Centre, burst to a different cloud service provider for a short duration or availing backup services from an alternate Cloud service provider.

j) MSI is required to prepare and submit along with their technical proposal, the details of methodologies and computations for sizing and capacity of storage, compute, backup, and network and security resources.

k) DSCL shall retain ownership of all virtual machines, templates, clones, and scripts/applications created for DSCL's applications. DSCL shall retain the right to request (or should be able to retrieve) full copies of these virtual machines at any time.

l) In no circumstances, the data accumulated and processed by Command and Control Centre should be compromised. Hence, provisions will be made to keep all the data stored in this platform highly secured with required multi layered security access control and authorization framework. Further the platform shall provide an open standards based integration Bus with API Management, providing full API lifecycle management with governance and security features.

m) Additional Parameters

- Cloud services should be accessible via internet and MPLS.
- MSI should configure, schedule and manage backups of all the data including but not limited to files, folders, images, system state, databases and enterprise applications.
- Encryption of all backup files and data and management of encryption keys as a service that can be enabled for Government Departments that require such a service.
- MSI should offer dashboard to provide visibility into service via dashboard.
- MSI shall not delete any data at the end of the agreement (for a maximum of 45 days beyond the expiry of the Agreement) without the approval of the DSCL.

The below High Level Design (HLD) is just for reference over cloud deployment. MSI can suggest security stack & deployment method according to their recommendations;

Preparation of Disaster Recovery Operational Plan

The bidder should provide detailed operating procedures for each application during the following scenarios. These will be mutually agreed upon with DSCL during the project kick off.

- Business as usual: the primary site is functioning as required, procedures for ensuring consistency of data availability at secondary site.
- Disaster: Declaration of disaster, making the DR site live for production, ensuring availability of users to the secondary site.
- Operations from DR site: Ensuring secondary site is addressing the functionality as desired.
- Configure proposed solution for usage.

MSI shall provide DR Management (DRM) Solution to DSCL meeting following specifications:

Sl no	Features
1	The proposed solution must offer a workflow based management& monitoring and reporting capability for the real time monitoring of a DR solution parameters like RPO (at DB level), RTO, replication status and should provide alerts(including SMS and e-mail alerts) on any deviations. The proposed solution should be able to conduct DR Drills from a centralized location
2	The proposed solution should provide a single dashboard to track DR Readiness status of all the applications under DR
3	The proposed solution should be capable of reporting important health parameters like disk space, password changes, file addition/deletion etc. to ensure DR readiness
4	The proposed solution should have inbuilt ready to use library of recovery automation action for heterogeneous databases and replication environment. This must significantly reduce custom development of scripts and speedy deployment of DR solutions
5	The proposed solution should facilitate workflow based switchover and switchback for DR drills for standard applications based on industry best practices
6	The proposed solution should facilitate workflows for bringing up the applications and all the components it depends on at DR while it is up at primary site without pausing/stopping the replication

Periodic Disaster Recovery Plan Update

The service provider shall be responsible for –

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

4.10 Intelligent Traffic Management System

Intelligent Traffic Management System

The MSI shall ensure the successful implementation of the proposed Intelligent Traffic Management System (ITMS) and shall provide capacity building support to city authorities as per the scope of services described below. Any functionality not expressly stated in this document but required to meet the needs of the DSCL to ensure successful operations of the system shall essentially be under the scope of the MSI and for that no extra charges shall be admissible. MSI shall be responsible to install ITMS systems (List of the proposed locations are given at Annexure).

The following key tasks shall be covered under this initiative:

- To provide CCTV cameras including Fixed and PTZ cameras for live video monitoring of key traffic junctions
- To provide an integrated traffic management platform for viewing, controlling and managing all the traffic components installed across the city.
- To monitor the ongoing activities of the key traffic junctions from the DICCC.

- To facilitate traffic rules enforcement through design, supply, and installation of Red Light Violation Detection (RLVD) and speed violation detection. Each of these systems shall be integrated with the DICCC.
- To integrate e-challan system with traffic enforcement cameras, sensors, echallan handheld devices for automated issuance of challans
- To provide API integration of Variable Message Sign boards with existing/proposed Smart City Infrastructure to provide real time information and services, such as traffic related, journey planners and accident reporting
- To create a Centralized Management Information System (MIS) as a part of the IT solution for faster decision making in traffic emergency such as heavy rain fall, accidents, terrorist attack, VVIP movements etc.
- To create centralized Traffic data management including, real time traffic monitoring, traffic status, count, classification, gap, head way, occupancy, average speed and provide historical as well as live data to manage traffic in present and near future and help decongestion.
- To operate, manage and train the administrative staff and offer back-end support on the operations of the ITMS using the departmental manpower

MSI shall implement and deliver the following systems and capabilities linked with DICCC & ITMS Platform.

ITMS Platform

- Adaptive Traffic Control System (ATCS)
- Smart Traffic sensors for smart traffic management and planning
- Smart Traffic Suit for Information and Traffic planning
- Automatic Number Plate Recognition (ANPR) System
- Red Light Violation Detection (RLVD) System
- Speed Violation Detection (SVD) System
- ANPR
- E-Challan
- Variable Message Sign boards
- TARS

4.10.1 Adaptive Traffic Control System (ATCS)

As part of the Smart City mission, the city of Dehradun also wants MSI to supply, install, commission and maintain an Area Traffic Control System (ATCS) for 5 years. The key features of the system being:

Adaptive system – The system shall change traffic signal timings based on inputs from certified 4D forward firing Radar based vehicle detectors deployed at each approach of each junction.

Standards compliant – The system shall employ industry standard open communication protocols like UTMC/UG405.

Tactical traffic control – The system shall be capable of managing the traffic signals in near real-time, based on inputs from the traffic detectors.

Strategic traffic management – The system shall use data fusion models to understand the current state of the network, employ short term prediction models and then use simulation models to strategically manage traffic across the network, before things get worse.

Central control centre – The CCC is expected to act as the core of the system. The system shall employ a reliable communications network to ensure maximum availability for the communication link between the CCC and the traffic signals.

Objectives:

- Manage traffic centrally, while receiving traffic inputs from sensors
- Optimally configure the traffic signal timings, in near real time
- Minimize traffic congestion and waiting time
- Improve Journey Time Reliability
- Ensure smooth movement of emergency response vehicles like ambulances, police etc.
- Manage VIP movements better
- Perform data analytics on the traffic data to analyse travel demand and manage traffic effectively
- Send real time information to commuters
- Improve compliance with traffic rules
- Generate count and classification data for each approach

Scope of work:

Preliminary surveys:

- Collect data of existing operating conditions, traffic volumes across various time periods of a day, which will cover all peak and non-peak hours, weekends, etc., saturation flow rates, travel times along major corridors during different times of the day. At the minimum, the following data shall be collected:
- Classified turning movement counts for vehicles at major junctions
- Pedestrian volumes at major junctions
- Physical and visual characteristics of the area
- Travel times, delays between different points on the network
- Additional dependencies with respect to the available infrastructure and geometry at the junctions
- Study the existing traffic management systems and processes deployed by the competent authorities, MIS reporting needs, problem areas and expectations of the city. Perform Gap Analysis and finalize the key requirements with the city.

Design and planning:

- Prepare the solution architecture and design drawings
- Seek approval of the designs from the city
- Prepare the execution plan and get it approved by the city
- Prepare work zone safety and traffic management plans

Installation and commissioning:

- Procure, supply and install certified 4D radar based vehicle detectors, controllers and other required accessories as per the approved design
- Procure, supply and install all relevant hardware, like servers and workstations in the CCC
- Connect the signal controllers to the CCC via a suitable communications media
- Install the ATCS software in the servers within the CCC
- Integrate all components of the system and configure the traffic signal plans at each of the junctions, for varied operating conditions like peak and off-peak traffic, weekend traffic, traffic flows during special events etc.

Functional requirements of ATCS

General:

- The system would be used to monitor and control traffic signals, including signalized pedestrian crossings, using a traffic responsive strategy based on real time traffic flows obtained using vehicle presence sensors.
- All signal controllers under Adaptive Traffic Control System shall be provided with inputs from 4D radar based vehicle detection sensors for detecting demand and communications equipment to send the demand data and to receive instructions on the control strategy in near real-time.
- The system should be extensible to add more signals whenever required.
- Any existing infrastructure at the junctions that might help in traffic control, where possible, should be integrated with ATCS.
- ATCS shall use standard communication protocols UG405 or NTCIP. It should also provide the functionality of integration with on-ground hardware of any third-party traffic controller that is UG405 or NTCIP compliant.

- Dehradun is home to the National Institute of Visually Handicapped. It is suggested that traffic signals in Dehradun have pedestrian signals that are accessible to the visually handicapped. Blind friendly pedestrian signals shall include an audio-tactile device at each crossing. The device should emit an audio clue indicating when it is safe to cross the road. In addition, there should be a tactile feedback device that indicates when it is safe to cross the road (e.g. https://www.bbc.com/news/blogs-ouch-22706881).

The tactile device is important at small junctions where there is a possibility of audio cues from multiple approaches causing confusion. It is also helpful for people who are both blind and deaf.

Vehicle detectors:

To Make Intersections junction in the city more advances and more functions. It is required that sensor used in not dependent on the image but is able to work in fog, rain and bad weather. The single sensor used should be flexible in installation and should be able to do stop line and forward traffic analysis. Counting, classification and volume analysis should be done by forward firing radar which is able to analyse and track traffic for minimum 180 meters and should simultaneously track 125 objects

The sensors used by MSI should be able to perform in all weather conditions including FOG, RAIN, BAD weather and should provide not only, stop line control but also advance detection and data for counting, classification, gap detection, occupancy, average speed, queue length, wrong direction helping city traffic control authorities to plan traffic timing and adapt to junction adaptive systems based on traffic. It is important that sensors used do not require cleaning and work in dusty environment of city. The detectors manufacturer should have at least supplies 20,000 radars and should have experience in such technologies.

Traffic signal controller:

- The controller shall have a facility to list all conflicting phases at an intersection. After configuration, a traffic engineer shall verify that the signal aspects are running as expected, for each program coded in the controller, before being put to use.
- The controller shall be able to take queue inputs from the 4D radar and optimize the signal timing based on count, classification, traffic volume, speed, gap, and queue lengths.
- During power up the controller shall initially execute the Flashing Amber / Flashing Red plan for a time period of 3 Seconds to 10 Seconds. The default value of this Starting Amber is 5 Seconds. Facility shall be available to configure the time period of Starting Amber within the given limits at the site.
- Health monitoring should be available for the traffic controller and the signal aspects in all modes of operations.
- A hardware failure leading to a conflict condition (due to faulty devices or short circuit in the output) shall force the signal into Flashing Amber/ Flashing Red.
- The controller shall be able to interface with the 4D radar based detector using an industry standard open collector interface as well other standard communication protocols as per the requirement.

The signal controller shall have a police control panel with:

- Hurry call buttons,
- Auto/Manual selection button,
- Manual advance button,
- Normal/Flashing mode button, and
- Junction On/Off button.

The controller shall have the following modes of operation:

- Fixed time mode - the controller shall execute a pre-set program, which does not consider the inputs from the traffic detectors.
- Vehicle actuated mode - the controller shall execute pre-set programs that do not have fixed green times. The green time for each approach shall be bound by the constraints of minimum green and maximum green times. The actual green time is determined based on the vehicular demand obtained from the traffic detectors.
- ATCS mode - the controller shall execute the programs determined by the ATCS application in the control Centre and shall take inputs from traffic detectors to optimally split green times.

- The controller shall either have a fixed operator console or a portable one to allow traffic engineers to program the controller on-site.
- It should be possible to configure a program and set it remotely from the control centre.
- The controller shall allow interfacing with the ATCS application using an industry standard protocol such as UTMC/UG405 or NTCIP. No proprietary communications protocol shall be allowed, in any case.

ATCS application:

- The application is at the core of the system and shall be hosted on a server in the control center.
- The application should allow creation of green corridors to ensure priority movement of Emergency Response vehicles, such as ambulances, fire engines and police vehicles.
- The application shall interface with a popular microscopic traffic flow simulation software for pre and post implementation analysis and an online simulation for study of the proposed ATCS control strategy at various times of the day. The simulation shall be capable of identifying the impact of any anomaly in the system along with the strategy chosen. The simulation model shall assist the traffic engineers/police to identify the best possible strategy in any unusual/unprecedented event.
- The application shall be estimate a comprehensive network state using data from ANPR, GPS or any other such data collected from other third party sensors/detectors/cameras.

The application should be capable of running in the following four modes:

Connected signals mode: This mode should enable traffic police personnel to remotely configure and control the signal timing plans using the ATCS interface available in the CCC.

Automatic plan switching mode: The system should be configured to run the most appropriate signal timing plan for a group of junctions from a library of signal plans. The system should automatically select the most appropriate plan for the prevalent traffic conditions based on a set of customizable rules.

Optimization mode - tactical: Signal timings for a group of junctions should be optimized for pre-defined performance indicators, like delays, travel times etc. Short term prediction models shall forecast the traffic demand for 5, 10 and 15 minutes. The traffic demand shall be input into a traffic simulation model and the outputs of the simulation model shall be employed to establish performance indicators. The optimization model shall use these performance indicators to determine optimal signal timings.

Optimization mode - strategic: The system shall have a short term traffic state prediction model which continually estimates the state of the network, in terms of traffic flows and travel times. The traffic flows and travel times are to be input into a microscopic traffic flow simulation model. If significant changes in the network state are observed, traffic engineers shall be able to run simulation models to perform what-if analysis on pre-defined traffic management strategies.

The application shall have a Graphical User Interface (GUI) with an underlying GIS map that shall display the network and the traffic signals, traffic cameras/detectors, Variable Message Sign (VMS) boards and Public Address (PA) systems deployed.

ATCS application should be capable of displaying live video from CCTV cameras that have been deployed for traffic surveillance.

The GUI shall provide:

- Flexibility to the operators to zoom and navigate with ability to interact with objects on the map.
- Interoperability across multiple platforms.
- Web browser based access, requiring no local setup on the
- Graphically present signal plan execution and traffic flow at the intersection on desktop

The GUI shall have the following features:

- User login – Operator authentication shall be verified at this screen with login name and password.
- Network Status Display – This online display shall indicate with appropriate colour coding on site map whether an intersection under the ATCS is online or off.
- On double clicking the intersection a link shall be activated for the traffic flow display for the intersection.
- Live video feed – The operators shall be able to see the live video feed from CCTV cameras that have been deployed for traffic surveillance.
- Traffic Flow Display – This online display shall indicate the current traffic flow with animated arrows, mode of operation, stage number being executed and elapsed stage time.
- Saturation Snapshot – This display shall show the current saturation levels of all intersections in a corridor.
- Reports Printing / Viewing – This link shall allow selection, viewing and printing of different reports available under ATCS.
- Time-Space Diagram – The time-space diagram shall display the current stages being executed at every intersection in a corridor with immediate previous history.
- Junctions shall be plotted proportional to their distance on Y-axis and time elapsed for the stage in seconds on X-axis.
- ATCS application shall graphically show the execution of the signal plans, in real-time.

The solution should include the following reports at a minimum:

- Stage Timing report – The report shall give details of time at which every stage change has taken place. The report shall show the stage sequence, stage timings and stage saturation of all stages of all cycles for a day.
- Cycle Timing report – The report shall give details of time at which every cycle has taken place.
- Stage switching report – The report shall give details of time at which a stage switching has taken place. The report shall show the stage sequence, stage timings and stage saturation for a day.
- Cycle Time switching report – The report shall give details of time at which a cycle switching has taken place.
- Mode switching report – The report shall give details of the mode switching taken place on a day.
- Event Report - The report shall show events generated by the controller with date and time of event.

- Power on & down: The report shall show time when the master is switched on, and last working time of the master controller.
- Plan Change – The report shall show the time of change of plan either through keypad or remotely through a PC or Server.
- Mode Change – The report shall show the time when Master controller's operating mode is changed either manually through keypad or a remote server. The typical modes are FIXED, VA, FLASH, LAMP OFF and HURRY CALL.
- Count & Classification Report – The report shall show the count & classification data on each approach at various times of the day. It shall be possible to extract/integrate this data for other applications.
- Queue Report – The report shall show the queue lengths at each approach of the junction at various times of the day. It shall be possible to identify the impact of the queue length on the signal timings.
- Lamp Status Report – The report shall show lamp failure report with date and time of failure, colour of the lamp and associated phase.
- Detector Failure Report – The report shall show the date and time of detector failure with detector number and associated phase.
- Conflict – The report shall show the conflict between lamps (RED, AMBER, GREEN) in the same phase or conflict between lamps with other phase.
- Corridor Performance Report – The report shall show the saturation of all the intersections in a corridor for every cycle executed for the corridor and the average corridor saturation for a day.
- Corridor Cycle Time Report – The report shall show the Corridor cycle time, Intersection cycle time, Mode of operation and degree of saturation of all the intersections in a corridor for every cycle for a day.

Technical Specifications of ATCS components:

Traffic signal controller:

Traffic signal controller in conjunction with an Outstation Transmission Unit (OTU) should be able to run any ATCS algorithm having demand actuated dynamic signal timing plan selection. The communication between the controller and the ATCS software shall happen over industry standard G405 or NTCIP protocols. The following specifications are to be adhered with, either directly or using the OTU:

Power supply:	230 V AC @ 50 Hz
Communication protocol:	UTMC/UG405 or NTCIP
Number of signal groups:	16 minimum
Number of signal head outputs:	32 minimum
Number of phases:	16 minimum
Number of signal plans:	32 minimum
Number of stages per plan:	16 minimum

Number of detector inputs:	16 minimum
Interfaces:	Ethernet, RS232, USB
Signal head compatibility:	230 V AC @ 50 Hz or 12/24/48 V DAC
Hurry Call Buttons:	Minimum 4
Police Control Panel:	Yes, with hurry calls and push to change buttons
Temperature:	0°C to 60°C
Communication standard:	UTMC/UG405 or NTCIP protocol over TCP/IP
Media interfaces:	1 x 10/100 Ethernet interface
RAM:	128 MB SDRAM minimum
Storage Capacity:	512 MB minimum
Timing Resolution:	Minimum 100 msec (input resolution to 2ms)
Input Pins for detectors:	Minimum 16 Open Collector Interface pins

Vehicle Detector for ATCS

The Traffic detector shall be a 4D forward firing radar with refresh time of better than 75 ms and should comply to below specifications

1 The vehicle detector used should be forward firing 4D Radar with high definition for making Intersections and traffics lights smarter. The sensor should work with in the frequency band of 24 GHz or 77 Ghz

2 Vehicle detector should be able to protect in Fog, Rain, and darkness night and in dust environment and should not have cleaning requirement as in video sensors

3 The vehicle detector should have had a wide field of view of 40 degrees, and at the same time a range of atleast 180m

4 Vehicle detector should be multi-lane and should Detect atleast 126 individual objects, and measure their position and speed

5 The sensor should have 4D object tracking and should measure (X, Y, speed and elevation) Cartesian coordinates or polar coordinates range, azimuth and elevation angle, as well as the speed vector simultaneously for atleast 126 objects

6 The 4D with HD technology used should provide high-resolution capability in scenarios where many vehicles are closely spaced, i.e. in many lanes, dense traffic, traffic jams, stop and-go situations

7 One single sensor should allow atleast 16 virtual loops and should have very high detection performance compared to video detectors.

8 Vehicle detector should detect moving and stopped traffic i.e. should detect vehicles, no matter if stopped or moving. Atleast -320 km/h--+320km/h: no matter what the traffic direction.

9 Proposed radar should be manufactured by company who has experience of radar technology and should have manufactured more than 20000 Radars, should have service centre in India

4.10.2 Traffic Monitoring and Management:

DEHRADUN smart city is looking forward to having real time traffic monitoring of major strategic arterial/urban road network across the city to control congestion situation and allows real time data traffic monitoring, having traffic status from all such locations.

Dehradun city will have following modules to attain goal of safe and smart traffic city.

- Installations of ANPR & Smart traffic sensors – to provide control of all city incoming and outgoing traffic with exact classification count and other traffic statistics
- Smart traffic sensors in few of city strategic roads to have exact city traffic count, classification, real time traffic situation, congestion & traffic volume management, wrong direction, incident detection with sensors which can perform in all weather (FOG, RAIN, DARK Night, etc.) without any cleaning activity
- City Junctions will be made more Fluid & adaptive using smart 4D UHD Vehicle detector sensors for stop bar and advance vehicle detection including wrong direction, queue length, vehicle counting classification using sensor which can simultaneously detect at least detect 250 vehicles and provide the controller with exact information to have smart schedules.
- RED LIGHT VIOLATION: city junctions will have red light enforcement systems, which can automatically issue fine to people who do not respect traffic signals and create life threatening situations for others.
- Some of the city roads will be fitted with certified solutions for Instant and Average speed enforcement systems, assuring people of their fairness and use when issuing E fines to them and making citizens safer.
- E Challan Systems for Mobile as well as Fixed Systems
- TARS: Traffic Accident reporting system for City police to register and report complete accident
- Centralized Traffic suit which can centralize all above modules and provide active information and reports to city police to make Dehradun a smart city with smart traffic cell in place.

In addition, all these solutions will be centralized in a traffic suit which can not only help in traffic management but also provide e live traffic status, average speed, gap, headway & occupancy, counting, classification data along with complete incident reports as required by the client. The data will not only provide real time information of traffic information but will also help in planning resource allocations based on traffic status and possible forecast. The data should be collected and stored and should be available to traffic police and authorities/CCR to compare them with present data or help in forecasting of traffic helping in better management of city roads and traffic management.

DEHRADUN URBAN & ARTERIAL ROAD MANAGEMENT

DEHRADUN smart city is looking forward to having real time traffic monitoring of major strategic arterial/urban road network across the city which allows real time data traffic monitoring, having traffic status from all such locations. In addition, the solution should provide live traffic status, average speed, gap, headway & occupancy, counting, classification data.

The data will not only provide real time information of traffic information but will also help in planning resource allocations based on traffic status and possible forecast. The data should be collected and stored and should be available to traffic police and authorities/CCR to compare them with present data or help in forecasting of traffic helping in better management of city roads and traffic management. The entry and exit of some stretches roads/zones will be done initially to evaluate flow of traffic and evaluate its effect on traffic conditions at various times of the day/weeks etc.

Forward firing 4D object tracking with high definition resolution along with laser scan technology will be used to get the best results in all weather conditions for traffic management in all arterial roads.

All traffic junctions will be fitted with 4D forward firing sensor which will be able to provide stop line as well as advance detection capabilities with counting, classification, queue length, gap, average speed etc. to make city junctions more adaptive. Moreover all these sensors should perform in all-weather situation like FOG, RAIN, BAD Weather and should not be depended on image/video.

The sensors should not be image dependent, should not require cleaning activities and should work with minimum bandwidths available.

The analysis and processing of traffic data software should provide customizable reports both in tabular and in graphical form, based on the variables of interest as agreed with client during execution. The report generation can be done by selecting various parameters through a simple and intuitive graphical interface allowing to achieve maximum flexibility, or by selecting the standard reports with variables previously set.

The standard reports will be agreed during the executive project phase with the authorities and will Include:

- Average daily traffic weekday / holiday / seasonal

-Average hourly traffic weekday / holiday / seasonal

- Peak hour traffic

- Thirtieth rush hour

- Trend of variation of daily traffic

In addition to the reports mentioned above, further ten standard reports will be implemented for evaluating the traffic (eg traffic per month, annual traffic, hours of slow traffic per day / month / season, hours of stopped traffic (queue) daily / monthly /seasonal ...) accordingly to the client's needs.

The main functionalities which are required at traffic suit at CCR are:

- GIS: interactive map/synoptic allowing easy and quick monitor of the equipment located in each position.
- Visualization of summary and detailed information from the traffic monitoring sub-systems
- Visualization of Traffic forecasted data in the Maps (for next 30, 45 and 1 hour)
- Visualization of alerts and anomalies reported by monitoring sub-systems;

- Visualization of “real time" data from the traffic monitoring system by selecting an item on the map;
- Access to control and configuration interfaces of each traffic count station.
- Access to the diagnostics of substations
- Access to historical traffic data and statistics
- Various data comparison possibilities for hourly, daily or weekly to evaluate traffic data
- Complete back up of data for sensors at least next 5 years
- Graphical interpretation of data
- Optional (time to travel & other information’s with possibility of integration with VMS)

S. No.	Functionalities
1)	GIS interactive map allowing easy and quick monitoring of all sensors located in each position.
2)	Average daily traffic with classification
3)	Average hourly traffic with classification
4)	Trend of variation of daily traffic with classification. Prediction of traffic based on trends to allow logistics planning.
5)	Visualization of summary and detailed information from the traffic monitoring sub-systems
6)	Visualization of alerts and anomalies reported by monitoring sub-systems like incident detection, wrong direction, prolonged congestion wherever applicable
7)	Visualization of “real time" data from the traffic monitoring system by selecting an item on the map
8)	Access to historical traffic data and statistics.
9)	Various data comparison possibilities for hourly, daily or weekly to evaluate traffic data.
10)	Graphical interpretation of data.
11)	Time to travel and other information with possibility of integration with VMS
12)	Complete back up of data for at least next 10 years
13)	Administrator will have Access to control and configuration interfaces of each traffic count station
14)	The application software should maintain the logs of user activities to facilitate the audit trail.
15)	Database server should be able to handle the data of all the devices at one time simultaneously with huge database size without affecting the performance.
16)	The software should be able to generate various periodical reports, summaries, MIS reports, query reply etc. as per the requirements.
17)	Administrator should be able to modify the master tables as and when required

SMART TRAFFIC SENSOR -A

The sensor will be placed in strategic locations to provide accurate count, classification, gap, headway, occupancy, average speed, traffic status etc for traffic control, planning and management for present and future traffic planning.

S. No.	Features	Description
1	Technology	System should work in day and night condition and should use time of light measurement using scanning laser 905nm non-visible with integrated optional doppler technology.
2	Processor	The processor should be minimum an ARM9 microcontroller clocked at 400 MHz with an internal memory of 64 MB SDRAM and 128 MB FLASHES. Power consumption should be less than 5W.
3	Main features	System should provide vehicle count, class of vehicles (minimum 8 class when installed over the lane and 4 lasses when installed on the side for multilane. Sensor should able to distinguish between car, Bus truck, trailor auto etc) and other information to be used for ITMS viz. Transit id, direction, classification, counting, height, occupation time, headway time, average speed and Traffic status. OEM should be able to replace a class with new classification of vehicle. For example if client wants to add a auto rikshaw with a pre-existing vehicle.
4	Precision	Maximum error permissible ± 5% for counting and classification in a single lane with 3D image option in standard traffic condition. in 2 lane installations sensor should be able to provide accuracy of minimum 92%.
5	Measurement	Sensor should make 274 measurements on 4 planes with an opening angle of 96° with speed from doppler when radar is fixed inside the sensor.
6	Scan angle	96 degrees
7	Power consumption	Less than 7W, transmission power 16 dB
8	Data	Sensor should provide lane wise data
9	CE & RoHS Compliance	CE and RoHS compliant certificate
10	System	The System should have inbuilt processing unit and should not require additional CPU at site or at CCR

11	IP 65 Rating	Test reports for IP 65
12	OEM	The OEM should have experience of installing such sensors in India in at least 2 similar projects. Project executor should provide declaration.

SMART TRAFFIC SENSOR –B

Advanced 4D object tracking radar with UHD resolution.

It is important to have real-time data for the traffic flow on arterials and all strategic roads of the city.

The precise information from advance object detection for higher distances of 320 meters and above combined with counting and classification, with incident- and wrong-way detection with 4D UHD object tracking radar technology will help traffic planning and congestion control. All live information of incidents, wrong way traffic data can help ease traffic and plan it in a much better way.

S. No.	Features	Description
1	Technology	Forward Firing 4D object tracking radar with UHD resolution able to work in fog, rain and with all dust without any cleaning requirement. The sensor should be able to simultaneously track minimum 250 objects.
2	Number of lanes	The sensor should cover at least 8 lanes in dual direction and should detect 320 meters for trucks and 200 meters and above for cars. Minimum detection range of should be 1.5 m
3	Main features	System should continuously track vehicles in entire area and should provides, speed, direction, Volume / Class, Average speed with 85th percentile. Incident detection, wrong direction etc.
4	Main features	INCIDENT DETCTION: For incident detection applications, using Event Trigger Module, zones of interest should be configurable and can be combined with a specific event. If, for example, a car stops in the middle of a road or at the hard shoulder, the sensor should send a trigger message. Changes in speed should be detected immediately, vehicles slowing down are often an indication for possible incidents and should be detected and alarm raised. Sensor should also work for curved road. The RTS overlooking the road shall be able to signal the occurrence of incidents. Incidents shall be user definable and shall comprise at least presence, wrong way driving, warning of speeding and warning if vehicle speed/s is/are below or over a defined threshold.

5	Object tracking	the sensor should use (X, Y, speed) Cartesian coordinates or polar coordinates range, azimuth, elevation angle, as well as the speed vector of atleast 256 objects simultaneously in the field of view.
6	Frequency band	Frequency: 24.0 to 24.25GHz (K Band)/ 75Ghz GHz; 13dBm, 8 to 32 VDC, 12 W
7	Communication	Ethernet, RS485, CAN Bus, Relays (Option)
8	Shock Vibrations:	100g rms; 14g rms
9	Temperature:	-40 to 70°C
10	IP Ratting:	IP 67
11	Sale & Service	The OEM should have sales and service centre in India with clear authority from OEM and should have experience in some projects in india.
12	Minimum detection range and refresh time	1.5m (5ft) , refresh time should be better than 75ms
13	Speed Interval	-88.8 to +88.8m/s (-320 to +320km/h)
14	Refresh time data	Less than 70 m second
15	Connector	12 Pin plug Hirose LF10WBRB 12PD (Bayonet)
16	Azimuth Field of View	-50° to +50°
17	Surge protection	Option of Surge protection
18	Test Reports	Complete test reports from certified labs should be provided for FCC title 47 CFR Part15 & EN 300 440 with unwanted emissions in spurious domain
19	OEM	All Radars quoted for speed, for Vehcile detector, smart traffic should be from single OEM so as to avoid integration issues.

4.10.3 TRAFFIC ENFORCEMENT:

Dehradun smart city will have various traffic enforcement and E challan systems which will help make traffic more safe and mobile. The combination of ANPR systems, Red light violation and Speed enforcement systems based on instant and average speed system will help a lot.

4.10.3.1 Functional Specifications of ANPR

Sl. no	**Specification**	**Minimum User Requirement**

1	General	The entire ANPR process shall be performed at the lane location in real-time. The information captured of the plate alphanumeric, date-time, and any other information required shall be completed in approximately a few milliseconds. This information shall be transmitted to the Control Room for further processing if necessary, and/or stored at the lane for later retrieval. The ANPR systems will be fitted at all entry exits of city along with Traffic Sensor Type A (see specification). The sensors whould be integrated with ANPR system and should provide counting, classification, traffic flow, traffic status, gap, occupancy etc to help city traffic coordinators in planning traffic along with control of all vehcilur moments
2	Lane Coverage	Each camera system covers at least 1 lane having width of 3.5 meter or more.
3	Detection Zone	15 m to 20 m for ANPR data
4	Maximum Vehicle Speed	System captures clear images of all vehicles moving at a speed atleast 200 km/hr.
5	Vehicle Detection and Video Capture Module	The System shall automatically detect the license plate of all vehicles in the camera view in real time using video detection and activates license plate recognition software.
6	Optical Character Recognition	The system shall perform OCR (optical character recognition) of the license plate characters in real time. (English alpha-numeric characters in standard fonts). OCR accuracy shall be at least 90% during day time and 70% during night time for standard plates. System is should be able to detect and recognize the English alphanumeric License plate in standard fonts and formats of all vehicles including cars, HCV, LCV and two wheelers. The system is should be robust to variation in License Plates in terms of font, size, contrast and colour.
7	Network	Connectivity from site to control room shall be through proper network and local storage should be provided to account for any data loss.

8	Data capture and transfer	The OCR data of all vehicles along with the JPEG image of the vehicle etc shall be automatically transferred immediately to the nominated server in the Control Room. Each vehicle record shall be a single file and shall contain, as a minimum, an ASCII header that contains the following: a) vehicle registration number b) date and time that the vehicle is identified c) OCR confidence level d) ANPR site location, and e) All traffic flow info along with counting, classification, traffic status , speed etc The sensor should be able to send info on type of vehicle moment (BUS; TRUCK; CAR, AUTO , etc) It shall be possible to include one or more of the following in the same single vehicle record: a) image of the number plate b) image of the front of the vehicle from the ANPR IR camera, and/or c) wide angle vehicle / lane image (with additional scene camera). A detailed description of the file format can be finalized by the user to further develop post processing software.
9	OEM Experience	OEM should have experience with ANPR projects in India and should have at least done 3 such projects. Proper undertaking should be submitted

10	Hot List creation	The system shall have option to input certain license plates according to hot listed categories like “Wanted”, “Suspicious”, “Stolen” etc. The system should generate automatic alarms to alert the control room personnel for further action, in the event of detection of any vehicle falling in the Hot listed categories.
11	Alert Generation	On successful recognition of the number plate, system shall be able to generate automatic alarm to alert the control room for vehicles which have been marked as "Wanted", "Suspicious", "Stolen", etc.
12	Data Storage	The System shall store JPEG image of vehicle and license plate into a database management system like MySql, PostgreSQL etc. along with date timestamp and site location details.
13	Data Retrieval and Reports	The system shall enable easy and quick retrieval of snapshots, video and other data for post incident analysis and investigations. Database search could be using criteria like date, time, location and vehicle number. The system shall be able to generate suitable MIS reports as desired by the user. The system shall also provide advanced and smart searching facility of License plates from the database.
14	Context camera	System should have possibility to add context camera
15	Vehicle Counting and Classification	The system should have possibility to integrate with Traffic sensors
16	Integration with Third Part VMS	The system should be integrated with the proposed Video Management System.
16.1	Camera	The camera should be IP 66 and Complete camera unit should have CE certificate and test certifications. The box camera should have below specifications 1-1/2.8” progressive scan RGB CMOS or better 50 H with IR cut filter Colour: 0.15 Lux @ 30 IRE F1.3 1/66000 s to 2 s or better H.264 in High and Base profile, MPEG4, MJPEG Minimum 4 Streams in H.264, 2MP, 25 fps Resolution Minimum 1920 x 1080 Certification for box camera UL, CE

		Lens : should be minimum 3M , IR corrected 1/ 2.8
16.2	Illuminator	Integrated external Infrared capable to take images in night time and detect automatically number plate at distance of minimum 30 meters. The IR unit should be integrated with main camera with single power source. Safety report for the IR should be submitted
16.3	Processing unit	The industrial processor used should be able to work with 2 cameras. Should be minimum multicore, RAM 2 GB, with SD storage and USB storage options, temp -40 to 65 degrees and should consume max. 25 W. Or As required for the system.
16.4	Outdoor equipment housing	IP66 of better standards capable of withstanding vandalism and harsh weather conditions.(certification to be produced) Lightening arrester shall be installed for safety on each VMD
16.5	Data Storage at site	The output of the OCR process and all captured images shall be stored on an industrial processing unit (with internal solid-state memory storage device and can should work atleast 60 degrees) housed in the ANPR field cabinet. When the data storage reaches capacity, the image processor shall automatically over-write the oldest data. The system should push data automatically data to data centre in central site and raise alarms if any
16.6	Existing	Dehradun city already has few ANPR, RLVD systems and E fine Software. It is required that MSI understand the existing systems and proposed systems should be integrated to the existing systems. Letter for Integration

		should be submitted by the existing as well as proposed solution.

4.10.3.2 RED LIGHT VIOLATION

Sl no.	Specification	Minimum User Requirement
1	General	System should be totally digital
2	Vehicle violation criterion at Intersection	The system shall detect and capture vehicle details when: It violates the stop line/zebra crossing It violates the red light signal
3	Red Light detection	System shall be Non-Intrusive. It shall not be physically connected with traffic light and red-light status is detected without any physical connection to traffic light.
4	Fair System	Red light system shall be completely fair system with all evidences captured before and after the red light jumping infraction has happened.
5	Lane Coverage	Each camera system shall cover at least 1 lane having width of 3.5 meter or more.
6	Detecting Vehicle Presence	Red light system should detect vehicle presence without intrusive sensors like magnetic loops. This is to avoid street working during installation and to reduce maintenance cost
7	System Mounting	System can be composite unit with all components inside the IP65 box OR comprised of camera or other units mounted on poles or gantries with controller and processors at side poles to make sure all lanes of the road are covered.
8	Number Plate Capture	System should be able to recognize automatically the number plate of cars in violation. The system shall perform OCR (optical character recognition) of the license plate characters (English alpha-numeric characters in standard fonts). ANPR system works with Indian number plates

9	Accuracy of Number Plate capture (ANPR)	OCR accuracy shall be at least 80% 90%during day time and 60% 70%during night time for standard plates
10	Infraction data to be provided by system	Date, time, location of incident image of vehicle, speed, Image of the number plate, text conversion of number plate after OCR
11	Context Image	System shall provide Context image (always color to have proof of signal light) of the signal and shall show wide angled context of the offence as well as details of the offending vehicle. Multiple stitched images of the same should be is possible. The system shall produce, store and transmit a sequence of at least 6 image relatives to red light violation, or a movie in standard format like avi, mp4, mov, vfw etc
12	Speed detection	Option of Integration with speed system should be provided. The proposed solution should have certification for RED SPEED:
13	Cameras specifications	The camera should be IP 66 and Complete camera unit should have CE certificate and test certifications. The box camera should have below specifications 1-1/2.8” progressive scan RGB CMOS or better 50 H with IR cut filter Colour: 0.15 Lux @ 30 IRE F1.3 1/66000 s to 2 s or better H.264 in High and Base profile, MPEG4, MJPEG Minimum 4 Streams in H.264, 2MP, 25 fps Resolution Minimum 1920 x 1080 Certification for box camera UL, CE Lens : should be minimum 3M , IR corrected 1/ 2.8
14	Data Retrieval and Reports	Database search could be using criteria like date, time, location and vehicle number. The system should be able to generate suitable MIS reports as desired by the user.

15	IP camera for License Plate Capture	The system shall support all standard brands. One camera shall cover at least 3.5 meter width of lane, and capture the license plates of vehicles which violates the traffic signal and moving at a speed of 0 to 200 km/hr
16	IR Illuminator	Integrated external Infrared shall be capable to take images in night time and detect automatically number plate at distance of minimum 25 meters. The IR should be integrated with camera unit with single power source. Eye safety test report should be submitted
17	Working temperature	0 to +60 deg.C
18	Security	Standard Digital signature on each violation to assure data integrity. Strong encryption on data during local storage and data transfer to back office
19	Local Storage	Minimum local storage 64 GB. Industrial processing unit should be provided as per solution requirement.
20	Communication	Connectivity from site to control room shall be through fiber optic/leased lines or better with minimum uptime of 99.5%
21	Alert Generation	On successful recognition of the number plate, system shall generate automatic alarm to alert the control room for vehicles which have been marked as "Wanted", "Suspicious", "Stolen", "Expired".
22	Compliance certificate	CE and RoHS compliant certificate
23	Proof of infraction	Complete images with time stamp should be available.

24	BACK office software	The system should provide facility to privileged users to manually check the entry in database using standard Web browsers and edit the numbers which may be wrongly OCR-read, before the numbers are fed to the Challan generating sub-system. An audit trail should be maintained to record such editing activities. No deletion or addition of data without validation, proper password protection The system should provide facility to search for the cases of violations occurred during any specific span of time, and provide a statistical analysis of the number of such incidences occurring during various days of the month
25	Challan	System can should be integrated with E-challan generating systems with fine generated for each infraction with multiple images clearly showing color of red light signal and violation (i.e. color image of context camera), date, time, vehicle registration number, classification of offence, speed of violating vehicle, notified speed, etc.
26	Integration	Dehradun city already has few ANPR, RLVD systems and E fine Software. It is required that MSI understand the existing systems and proposed systems should be integrated to the existing systems. Letter for Integration should be submitted by the existing as well as proposed solution.
27	Certifications:	As Speed might be part of some RED LIGHT VIOLATION systems. It is required that System proposed should have proper TEST reports and CERTIFICATIONS for speed violation from certified labs who are authorized to issue certificates for speed enforcement. The proposed speed systems should b to OIMeen tested as per OIML R 91, D11 compliance requirement
28	SPEED DETECTION	Option of Speed detection should be available and proper TEST reports & Certificate in name of OEM for the solution should be submitted. OIML R 91 and D 11 should be in name for the complete solution. The proposed sensor for speed should not be dependent on image and should provide image of all vehicles irrespective of Plate type or script.

		Sensor should work in Fog, rain and should not require cleaning.

4.10.3.3 SPEED VIOLATION DEDUCTION SYSTEM (SVD)

S No.	Specifications
The broad technical and functional specifications of the required speed violation check camera systems given in the following paras	
1	Traffic violations should be automatically detected by the system. System should provide image of over speeding vehicle with control image for speed test.
2	Complete data for each infraction should be provided: data, time, location, speed, with automatic number plate detection mechanism (to recognize vehicle automatically)
3	System should generate automatically the number plate of the Vehicle automatically
4	System can be composite unit with all components inside the IP65 box Or comprised of camera or other units mounted on poles or gantries with controller and processors at side poles to make sure all lanes of the road are covered. Preferred systems will be systems installed at minimum height of 5 meters and above.
5	System should work in day and night condition
6	-Speed should be measured use using advanced forward firing radar technology -Speed should be measured using 3D advanced radar Frequency band should be 24.0 to 24.25 GHz or 77 GHz Max. Transmit Power (EIRP)- 20 dBm Operating temp -40 °C ,85 °C -Speed: 30 -320 km/h -Range Accuracy typ. <+/-2,5% or +/-0,25m (bigger of) -Speed Accuracy : typ. <+/-1% or <+/-0,28m/sec(bigger of) -Tracking radar with possibility to take control image -Cycle Time. -50 Msec -Vibration; 14g rms -Power Consumption: 7V - 32V -Lanes : Multilane

	Number of tracked objects : 64
7	System should provide color image at least in daytime
8	Camera Unit: The camera should be IP 66 and Complete camera unit should have CE certificate and test reports for IP 66 The box camera should have below specifications 1-1/2.8" progressive scan RGB CMOS or better 50 H with IR cut filter Colour: 0.15 Lux @ 30 IRE F1.3 1/66000 s to 2 s or better H.264 in High and Base profile, MPEG4, MJPEG Minimum 4 Streams in H.264, 2MP, 25 fps Resolution Minimum 1920 x 1080 Certification for box camera UL, CE Lens : should be minimum 3M , IR corrected 1/ 2.8
9	Integrated external Infrared capable to take images in night time and detect automatically number plate for minimum 20 meters.
10	Control : speed setup Km/hr, atleast 250 km/hr ± 3%
11	Working temperature -5 to +60 deg.C, 80% and above humidity
12	Processor: minimum local storage 64 Gb, multicore processor GUI for configuration and diagnostic Security: Standard Digital signature on each violation to assure data integrity. Strong encryption on data during local storage and data transfer to back office
13	BACK office: the system should provide data decryption and storage, automatic challan issue possibility with automatic number plate detection with multiple images. No deletion or addition of data without validation , proper password protection The system should have header and footer as per Dehradun Police SOP. MSI should assure that proposed speed enforcement solution should be integrated to existing speed solution and should have all certifications for speed authenticity. The specifications in this document has taken in consideration of existing systems used by Dehradun police.
14	Possibility to import data files and infractions should be provided as per Dehradun police requirement. Violation retrieval should be available for selected location, time and number series (one time configuration of software as per Dehradun police requirement should be considered
15	System should be able to recognize automatically the car's number plate of cars in violation the accuracy should be more than 70% in day and 60 %night condition. ANPR

	system should be capable to work with Indian number plates and should preferably have experience in Indian plates.
16	Communication, the system should have proper communication with control room and should be able to provide online infraction reports and live infraction. Automatic number plate detection should be part of the system
17	Back office computer: MSI should assure that systems proposed are integfrated to existing E Fine systems used in Dehradun police.
18	Stability of product and after sale services: Bidder should have local support engineers and system should be repairable or replaceable locally. Bidder should show spares availability for minimum 2 such systems
19	Certifications: The Quoted solution should have OIML R 91, OIML D11 and Welmec 7.2 test certification compliance (India is signatory to OIML regulations). The system should have proper test reports for speed accuracy and should have legal decree in name of OEM from EU/US/JAPAN/UK/SWIZERLAND/SOUTH AFRICA/CANADA The certification copy should be authenticated by Indian embassy (to authenticate that systems are legalized and tested for infractions to avoid legal issues) or should have Apostille. Speed test reports to be submitted from third party (authorized company to issues test reports for E fine generation for speed) before date of publication of tender. Product should already be in use with enforcement authorities and should be in use for generating fines and legal decree/should be in name of solution OEM and not sensor.
20	CE and RoHS compliant certificate with third party speed test report
21	Test reports for IP 66 for cameras, laser should be provided. this is to support harsh rainy season and dust environment in Dehradun
22	Certification should be provided for the system (and not for the sensor only) and Road test reports should be tested for speed tests.
23	It is MSI responsibility to propose solution after cross checking the authenticity for speed enforcement.

4.10.3.4 Average Speed (Point to Point) Violation System (SVD2) Functional Specifications

Sl n0.	**Specification**	**Minimum User Requirement**

1	General	Technology to be used is non-intrusive. The measure of vehicle speed shall be the Average Speed in a control section. The system may also be used for measuring Instant Speed at any point(as option) All vehicles passing through the control section at a Speed greater than a determined speed limit (values to be made configurable via software) shall be detected as violation and System shall produce a sequence of relative images (or a movie) with value of speed detected and executing ANPR process to automatically extract number plate of vehicle in infraction. The system should not be based on ANPR and should be able to find speed of non readable ANPR vehicles. System shall have provision for setting different speed thresholds for minimum of two vehicles categories (light, commercial). System shall work in day and night conditions and should be
2	Data capture	Cameras fitted in the equipment shall record a digitized image or video frames of the violation covering defined lanes on each approach arm at any point of time simultaneously with relevant data about the offence, i.e. date, time, fixed location and speed etc. The photograph generated by the system at both locations shall be stitched together and ANPR be performed. The results are independent of number plate recognition at individual points.
3	Camera Unit	The camera should be IP 66 and Complete camera unit should have CE certificate and test certifications. The box camera should have below specifications 1-1/2.8” progressive scan RGB CMOS or better 50 H with IR cut filter Colour: 0.15 Lux @ 30 IRE F1.3 1/66000 s to 2 s or better H.264 in High and Base profile, MPEG4, MJPEG Minimum 4 Streams in H.264, 2MP, 25 fps

		Resolution Minimum 1920 x 1080 Certification for box camera UL, CE Lens : should be minimum 3M , IR corrected 1/ 2.8
4	IR Module:	External IR (no flash) Distance: 25 meters with 20 degrees beam IR Eye Safe report should be submitted
5	Housing	The mounting(s) shall house all the required connections including the electricity and network connectivity. It also houses the microprocessor unit and electronic interface with the sensors, camera(s) etc. and an UPS The housing(s) confirms to IP 66
6	Optional Instant Speed	In case if instant speed system are installed along with Average speed the instant speed systems should be in compliance to OIML R 91, D11 and Welmec 7.2
7	Calibration	The OEM should be certified lab for Average Speed system and should have certification for it.
8	Calibration	The vendor shall calibrate the cameras from time to time and ensure that the calibration certificates are provided to the client to ensure accuracy of system.
9	Certificates	The system should have legal decree/homologation certificate. OEM should also submit road test report/calibration reports from lab whose certifications are accepted for fine generation on country of origin.
10	Accuracy	Accuracy should be higher than 90 percentage on free flow traffic for test and for all vehicles passed. System should not miss vehicles with bad ANPR plates
11	Violation Retrieval	Violations should be available for selection from a displayed list corresponding to each location separately. The retrieval could be sorted by date, time, location and by vehicle registration number.
12	Statistical Analysis	Various automated reports should be available for hourly data, infraction per hour/day week etc.

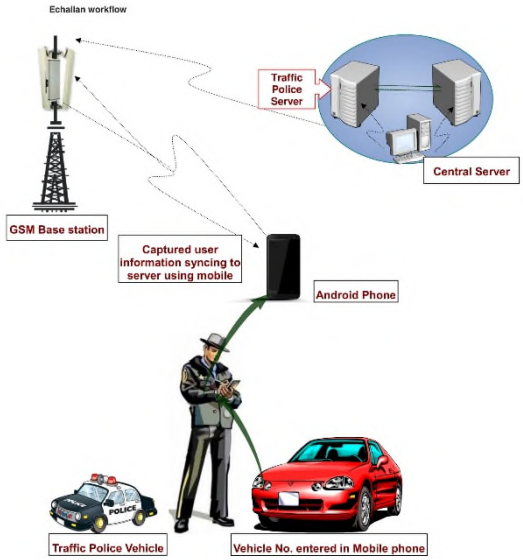
13	User Interface	The user interface broadly falls into the categories of viewing, sorting and printing violations and system configuration/housekeeping. The violation viewer shall be provided with a means of listing the invalid violations along with the reason(s) of invalidation without deleting the original record(s). Complete database management and E fine issuance Software shall provide interface for taking printouts of violations. There shall be a password access system along with user type (admin, user). It permits role based permission system for accessing the data base and printouts.
14	OEM	OEM of the proposed solution should give an undertaking that the proposed solution is already in use with atleast 10 enforcement agencies and fines are being generated for average speed. Any Patent infringement will be taken care by OEM/MSI
15	Local Processing Unit	The industrial processor used should be provided with each camera . Should be minimum multiple core , RAM 2 GB, with SD storage and USB storage options, temp -40 to 60 degrees and should be part of system. Or any industrial processor as required for the system working.
16	Speed enforcement	Approval from ministry of traffic or equivalent department from respective country of origin for speed enforcement , document authenticated by Indian embassy (to authenticate that systems are legalized and tested for infractions to avoid legal issues). Or systems should be submitted with apostille stamped. It is required that MSI provides system which are dully certified and is able to prove that systems are certified and stand in court of law.
17	Integration	The proposed solution should be integrated to existing E fine systems for Speed enforcement at Dehradun police.

4.10.4 Automatic E Challan & Centralized monitoring with TARS

The proposed system should be a comprehensive digital solution for Transport enforcement wing and Traffic Police delivered through an Android based mobile application and a web portal. The system should capture all challans information by infield officer using android device at the time of violation and capture information will be sync to centralized server.

The system should be integrated with Vahan and Sarathi applications and provides a number of user-friendly features, covering all major functionalities of Enforcement System. An end to end digital solution for multiple stakeholders: ease of operations for Transport Enforcement

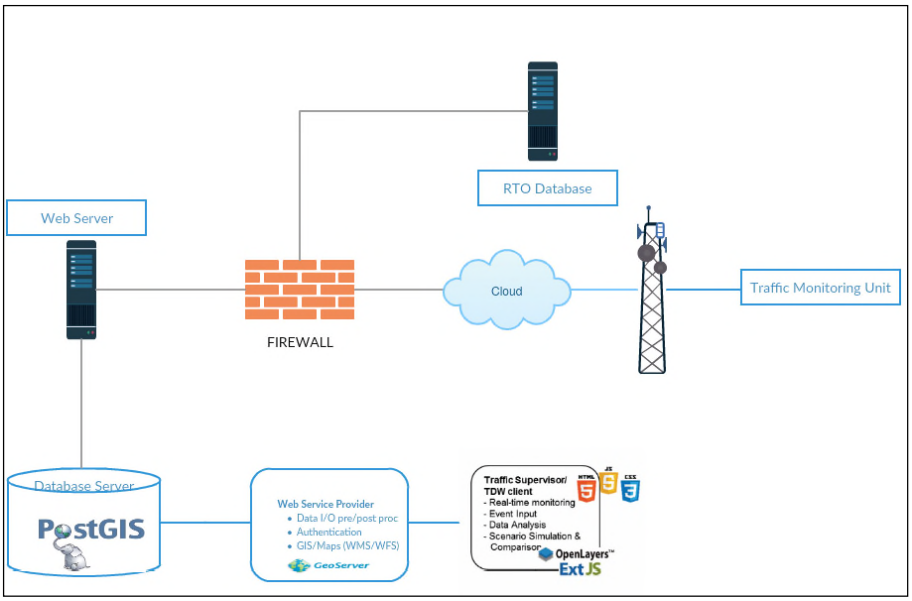
Officers/Traffic Policemen, increased visibility in operations for the State Transport department and improved support in maintaining compliance for citizens should be considered.



4.10.4.1 SPECIFICATIONS FOR E CHALLAN

S. No	Functionalities of Echallan system.
1)	E-challan software shall work in client- server mode, where the devices units, workstation units will act as clients connected to the server through cellular network for data transfer
2)	E-challan system shall be able to retrieve vehicle owner's details and vehicle data from RTO data base to minimize data entry.
3)	E-challan system shall be able to retrieve vehicle system registration details and driving license details by reading appropriate smart card to minimize data entry.
4)	Server should maintain log of all current devices. Any access to the system must be recorded along with data, time user id and IP address.
5)	Traffic officer should log in to the hand-held device through the unique user id and password or smart card issued or the purpose.
6)	A unique Challan number should be generated through client software for each challan.
7)	As soon as a vehicle registration number is entered, the handheld device should automatically check from the server if the vehicle is stolen, wanted in any criminal case or is in the list of suspicious vehicles.

8)	The most frequent traffic offences should be kept at the top of the drop-down menu and offence ingredients should be available if required by officer.
9)	Date, time and GPS coordinates of place of challan should be automatically populated in the relevant fields of client software.
10)	Compounding amount must populate in the field automatically from master table.
11)	The successful bidder should develop the GUI and functionality as per requirements.
12)	It should be possible to integrate payment gate way operator with the system for facilitation of payment.
13)	The Application Software should work in a web based environment.
14)	The application software should be user friendly, easy to operate.
15)	The system will function in web based system where the hand-held device shall work as a node.
16)	The application software should maintain the logs of user activities to facilitate the audit trail.
17)	Database server should be able to handle the activities of all the handheld devices at one time simultaneously with huge database size of prosecution, ownerships, driving license etc. without affecting the performance.
18)	The software should be able to generate various periodical reports, summaries, MIS reports, query reply etc. as per the requirements.
19)	Administrator should be able to modify the master tables as and when required and should have the capability to push the changes to hand –held devices.
20)	All database tables, records etc. required for various dropdown menus etc. shall also be created by the vendor.
21)	E-challan system should show alert on Hand held device in case Speed system detect any violation.
22)	In case of speed violation, Echallan system will send alert and SMS to nearby officer using geofence.
23	It is required that MSI integrate existing E Fine system used for Dehradun police for speed enforcement and E challan. Integration responsibility lies with MSI



Minimum Hand Held Devices Requirements:

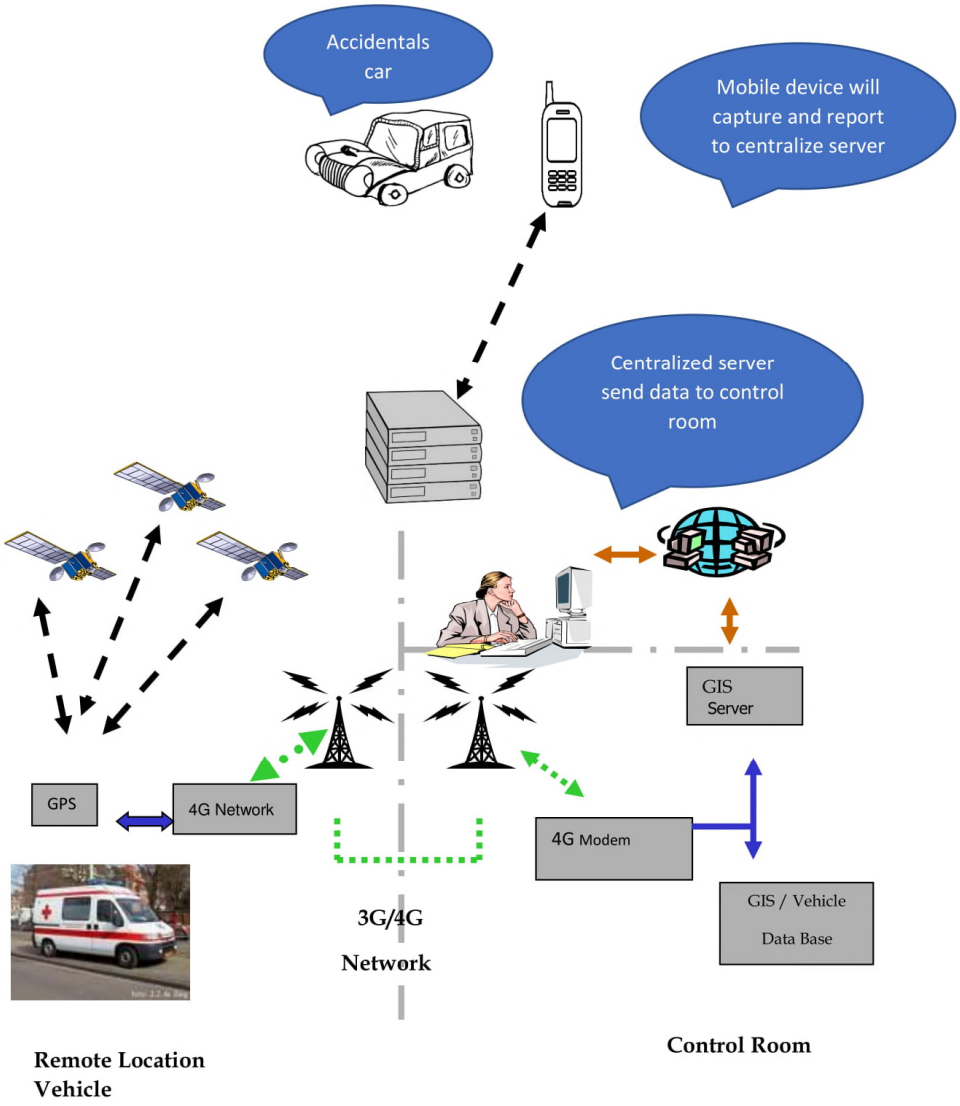
S No.	Parameter	Description
1)	Operating System	Android
2)	OS version	Android v5.0 and Above
3)	Processor	Min 800 MHz
4)	Memory (Flash Rom)	Min 8 GB
5)	RAM	Min 1 GB
6)	Extend Slot	Micro SD 32 GB
7)	Display	Min 3.5 inch
8)	Touch Screen	Yes
9)	GPS	Yes
10)	Bluetooth	Yes
11)	Wifi	Wifi (802.11 b/g/n)
12)	Thermal printer	Yes
13)	Barcode scanner	1D and 2D scanner
14)	Protection class	IP55
15)	Drop resistance level	1.5m
16)	Camera	Min 3 MP

4.10.4.2 Tars system.

Tars system should provide the accident investigator with advanced techniques in accident data storage and analysis with tools to identity blackspots, analyse root causes, and for isolating common features in accidents. A visualization package that combines advanced accident analysis with location mapping features shall be provided.

Tars system shall consist of:

- Accident reporting system.
- Accident recording system.
- Analysis of accidents.



Tars system has designed and implemented on server and client base architecture. Tars system will record and capture accident using mobile application on the accidentals site and after capturing information data will be sync to centralized server, which will further send data to control room. User also can report accident information to web based application.

All information can be manipulate using centralized server which will be accessible from control room, user can track nearby ambulance in case they get any accident information on web base application and can send alert to nearby ambulance and nearby police station.

On accidentals site user can capture information using hand handled device which will be push to server and will show alert on control room.

Functional requirements of the Tars System:

S. No	Functionalities of Tars system.
1)	Tars application should be a browser based software application that allows operator and other users who have access to perform all of their traffic management related function.
2)	Tars application shall work in client- server mode, where the devices units, workstation units will act as clients connected to the server through cellular network for data transfer
3)	Tars application GUI shall be fully browser-based, allowing authorized users of the software to access the system without the need for any client-side software.
4)	Tars application shall have response plan/ Standard Operation Procedures (SOPs) feature.
5)	Tars software shall work in client- server mode, where the devices units, workstation units will act as clients connected to the server through cellular network for data transfer
6)	The system should not allow unauthorized users to register and alter accident records.
7)	The system must be simple and easy to be used by all its potential users
8)	Tars application should display historical accident data on map.
9)	Tars application should able to send alert to nearby ambulance.

4.10.5 Variable Message sign board application

- Central Control Software shall allow controlling multiple VMSB from one console.
- Capable of programming to display all types of Message having alphanumeric character in English and Hindi and combination of text with pictograms signs. The system should have feature to manage video / still content for VMSB display.
- The system shall have capability to divide VMSB screen into multi parts to display diverse form of information like video, text, still images, advertisements, weather info, city info etc.
- Capable of controlling and displaying multiple font types with flexible size and picture sizes suitable as per the size of the VMSB.
- Capable of controlling brightness & contrast through software.
- Capable to continuously monitor the operation of the Variable Message sign board, implemented control commands and communicate information to the Traffic Monitoring Centre via communication network.
- Real time log facility – log file documenting the actual sequence of display to be available at central control system.
- Multilevel event log with time & date stamp.

- Access to system only after the authentication and acceptance of authentication based on hardware dongle with its log.
- Report generation facility for individual/group/all VMSBs with date and time which includes summary of messages, dynamic changes, fault/repair report and system accessed logs, link breakage logs, down time reports or any other customized report.
- Configurable scheduler on date/day of week basis for transmitting pre-programmed message to any VMSB unit.
- Various users shall access the system using single sign on and shall be role based. Different roles which could be defined (to be finalized at the stage of SRS) could be Administrator, Supervisor, Officer, Operator, etc.
- Apart from role based access, the system shall also be able to define access based on location.
- Rights to different modules / Sub-Modules / Functionalities shall be role based and proper log report should be maintained by the system for such access
- Components of the architecture must provide redundancy and ensure that there are no single points of failure in the key project components. To take care of remote failure, the systems need to be configured to mask and recover with minimum outage.
- The architecture must adopt an end-to-end security model that protects data and the infrastructure from malicious attacks, theft, natural disasters etc. provisions for security of field equipment as well as protection of the software system from hackers and other threats shall be a part of the proposed system. Using Firewalls and Intrusion detection systems such attacks and theft shall be controlled and well supported (and implemented) with the security policy. The virus and worms attacks shall be well defended with Gateway level Anti-virus system, along with workstation level Antivirus mechanism. There shall also be an endeavour to make use of the SSL/VPN technologies to have secured communication between Applications and its end users. Furthermore, all the system logs shall be properly stored & archived for future analysis and forensics whenever desired.
- 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.
- System shall use open standards and protocols to the extent possible
- Facility to export reports to excel and PDF formats.

Remote Monitoring

- All VMSB shall be connected/configured to Traffic Monitoring system for remote monitoring through network for two way communication between VMSB and control Room to check system failure, power failure & link breakage.
- Remote Diagnostics to allow identifying reason of failure atleast the level of failed individual LED.

The broad scope of work to be covered under this component shall include the following, but is not limited to:

- Variable Message Sign Board (VMSB) referred herein) shall be installed at identified strategic locations. The location of VMSB shall be on the key junctions (mostly on the sides without obstructing the traffic) and other strategic locations with large foot fall. The VMSB software application will allow user to publish specific messages for managing traffic and also general informative messages.

- VMSB shall enable DSCL/ Police to communicate effectively with citizens and also improve response while dealing with exigency situations. These shall also be used to regulate the traffic situations across the city by communicating right messages at the right time.

Functional & Technical Requirements

1. The system shall be capable to display warnings, traffic advice, route guidance and emergency messages to motorists from the DICCC in real time.
2. The system shall also be capable to display warnings, traffic advice, route guidance and emergency messages to motorist by using local PC/Laptops. The system shall display graphical representation of the lanes with directional arrows and colour such as green, yellow, red for depicting density of traffic
3. The VMSB shall display text and graphic messages using Light Emitting Diode (LED) arrays.
4. The System shall able to display failure status of any LED at DICCC.
5. The System shall support Display characters in true type fonts and adjustable based on the Operating system requirement.
6. The DICCC workstation shall communicate with the VMSB controller through the network. It shall send out command data to the variable message sign controller and to confirm normal operation of the signboard. In return, the DICCC workstation shall receive status data from the VMSB controller.
7. VMSB controllers shall continuously monitor the operation of the VMSB via the provided communication network.
8. Operating status of the variable message sign shall be checked periodically from the DICCC.
9. It shall be capable of setting an individual VMSB or group of VMSB's to display either one of the pre-set messages or symbols entered into the computer via the control computer keyboard or by another means.
10. It shall be capable of being programmed to display an individual message to a VMSB or a group of VMSB's at a pre-set date and time.
11. A sequence of a minimum of 10 messages/pictures/ pre-decided sign or group of signs shall be possible to assign for individual VMSB or group of VMSB's.
12. It shall also store information about the time log of message displayed on each VMSB. The information stored shall contain the identification number of the VMSB, content of the message, date and time at which displayed message/picture starts and ends.
13. The central control workstation shall perform regular tests (pre-set basis) for each individual VMSB. Data communication shall be provided with sufficient security check to avoid unauthorized access.

4.10.6 Public Address System – Functional

Public Address system shall be used at intersections, public places, market places or those critical locations as identified by Purchaser to make important announcements for the public. It shall be able to broadcast messages across all PA systems or specific announcement could be made to a particular location supporting single zone /multi zone operations.

The system shall also deliver pre-recorded messages to the loud speakers attached to them 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.

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

Public Address System Specifications

Sr. No	Parameter	Compliance Yes/No	Reference Document
1	Should have the capability to control individual PAS i.e. to make an announcement at select location (1:1) or multiple locations (1: many). The PAS should also support both, Live and Recorded inputs		
	Field Side Equipment		
2	IP amplifier with minimum 250 Watts, Class D.		
3	Native IP connectivity, no convertors to be used		
4	0 to 55 C Temperature rating for Amplifier		
5	Automatic Volume Control		
6	Frequency Response: 50Hzto 15000 Hz for Amplifier		
7	2Inputs and 1Output relay contacts in Amplifier		
8	Speaker: Minimum 4 Speakers 20 W capacity		
9	Frequency Response of Speaker 350 - 10,000Hz		

10	Line Monitoring Facility for speakers		
11	IP 55 Housing for amplifier		
Control Side Equipment			
1	Central Software based server application capable of working on virtual environment/cloud with 100% redundancy		
2	Access control mechanism would be also required to establish so that the usage is regulated.		
3	Integration with VaMS and Command and control centre or any other component if required		
4	PA Master Controller to have facility for multiple mic inputs, direct dialling buttons, LCD screen		
5	Software Client for making Calls to PA and ECB		
6	Automatic Volume Control		
7	Transmission bandwidth16000 KHz		
8	Operating temperature for control desk 0 to +60C		

4.10.7 Emergency Call Box – Functional

A high-quality digital transceiver, to be placed at certain key locations.

Key is to make it easily accessible by public

The unit shall preferably have a single button which when pressed, shall connect to the Doon Integrated Command and Control Centre over the existing network infrastructure setup for CCTV Surveillance system

At some locations, this can be also used for Public Address

These shall be installed at select locations such as Traffic Junctions, Smart Bus Stops, and pedestals or within the vicinity of constant supervision to avoid misuse and vandalism of the call box.

ECB will be prime importance along with the surveillance system mentioned in section 4.8 For safety and security of citizen especially women as well as for helping elders/children during any emergency

II	**ECB Technical**	
	Field Side Equipment Compliance	
S. No.	**Parameter**	**Compliance Yes/No**
1	Construction: Cast Iron/Steel Foundation, Sturdy Body for equipment	
2	Call Button: Watertight Large Push Button, Visual Feedback for button press	
3	Connectivity: GSM/RF/PSTN/Ethernet as per solution offered	
4	Sensors: For tempering/ vandalism	
5	IP66, IK09 Protection	
6	Operating Temperature 0 to 70 C	
7	Speaking Distance minimum 5 ft	
8	Inbuilt Class D Amplifier	
9	Minimum 3 Inputs ad 2 Output relay contacts	
10	ECB should be able to make calls to the PA system	
CCR Side Equipment		
1	Central Software based server application capable of working on virtual environment/cloud with 100% redundancy	
2	Access control mechanism would be also required to establish so that the usage is regulated.	
3	Integration with VaMS and Command and control centre or any other component if required	
4	PA Master Controller to have facility for multiple mic inputs, direct dialling buttons, LCD screen	
5	Software Client for making Calls to PA and ECB	
6	Automatic Volume Control	
7	Transmission bandwidth16000 KHz	

8	Operating temperature for control desk 0 to +60C	

4.11 Transit Management System

The City of Dehradun plans to induct E vehicles as part of city vision of " green, Clean and Economically vibrant city with healthy and safe citizens". The city would induct 30 Electric Buses along with 200 e-rickshaws.

The transit management solution shall bring a system for enhancement and monitoring of its fleet for safety , efficiency for its operations. The system is expected to meet the Authority's objective of enhancing service standards, Informed commuters with efficient operations.

The project also intends to increase security and safety aspect by installing vehicle tracking devices in the buses and e-rickshaws.

The system will deliver the stakeholder requirements by deploying technologies onto an integrated platform which will should cater to following requirements of the city

Sr. No.	System	Sub System
1	Vehicle Tracking System	Automatic Vehicle Location System for city buses
		Automatic Vehicle Location System for e-rickshaws
2	Smart Bus Stops	Passenger Information System Display
		CCTV Camera
		Small VMD for advertisements and information
		Panic Button for 2 way communication

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

Functional Requirement

Automated Vehicle Location System

The Automated Vehicle Location System (AVLS) shall primarily use Global Positioning System (GPS) for location tracking with the devices mounted on the vehicle as primary source of data for tracking purposes. The location and associated data acquired from the vehicle units

shall act as input source at DICCC for various processes for management of various functions as required by user executing their specific functions.

The solution shall enable the team at DICCC to monitor vehicle movement in real-time and synthesize the AVL field data to deliver the same on the public information system devices. The AVL data from vehicles shall be delivered to individual process owners within Dehradun Smart City for further use and processing based on the requirements identified for individual departments.

The AVLS shall be source for enabling public information system service which acts as a source of information to be made available across various types of end point devices like mobile, fixed displays, web etc. in form of text &voice. The AVLS for city bus shall essentially comprise of following components:

- Bus Mounted GPS based controller with two way communication interface.
- GIS Based Fleet Monitoring and Control System
- Passenger Information System (PIS)

The central AVLS system should offer functionality to manage diversity of end use requirement as may be required by transport department for operational use purposes. This should be facilitated by use of GIS platform and allowing customization of views with respect to asset identification, tracking and process management.

The AVLS system will essentially offer following features

• Service Monitoring

• BUS Live

• Messaging

• GIS Console

• Alarms and Alerts

• Equipment status etc

• Key Performance Indicators

• General Fault Reports

The system will also be compliant to GTFS / inter-operable data formats to enable external technology ecosystem provider to build complimentary applications to further boost consumer-oriented delivery and service environment.

Automated Vehicle Location System for E-rickshaws

The AVLS for E-Rickshaws should comprise of following components:

VTS installed for vehicle tracking to transmit their real time information to the DICCC and to the officials. The AVLS system will improve the operations and accountability of these Vehicles as they will be mapped with their KPIs.

Tracking of E-Rickshaw will provide safety aspect to the citizens. The flow of information will be through GPRS/GSM/LoRa based system.

Since Dehradun is looking at creating a green city Environment friendly and mass transit plays an important role in achieving the goal. And bus stops formulate an important element in the

mass transit as commuters need a safe and smart bus shelters to have the required comfort and safety before they board the bus. Hence smart and safe bus stops provide passengers the needed information like ETA, Required Lighting for Safety and Surveillance cameras with panic buttons in case of any eventuality.

The Smart Bus Shelters will house following elements connected to DICCC via OFC

A. PIS system
B. CCTV camera
C. Panic Buttons
D. Smaller Size VMDs.
E. Smart LED Lights

A. PIS system will be as below:

- PIS Display on Bus Stop
- PIS at bus stop will be connected through OFC to Central Control Centre
- GIS module to generate the ETA information for various bus stops
- PIS algorithm to be used for ETA/ETD prediction, considering historical data, GPS data,
- Traffic data and others operating parameters
- PIS at Depot cum Terminal and Bus Stops/Shelters
- LED based Passenger Information Displays (Stops will have 1 number of LED based display terminals).
- The MSI 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 vendor for the entire duration of the contract.
- Power for PIS displays will be facilitated and provided by the department.

B. CCTV Surveillance Camera

Each Bus Shelters will host a Fixed Box Camera in it. For Functional Requirement of Surveillance Camera, please refer to compliance in section 4.9.4

C. Panic Button

For safety and security of citizen especially women as well as for helping elders/children during any emergency, Smart Bus Shelters will also host an ECB through which citizen can alert the authorities. For functional /Technical Requirement of ECB, please refer to section 4.7.7

D. Variable Message Display

Smart Bus Shelters will also host Smaller Size VMDs, which can be sued for advertisements as well by Government/Authorities to push important/emergency alerts or messages. For Functional/Technical Requirement of VMDs, please refer to section 4.7.5

F. Centralized control centre

All the AVLS and PIS equipment will be integrated with the DICCC. This one DICCC 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, Incident management (Accident and Breakdown).

The vendor shall develop application module with Dashboard for each of the modules and role based access for the smooth operation of Central control center, and shall deploy support and maintenance manpower at the central/depot control center.

G. Communication Overview

The figure below shows a pictorial representation of the communication network plan for city bus and E-Rickshaw for the VTS connected vehicle 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 and E-Rickshaws, bus station, depots, terminal's, data centre, control centre and data recovery site is concerned.

H. General Packet Radio Service (GPRS)

The information captured by the Integrated Control unit is to be transmitted to the control station server through GPRS/GSM network creating a communication network between Bus, and DICCC. The communication network is connected to the internet for accessing information regarding bus arrival, routes etc.

I. 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.

J. 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. Vendor may use [the Authority] existing GIS base-map or Google map for this purpose

Smart Bus Stop

Smart Bus Shelters will deploy following elements (but not limited to) Passenger Information System, CCTV camera, ECB, VMDs etc. The components shall consist of LED based display system for bus shelters, Terminals and Buses, Fixed Box Camera, VMDs etc.

Following are the technical specifications for these units.

PIS at Bus Shelters and terminals

The passenger information system shall comprise of following –

Display Screen on Bus Shelters

LED based display screens that provide sufficient visibility in broad daylight condition shall be installed at Bus Shelters. Each Bus shelter would consist of two displays. They shall display –

Route Number, Route Details and estimated arrival time (ETA)

The display shall receive encoded information of route and ETA from the AVLS control system through the common wired/wireless communication link set up at each bus shelter. The displays must have the ability to decode the information received from DICCC and display appropriate message on the screen. LED Board at Bus Shelters shall have the following functional specifications:

a. Display of PIS in a display unit at bus shelter shall be configurable based on bus shelter. Single unit should display services of more than one platform.

b. Information Display units will be supplied and mounted appropriately, configured and commissioned by the MSI.

c. PIS information shall be displayed in Hindi and English alternatively

d. At all these bus shelters, display units will receive/display transmitted contents from the central system through a gateway or mention other suitable means in the technical architecture.

e. Display systems needs to support full colour display for streaming advertisements, Digital display of text, images and video on LED screens.

f. Displayed messages must be readable in high bright, day light.

g. Display system in addition to the display of information for PIS shall be capable of displaying advertisements and multimedia content at the bus shelters and may need to alternate between Passenger information and Advertisements.

h. The frequency and period of information display on PIS display shall be configurable from central location for advertisements and other transit information.

i. Display shall provide for modular configurable layout enabling parallel display of content on different areas of the screen Real time Transit information (Routes, ETA, Type of service,Fare, Time/Date, Public announcements, Safety information, Commercial advertising, a ticker tape at the bottom for text announcements /advertisements, other local Tourist information).

j. All displays for PIS will have a configurable refresh rate with minimum of 10 seconds.

Display System Technical Requirement (PIS)

a. Display units shall be mounted on a rugged enclosure to withstand harsh environmental conditions with reasonable physical security.

b. Display will be located at a convenient height to have a clear view of the message of next arrival bus.

c. Fitment provision will have to be provided in the Bus stations. The power supply shall be made available by Dehradun Smart City.

d. One Integrated tamper proof casing for complete PIS Unit addressing physical security considerations.

e. Provide any hardware like PC, networking, etc. required to run the PIS and advertisements on LED Display Units.

f. Ensure smooth transition from main power supply to UPS in case of power outage.

g. Aesthetic requirements such as fonts, colours, rows per page, display time to be remotely configurable and displayed based on business requirement.

Panic Button

1. A high quality digital transceiver, to be placed at smart bus stops

2. Key is to make it easily accessible by public

Sl no	Minimum Specifications		Bidder Compliance (Yes/No)	Product Documentation Reference
1	Make			
2	Model			
3	Construction	Cast Iron/Steel foundation, Sturdy Body for equipment		
4	Call Button	Watertight Push Button,		
5	Connectivity	GSM/PSTN/Ethernet as per solution offered		
6	Housing Cold Rolled Steel (CRC)	Housing Cold Rolled Steel (CRC)		
7	Operating Temperature	-40 C to55 C		
8	Relative Humidity	10% to 95%		
9	Storage Temperature	40 **° C** to 70 **°** C		
10	Installation	Pole Mounted		
11	Mic and Speaker	10 W and 2 W		
12	Sensors	For tempering/Vandalism		
13	Battery	Internal Battery with different charging options (Solar/Mains)		
14	Power	Automatic on/off operation		
15	Casing	IP-55 rated for housing		

3. The unit shall preferably have a button which when pressed, shall connect to the DICCC/Police Command Center/other locations over the existing network setup.

Variable Message display

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

The MSI shall install IP based VMD boards across city bus stops of Dehradun. These VMD boards shall have different characteristics depending upon the location and purpose of

16	Operating conditions	As per City weather conditions	

installation. VMD board displays are to be controlled through DICCC. The purpose of the VMD

Boards is for advertisement at the bus stops.

2. The MSI, in consultation with AMC can propose alternate locations apart from the locations mentioned in this RFP for installing the VMD boards where their effectiveness in communicating information.

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

Functional Requirements of the Variable Message Display (VMD) System

Sl no	Minimum Specifications	Bidder Compliance (Yes/No)	Product Documentation Reference
1	**Make**		
2	**Model**		
3	**System Requirements**		
a.	The system should be capable to display warnings, traffic advice, route guidance and emergency messages to motorists from the DICCC in real time.		
b.	The system should also be capable to display warnings, traffic advice, route guidance and emergency messages to motorist by using local PC/Laptops.		

c.	The VMD should display text and graphic messages using Light Emitting Diode (LED) arrays.		
d.	The System should able to display failure status of any LED at DICCC.		
e.	The System should support Display characters in true type fonts and adjustable based on the Operating system requirement.		
f.	The VMD workstation at the DICCC should communicate with the VMD controller through the network. It should send out command data to the variable message display controller and to confirm normal operation of the signboard. In return, the VMD workstation should receive status data from the VMD controller.		
g.	VMD controllers should continuously monitor the operation of the VMD via the provided communication network.		
h.	Operating status of the variable message display should be checked periodically from the DICCC		
i.	It shall be capable of setting an individual VMD or group of VMD's to display either one of the pre-set messages or symbols entered into the computer via the control computer keyboard or by another means.		
j.	It shall be capable of being programmed to display an individual message to a VMD or a group of VMD's at a pre-set date and time.		
k.	A sequence of a minimum of 10 messages/pictures/ pre-decided sign or group of signs shall be possible to assign for individual VMD or group of VMD's.		
l.	It shall also store information about the time log of message displayed on each VMD. The information stored shall contain the identification number of the VMD, content of the message, date and		

	time at which displayed message/picture starts and ends.		
m.	The central control computer shall perform regular tests (pre-set basis) for each individual VMD. Data communication shall be provided with sufficient security check to avoid unauthorized access.		
4	**Variable Message Displays (VMD) application**		
a.	Central Control Software allows controlling multiple VMD from one console.		
b.	Capable of programming to display all types of Message/ advertisement having alphanumeric character in English, Hindi, Bengali (any other language asked by ASCL) and combination of text with pictograms signs. The system should have feature to manage video / still content for VMD. The system should have capability to divide VMD screen into multi-parts to display diverse form of information like video, text, still images, advertisements, weather info, city info etc. The system should also provide airtime management and billing system for paid content management		
c.	Capable of controlling and displaying messages on VMD boards as individual/ group.		
d.	Capable of controlling and displaying multiple font types with flexible size and picture sizes suitable as per the size of the VMD.		
e.	Capable of controlling brightness & contrast through software.		
f.	Capable to continuously monitor the operation of the Variable Message Display board, implemented control commands and communicate information to the DICCC via communication network.		

g.	Real-time log facility – log file documenting the actual sequence of display to be available at central control system.		
h.	Multilevel event log with time & date stamp.		
i.	Access to system only after the authentication and acceptance of authentication based on hardware dongle with its log.		
j.	Location of each VMD will be plotted on GIS Map with their functioning status which can be automatically updated.		
k.	Report generation facility for individual/group/all VMDs with date and time which includes summary of messages, dynamic changes, fault/repair report and system accessed logs, link breakage logs, down time reports or any other customized report.		
l.	Configurable scheduler on date/day of week basis for transmitting pre-programmed message to any VMD unit.		
m.	Various users should access the system using single sign on and should be role based. Different roles which could be defined (to be finalized at the stage of SRS) could be Administrator, Supervisor, Officer, Operator, etc.		
n.	Apart from role based access, the system should also be able to define access based on location.		
o.	Rights to different modules / Sub-Modules / Functionalities should be role based and proper log report should be maintained by the system for such access		
p.	Components of the architecture should provide redundancy and ensure that there are no single points of failure in the key project components. To take care of remote failure, the systems need to be configured to mask and recover with minimum outage.		

q.	The architecture should adopt an end-to-end security model that protects data and the infrastructure from malicious attacks, theft, natural disasters etc. provisions for security of field equipment as well as protection of the software system from hackers and other threats shall be a part of the proposed system. Using Firewalls and Intrusion detection systems such attacks and theft shall be controlled and well supported (and implemented) with the security policy. The virus and worms attacks shall be well defended with Gateway level Anti-virus system, along with workstation level Anti-virus mechanism. There shall also be an endeavour to make use of the SSL/VPN technologies to have secured communication between Applications and its end users. Furthermore, all the system logs shall be properly stored & archived for future analysis and forensics whenever desired.		
r.	Ease of configuration, ongoing health monitoring, and failure detection are vital to the goals of scalability, availability, and security and should be able to match the growth of the environment.		
s.	System shall use open standards and protocols to the extent possible		
t.	Facility to export reports to excel and PDF formats.		
5.	**Remote Monitoring**		
a.	All VMD shall be connected/configured to DICCC for remote monitoring through network for two way communication between VMD and control Room to check system failure, power failure & link breakage.		
b.	Remote Diagnostics to allow identifying failure up to the level of failed individual LED.		
6	In the event of central server failure, each of the SMART VMS boards should be individually capable of continuous & uninterrupted display of real time traffic &		

	other information as per last configuration thereby ensuring continuous operation.		

Technical Specifications: Variable Message Display (VMD) System

Sl no	Parameter	Minimum Specifications	Bidder Compliance (Yes/No)	Product Documentation Reference
1.	**Make**			
2.	**Model**			
3.	**Dimensions**	Minimum 3.0m length X 1.5m height X 0.2m depth. (3000mm x 1500mm X 200mm approx)		
4.	**Colour LED**	Full Colour, class designation C2 as per IRC/EN 12966 standard		
5.	**Luminance Class/Ratio**	L3 as per IRC/EN 12966 standards.		
6.	**Luminance Control & auto Diming**			
a.	Should be automatically provide different luminance levels but shall also be controllable from the traffic centre using software.			
b.	Should have auto dimming capability to adjust to ambient light level (sensor based automatic control)			

c.	Photoelectric sensor shall be positioned at the Display front and Display rear to measure ambient light. Capable of being continually exposed to direct sunlight without impairment of performance.			
7.	**Contrast Ratio**	R3 as per IRC/EN 12966 standard		
8.	**Beam Width**	B6+ as per IRC/EN12966 standards.		
9.	**Pixel Pitch**	12mm or better		
10.	**Picture Display**			
d.	At least 300mm as per IRC /EN 12966 standards			
e.	Full Matrix: Number of lines & characters adjustable, active area: 2.88mX1.2m atleast			
f.	Synchronized Dot to Dot display.			
g.	Capable of displaying real time message generated by DICCC.			
h.	Special frontal design to avoid reflection.			
i.	Display shall be UV resistant			
11.	**Viewing Angle**	B6+ as per IRC/EN12966 standard- Viewing angle shall ensure message readability for motorists in all lanes of the approach road		

12.	**Viewing Distance**	Suitable for readability from 150 Mtrs. or more at the character size of 240mm, from moving vehicles.		
13.	**Self-Test**			
a.	VMD shall have self-test diagnostic feature to test for correct operation.			
b.	Display driver boards shall test the status of all display cells in the Display board even when diodes are not illuminated.			
c.	All periodic self-test results shall be relayed to the DICCC in real time to update the status of the VMD			
14.	**Alarms**			
a.	Door Open sensor to Inform Control room during unauthorized access			
b.	LED Pixel failure detection alarm			
15.	**Flicker**	Refresh Frequency should not be less 90 Hz. No visible flicker to naked eye.		
16.	**Multiple Data Communication interface/Port**	RJ45 Ethernet, RS232, RS 485, FC port or any other suitable		
17.	**Communication (connectivity)**	Wired & GPRS based wireless technology with 3G upgradable to 4G capability.		
18.	**Ambient Operating Temperature**	The system should be capable of working in ambient temperature as per Dehradun weather conditions.		
19.	**Humidity (RH)**	Operating ambient humidity should be as per Dehradun weather conditions		

20.	**Protection against Pollution/dust/ water**	Complete VMD should be of IP 65 protection level from front and IP54 from side and rear. As per EN60529 or equivalent Standard.		
21.	**Power**			
a.	Preferably 170-250V AC (more than 90% power factor) or DC as per equipment requirement.			
b.	Protection for overvoltage/ fluctuation/drop of the nominal voltage (50%) shall be incorporated.			
c.	The enclosure shall contain at least two 15 Amp VAC (industrial grade) outlet socket for maintenance purpose.			
22.	**Power Back-up & its enclosure**	Should have UPS provisioning as per SLA requirements. The enclosure of UPS and battery should be pole mountable with IP 65 protected housing and lockable.		
23.	**Material for VMD frame**	Preferably at least 2mm aluminum or Non-corrosive, water resistant or better. Frame of the VMD should be black & Powder coated.		
24.	**Mounting, Installation and finishes**			
a.	Mounting structure shall use minimum 6Mtrs. High Cylindrical GI Pole (Class B) or suitable structure with 5.5 mtr. Minimum vertical clearance under the VMD from the Road surface.			

b.	The mounting shall be capable of withstanding road side vibrations at site of installation.			
c.	It shall be provided with suitable walkway for maintenance access.			
d.	The sides interior and rear of enclosures shall be provided in maintenance free natural aluminium finish. All enclosure shall be flat and wipe clean.			
e.	Rugged locking mechanism should be provided for the onsite enclosures and cabinets.			
f.	For Structural safety, the successful bidder has to provide structural safety certificate from qualified structural engineers approved/ certified by Govt. Agency.			
25.	**Wind Load**	As per the city requirement		
26.	**Cabling, connections and Labelling.**			
a.	All cable conductors shall be of ISI marked for quality and safety. It shall be of copper insulated, securely fastened, grouped, wherever possible, using tie warps approximately every 10-20 Cms or cable trays.			
b.	All connections shall be vibration-proof quick release connections except for power cables terminating in terminal blocks, which shall be screwed down.			
c.	All terminal block shall be made from self-extinguishing materials. Terminations shall be logically grouped by function and terminals carrying power shall be segregated from control signal terminals.			
d.	All cables shall be clearly labelled with indelible indication that can clearly be identified by maintenance personnel using “As built : drawings”.			
e.	Lightening arrester shall be installed for safety on each VMD.			

f.	The successful bidder has to provide safety certificate from qualified Electrical engineers approved/certified by Govt. Agency.			
27.	**Local Storage in VMD**	Embedded VMD controller should be capable to store atleast 100 messages and symbols/pictograms to allow display to run in isolated mode on a predefined structures/timings, in case of connectivity failure.		

4.12 City Surveillance

A safe and secure city is a nicer and attractive place where people – residents and visitors – feel safe to live, work, travel and thrive. Today, the metropolitan environment is dynamic and complex, and the cities face threats from rising crime rates, civil unrest, terrorist attacks to natural calamities.

With more than half the global population today living in urban areas, to mitigate the impacts of these urban threats the governments around the world are investing in new and emerging technologies for safe and secure cities. With multi-layered structure of city security and numerous players involved, both public and private, the safe and secure cities concept is broad and still largely unformulated. However, the emergence of smart technologies is shaping its vision.

Surveillance system will be of prime importance for safety and security of citizen especially women as well as for helping elders/children during any emergency

DSCL intend and expect from MSI to install High resolution surveillance cameras with smart video analytical solution to provide world class infrastructure for safe and secure city for the citizens of Dehradun. Minimum specification for the cameras to be considered are given below.

TECHNICAL SPECIFICATIONS FOR CCTV SURVEILLANCE

4.12.1 Dome Camera

S. No	Features	Specifications	Compliance/Page No

1	Form Factor	Dome	
2	Image Sensor	1/1.8” CMOS or better	
3	Day/ Night Operation	Yes, with IR Cut Filter	
4	Minimum Illumination	Color : 0.2 Lux @ F1.8 B/W : 0 Lux (IR LED On)	
5	Lens	3.6 - 10 mm motorized zoom lens, P-Iris, Megapixel Lens with remote zoom and focus	
6	Electronic Shutter	1/30 ~ 1/10,000 s	
7	Image Resolution	5MP or better	
8	Compression	H.265, H.264 , M-JPEG	
9	Compression profile	Should support H.264, H.265, M-JPEG baseline, Main profile, and high profile	
10	Frame Rate and Resolution	RJ-45, 10/100/1000 Mbps Ethernet	
11	Simultaneous Stream	Minimum 2 streams should be configurable at 1920 X 1080 @ 25 fps simultaneously and support at least 2592x1944 @25 FPS	
12	White Balance	Auto / Manual / ATW / One Push	
13	GOV Length	It should be possible to vary the GOV length in the camera setting.	
14	Noise Reduction	Digital Noise Reduction 2D / 3D DNR	
15	Zoom	3x optical Zoom, 10x Digital Zoom	
16	Digital PTZ	Camera should support digital PTZ	
17	Video Streams	Quad Stream supportable, each stream should be H.265, H.264 configurable at different resolutions and support atleast 2592x1944 @25 FPS	
18	Video quality view	Video compression type (H.265, H.264 , M-JPEG) and bit rate of each stream should be viewable at home screen in web browser	

19	Image Setting	Saturation, Brightness, Contrast, Sharpness, Hue adjustable	
20	Two-way audio	Line in / Line Out	
21	Audio Compression	G.711 / G.726 / AAC / LPCM	
22	Iris	P iris	
23	Wide Dynamic Range	120 dB or better	
24	IR	at least 30 mtr IR distance or better	
25	Alarm	1 x Input / 1 x output	
26	Edge Video Content Analytics	Camera should have in-built Edge Bases Analytics Video Motion Detection, Active Tampering Alarm, Trip Zone.	
27	Storage backup on network failure	Camera should support network failure detection, Camera should have the capability to start the recording automatically on SD card in case of connectivity between camera and NVR/Storage device goes down	
28	Edge Storage	Built in SD card slot with support at least 128 GB SD card	
29	Network Interface	RJ-45, 10/100/1000 Mbps Ethernet	
30	Protocols	IPv4/v6, TCP/IP, UDP, RTP, RTSP, HTTP, HTTPS, ICMP, FTP, SMTP, DHCP, PPPoE, UPnP, IGMP, SNMP, QoS, ONVIF	
31	Text Overlay	Date & time, and a customer-specific text etc	
32	privacy masks	Support atleast 8 privacy masks	
33	Security	HTTPS / IP Filter / IEEE 802.1X	
34	Firmware Upgrade	The firmware upgrade shall be done though web interface,	
35	Audio Transmission mode	Full Duplex, Half Duplex, Simplex	
36	Enclosure	IP 66 weather proof,	

37	Vandal Resistant	IK 10	
38	Power	POE / 12 V DC /24 V AC	
39	Operating Temperature	-10 °C to 60 °C	
40	Operating Humidity	Humidity 10%–90% No Condensation	
41	Certification	UL/CE/FCC/BIS	
42	ONVIF	ONVIF Profile	
43	User accounts	20	
44	Supported Web Browser	Internet Explorer (10+) / Firefox / Safari/ Mozilla	

4.12.2 Bullet Camera

S. No	Feature	Specifications	Compliance/Page No
1	Form Factor	Bullet	
2	Image Sensor	1/1.8” CMOS or better	
3	Day/ Night Operation	Yes, with IR Cut Filter	
4	Minimum Illumination	Color : 0.2 Lux @ F1.8 B/W : 0 Lux (IR LED On)	
5	Lens	3.6 - 10mm motorized zoom , P-Iris, Megapixel Lens with remote zoom and focus	
6	Electronic Shutter	1/30 ~ 1/10000 S	
7	Image Resolution	5 MP or better	
8	Compression	H.265, H.264 (MP), M-JPEG	
9	Compression profile	Should support H.264 and H.265 baseline, Main profile, and high profile	
10	Frame Rate and Resolution	5M (2592 x 1944) @25 fps, 3M (2048 X 1536) @25/30 fps, 2 MP (1920 X 1080) @ 50/60 FPS	
11	Simultaneous Stream	Minimum 2 streams should be configurable at 1920 X 1080 @ 25 fps simultaneously and support atleast 2592x1944 @25 FPS	
12	White Balance	Auto / Manual / ATW / One Push	
13	GOV Length	It should be possible to vary the GOV length in the camera setting.	
14	Field of View	Wide : 90º (H), 67º (V), 116º (D) Tele : 37º (H), 27º (V), 46º (D)	
15	Noise Reduction	Digital Noise Reduction 2D / 3D DNR, defogging feature Should be supported.	
16	Zoom	3x optical Zoom, 10x Digital Zoom	
17	Digital PTZ	Camera should support digital PTZ using software platform	

18	Video Streams	Quad Stream supportable, each stream should be H.265 &H.264 configurable at different resolutions.	
19	Video quality view	Video compression type (H.265, H.264/MJPEG) and bit rate of each stream should be viewable at home screen on web browser	
20	Image Setting	Saturation, Brightness, Contrast, Sharpness, Hue adjustable	
21	Two-way audio	Line in / Line Out	
22	Audio Compression	G.711 / G.726 / AAC / LPCM	
23	Iris	P iris	
24	Wide Dynamic Range	120 dB or better	
25	IR	Atleast 30MTR Distance or better	
26	Alarm	1 x Input / 1 x output	
27	Edge Video Content Analytics	Camera should have in-built Edge Bases Analytics, Video Motion Detection, Active Tampering Alarm, Trip Zone	
28	Storage backup on network failure	Camera should support network failure detection, Camera should have the capability to start the recording automatically on SD card in case of connectivity between camera and NVR/Storage device goes down	
29	Edge Storage	Built in SD card slot with support at least 128 GB SD card	
30	Network Interface	RJ-45, 10/100/1000 Mbps Ethernet	
31	Protocols	IPv4/v6, TCP/IP, UDP, RTP, RTSP, HTTP, HTTPS, ICMP, FTP, SMTP, DHCP, PPPoE, UPnP, IGMP, SNMP, QoS, ONVIF	
32	Text Overlay	Date & time, and a customer-specific text etc	
33	Security	HTTPS / IP Filter / IEEE 802.1X	

34	Firmware Upgrade	The firmware upgrade shall be done though web interface, the firmware shall be available free of cost	
35	Image Rotation	Normal, Mirror, 90 deg clockwise , 90 deg anti clockwise , 180 deg rotate	
36	Privacy Masks	At least 8 privacy masks	
37	Audio Transmission mode	Full Duplex, Half Duplex, Simplex	
38	Enclosure	IP66, IK10 with inbuilt heater	
39	Power	POE / 12 V DC /24 V AC	
40	Operating Temperature	-10 °C to 60 °C	
41	Operating Humidity	Humidity 10%–90% No Condensation	
42	Certification	UL/CE/FCC/BIS	
43	ONVIF	ONVIF Profile	
44	User accounts	20	
45	Supported Web Browser	Internet Explorer (10+) / Firefox / Safari/ Mozilla	

4.12.3 PTZ Camera

S. No	Features	Specifications	Compliance/Page No
1	Certifications	UL/CE/FCC/BIS	
2	Compatibility	ONVIF profile S	
3	Sensor	1/1.7" CMOS	
4	Resolution	5MP or better	
5	Multiple Stream	Quad Stream	
6	Frame Rate	5MP@30fps, 3MP@25 fps,	
7	Focal Length	(f=6.5 - 202mm), 31x Optical zoom	

8	Field Of view	Wide : 58.2º (H), 34.4º (V), 65.2º (D) Tele : 1.99º (H), 1.13º (V), 2.3º (D)	
9	Optical Zoom	31X	
10	Digital Zoom	12X or better	
11	Focus	Auto / Manual	
12	WDR	120 dB	
13	Noise Reduction	2D / 3D should support defogging feature	
14	Shutter Speed	1/30 ~ 1/10000 sec.	
15	IR	Inbuilt IR, IR distance atleast 200mtr or better	
16	Illumination Adjustment	IR illumination adjustment by zoom ratio with inbuilt IR LEDs	
17	Day & Night	IR Cut filter	
18	Min Illumination	Color : 0.1 Lux @ F1.55 B/W : 0 Lux (IR LED ON)	
19	Iris	P iris	
20	Edge Video Content Analytics	Camera should have in-built analytics Video Motion Detection, Active Tampering Alarm, Auto Tracking, Should also support Face Detection	
21	Storage backup on network failure	Camera should support network failure detection, Camera should have the capability to start the recording automatically on SD card in case of connectivity between camera and NVR/Storage device goes down	
22	Edge Storage	Built in SD card slot with support at least 128 GB SD card	
23	Video Compression	H.265, H.264 , M-JPEG	
24	Privacy Mask	At leat 8 privacy zones	
25	PTZ	Pelco D, Pelco P, DSCP Protocol Support	
26	Audio	2 Way audio	
27	Audio Compression	G.711 / G.726 / AAC	

28	PAN	360 ° endless , Manual speed 0.1° ~ 300°/s , preset speed 9° ~ 350°/s	
29	Tilt	,200° , Manual speed 0.1° ~ 200°/s , Preset speed 7° ~ 300°/s , Auto flip	
30	Presets	256	
31	PTZ Operation	8 sequence, 8 cruise	
32	Speed by zoom	On / Off (Pan and tilt speed proportional to zoom ratio)	
33	Home Function	Preset / Sequence / Auto pan / Cruise	
34	Calibration	Auto(On/Off)	
35	Resume after power loss	Supported zero downtime power switching	
36	Protocols	IPv4/v6, TCP/IP, UDP, RTP, RTSP, HTTP, HTTPS, ICMP, FTP, SMTP, DHCP, PPPoE, UPnP, IGMP, SNMP, QoS, ONVIF, ARP	
37	Security	HTTPS / IP Filter / IEEE 802.1x	
38	Alarm	Input 8 / Output 2	
39	Alarm response	Preset / Sequence / Auto Pan / Cruise	
40	Ethernet Interface	1 X RJ 45	
41	Supported Web browser	Internet Explore (10.0+) / Firefox / Safari/Mozilla	
42	Weather Proof	IP66,IK10 & inbuilt heater housing	
43	Operating Temperature	, -10°C ~ 50°C	
44	Power Supply	802.3at (PoE+) 4-Pair 60W / AC 24VAC /PoE, ± 20% / DC 12V	
45	Power Consumption	70W or less (with IR & Heater on)	

46	Image Stabilization	Camera should support Image Stabilization	
47	Defogging	Should Support defogging feature	

4.12.4 Box Camera

S. No	Features	Specifications	Compliance/ Page No
1	Form Factor	Box Type	
2	Certification	UL/CE/FCC/BIS	
3	ONVIF	ONVIF profile	
4	Image Sensor	1/2.8” Progressive CMOS	
5	Day/ Night Operation	ICR	
6	Minimum Illumination	Color : 0.1 Lux @F1.2 BW : 0.01 Lux @ F1.2	
7	Lens	External Lens (5 mm to 50 mm)	
8	Electronic Shutter	1/30 ~ 1/10000 S or better	
9	Image Resolution	3M (2048x1536) or better	
10	Compression	H.265, H.264 , M-JPEG	
11	Frame Rate and Resolution	H.264 3M (2048 X 1536) @25/30 fps, 2 MP (1920 X 1080) @ 50/60 FPS	
12	Simultaneous Stream	Minimum 2 streams should be configurable at 1920 X 1080 @ 25 fps simultaneously	
13	White Balance	Auto / Manual / ATW / One Push	
14	Noise Reduction	3DNR / 2DNR / Colon	
15	Zoom	Digital Zoom	
16	Video Streams	Quad Stream supportable, all stream should be H.265	
17	Image Setting	Saturation, Brightness, Contrast, Sharpness, Hue adjustable	

18	Two-way audio	Line in / Line out	
19	Audio Compression	G.711 / G.726 / AAC / LPCM	
20	Iris	P - iris	
21	Wide Dynamic Range	120 dB	
22	Alarm	1 x Input / 1 x output	
23	Edge Video Content Analytics	Camera should have in-built Edge Bases Analytics, Video Motion Detection, Active Tampering Alarm, Trip Zone	
24	Network Interface	1 x RJ45	
25	Storage backup on network failure	Camera should support network failure detection, Camera should have the capability to start the recording automatically on SD card in case of connectivity between camera and NVR/Storage device goes down	
26	Protocols	ARP, IPv4/v6, TCP/IP, UDP, RTP, RTSP, HTTP, HTTPS, ICMP, FTP, SMTP, DHCP, PPPoE, UPnP, IGMP, SNMP, QoS, ONVIF	
27	Text Overlay	Date & time, and a customer-specific text etc	
28	Security	HTTPS / IP Filter / IEEE 802.1X	
29	Firmware Upgrade	The firmware upgrade shall be done though web interface, the firmware shall be available free of cost	
30	Power	PoE / DC 12V / AC 24V	
31	Operating Temperature	-10°C ~ 50°C	
32	Operating Humidity	,10% ~ 90%, No Condensation	
33	User accounts	20	
34	Supported Web Browser	Internet Explorer (10+) / Firefox / Safari/ Mozilla	

35	Digital Image Stabilization	Camera should support Digital Image Stabilization	

4.13 VMS and VA

4.13.1 Video Management System and Video Analytics

Sr.No	Required Parameter
1	The Software shall be Scalable , Client Server based , Enterprise level capable to handle at least 1000 camera in the same system by adding camera license and server. The VMS software should be third party ONVIF Profile S Conformant and independent of camera make and shall support at least 40 different makes of camera on Native Driver to showcase tight integration. (List of Supported Camera Make to be submitted)
2	The VMS shall be able to support cameras at at least 30 frames per second and any resolution supported by the camera and the camera driver. The VMS shall automatically offer only supported fps and resolution combinations for user convenience.
3	The system shall allow the recording, live monitoring, playback of recorded video,audio,and data simultaneously
4	The VMS Management software should allow load balancing feature for effective utilisation of resources for Server and client. It can allow system to be load balancing as per remote or local usage.
5	The Software shall be able to control Bit Rate /Quality of camera , FPS , Resolution as per requirement. The same can be applied from VMS System manager itself not from the camera web browser.
6	The VMS shall allow bidirectional audio communication with the cameras Two way Audio Communication can be in 3 different Modes , Recording shall be available with Audio & video Synced together :
A	Closed Mode : In the closed mode, the audio channels are not open
B	Listen Mode : In the listen mode, the user will hear audio from the camera and any potential audio going to the camera from any other VMS client. The audio channel from current user is not open.
C	Talk Mode : In the Talk mode, the user will speak from the Client Station to the camera.
7	The VMS shall be able to integrate with other systems using video, data or digital I/O , Scheduled I/O as well as logical I/O
A	The VMS shall support inbuilt Server based Video Analytics. The license and software link should come as single package to make it easy for the user. Software should able to handle Video Recording and Video Analytics a minimum of 100 cameras in one recorder. Recording to be done at 1080p,20 fps.
8	VMS should support 3 motion detection methods - Comparative , Adaptive and Hermeneutic for adverse conditions
9	The VMS shall be Windows based supporting native or virtualized Windows Server 2016 and Windows 10. The VMS shall allow operation with PC Keyboard, Mouse and DirectX compliant CCTV Keyboard(Joystick).

10	The VMS OEM shall be Microsoft Gold Certified Partner for enhanced experience.
11	The VMS shall support unlimited storage and should be able to record in NAS , SAN and DAS
12	The VMS shall support H.264, H.265 , MPEG-4 and MJPEG compression methods
13	The VMS shall support multi-live streaming, multi casting and thrucast streaming methodology
14	The VMS shall support exporting video in a tamper proof format. The media player provided in the software shall automatically notify if the video or audio has been modified
15	The VMS shall provide file export tool for export of single frame of video in BMP, GIF, TIF, JPG and PNG formats and export of video files in SEF, ASF, AVI and MKV format
16	Archiving Support
17	The Client software should have a "Help" Tab which should have all the details of operation and to include all topics related to the software for the operator.
18	Quick review of the recorded video
19	Support any video resolution like CIF, 2CIF, 4CIF & HD atleast 20MP.
20	Quick search of devices in the viewing application
21	Extended camera viewing on multiple monitors
22	Multi camera sequential tours
23	Digital zooming feature for live video and playback
24	Facility for exporting the video on a portable media such as pendrive/DVD/portable hard disk etc
25	The software should comply that all client to server and server to server communications are compressed and encrypted and connection specific key should be 256 bit AES and data encryption should be 256 bit AES. The exported video should be saved in SEF (Secure Export Format) for secure non tamper file system with Password key which can be set to 20 Characters. The Client application should support dual password mode for each user.
26	Video search on the basis of date, time, event, camera, location & alarm
27	Post recording motion search analysis
28	The VMS shall have the following licensing policies:
28.1	The VMS shall not have base licenses and standard channel modules. The VMS shall be flexible to provide and support licenses for any number of cameras.
28.2	The VMS licensing shall allow changing any and all of the cameras at any time without extra cost or license key change
28.3	The VMS shall not require online licensing process
28.4	The VMS shall support instant device/ Camera replacement using original IP address. The IP of the new device/ camera shall not be feeded in the software while replacing faulty camera / device
28.5	The VMS licensing shall require MAC Id of Server/ Recorder only, not of camera devices.
28.6	Recording redundancy :
28.7	The VMS shall support software inbuilt Secure Data distribution methodology for fault tolerance
28.8	The VMS Shall Support N:1 Failover for all recording server, where n=10
29	The VMS Management software should allow Dual Password Feature for Administrator.
30	Reporting

	i.Reporting tool shall be web based and required for analysis of Various types of alerts occurred vis a vis various time frame vis a vis camera
	ii.It shall be possible to create various formats of reports in graphical format
	iii.The reporting format can be saved as book mark as well as Audit trail should be possible
	iv. It shall be possible to find out where there is more events / activities .
	v. It can provide reports of all the recorder Integrated separately
	System watchdog feature be available to alert in case of failure of cameras and servers.
Client & Recorder Application	
1	Software should be of enterprise level and able to handle minimum 100 cameras with analytics in one recorder. One master recorder shall manage a system of atleast min of 150 Servers with the possibility to expand the system to include multiple master recorders. Recorder Software should have a spare of minimum 10 %
2	The system management server shall run as a Windows service on one of the recorders. The system management server shall control the following: a) Overall system operation. b) Data communication between recorders and client programs. c) Maintain user and profile lists. d) Authenticate and authorize users and applications. e) Maintain system logs. f) Handle system diagnostics.
3	Software shall allow the recording, live monitoring, playback of archived video,audio and data, network transmission and changes to settings simultaneously.
4	Server software shall enable the client to dynamically create connections between Cameras and workstations and view live or recorded video on the digital monitors(audio, video, serial ports and digitalis/Os)
5	Server software shall provide the client seamless operation of all cameras and workstations available in the system regardless of the actual connection to different archive servers
6	Offered software shall use standard servers for all the processing and shall not need any proprietary server hardware
7	The alarms may be triggered by the following events: a. Motion (or lack of motion) in camera view b. Change in sound level c. Text data string d. Digital input signal from an external device e. Missing camera signal (resulting for example from sabotage) f. Custom event from 3rd party application. g. Video Content Analytics (VCA) event from inbuilt.

8	The alarm management shall support the following automatic responses: a. Pre- and post-recording at least 60 minutes of video and audio b. Opening an alarm camera window or audio window (real-time or playback) on the workstation screen c. Displaying the alarm on the alarm list d. Activating a digital output e. Turning a dome camera to a preset position f. Starting a dome camera tour g. Sending an alarm e-mail message h. The alarm management shall be able to acknowledge alarm automatically or manually
9	The alarm management shall support the following alarm viewing features: a. It should provide the facility to assign the priority level to different alarms. b. It should allow pass the specifically arms to specified users rather than sending all alarms to every user. c. Users in same user group should see and be able to manage received alarms assigned for the same user group. All users should see the alarm status in real time. d. System should have single alarm stack even though there are multiple recording servers
10	Software should allow creation of multiple camera sequences. It should be possible to set the dwell time for the cameras within the sequence.
11	Software should allow taking the backup of the recorder server configuration and restoring the same if required.
12	Software should allow easy and user friendly menus for camera configurations. It shall allow changing settings for multiple cameras of the same type simultaneously
13	Software should provide totally configurable user privileges with independent user rights. The user privileges are saved in profiles which can be assigned for the required users
14	Software should provide the utility to interface the recorder servers with internet. Internet Gateway server shall allow clients to view live and playback video streams, control PTZ cameras and control digital I/O devices over the internet
15	Software shall allow the client applications to interact with multiple recorder servers simultaneously and allow the simultaneous display cameras from different recorders on the same monitor
16	The VMS shall support integration with different applications like different types of Sensors , Baggage Scanner, Perimeter Intruder Systems , RFID , Physical ACS etc
17	The client programs shall include end user client program, system management client program, browser-based client program and mobile client programs, atleast 10 concurrent client license to be provided which can later be expandable at least 20 User license without any charge.
18	The end user client program shall support multiple profiles for each user
19	Client applications shall provide an authentication mechanism, which verifies the validity of the user through the selected system management server

20	Client shall perform the following applications simultaneously without interfering with any of the Archive Server operations (Recording, Alarms, etc.) a. Live display of cameras and audio b. Live display of camera sequences c. Playback of video and audio d. Media search tools e. PTZ control f. Display and control of Maps g. Alarm management h. Digital I/O control
21	Client applications shall support any form of IP network connectivity including: AN, WAN, VPN, Internet and Wireless
22	Client applications shall support IP Multicast (RTP) and Unicast (TCP or RTP) video and audio streaming as required depending on the network capabilities
23	Client application should support both dynamic and predefined Video display layouts, for example Full screen, 2x1, 2x2, 3x2, 3x3, 3x3+1 large , 4x2, 4x2+1 large , 4x3, 4x3+1 large , 4x3+2 large , 4x4 , 4x4+1 large , 5x5 , 6x5 + 1 large, 7x5 , 10x10 , 12x12 , 16x16 .etc.
24	Client application shall enable playback of audio along with video. The monitor shall enable the user to work with multiple Audio layouts containing collections of audio clips
25	Users shall be able to define and store their own layouts, which they will be able to recall later through a layout list. Each layout shall contain information about the dimensions and positions of all windows along with image filter data and data about the active profile
26	Client application shall enable playback of audio mixed from both live and recorded audio sources, allowing the user to control the volume of each source independently as well as mute them
27	Client application shall be able to control the playback with play, pause, forward and speed buttons
28	Client application shall allow operators to save bookmarks with description of the recorded and live video, audio and text data
29	Client application shall provide drag and drop facility for selection of the devices to be viewed in the viewing layout
30	Client application shall support Graphical Site Representation (Maps) functionality, where digital maps are used to represent the physical location of cameras and other devices throughout facility. Maps should have the capability to add the hyperlinks to create interlinked maps. It should allow the selection of any camera for display from the map
31	Client application shall support digital zoom on a fixed/PTZ camera's live and recorded video streams
32	Client application shall provide management and control over the system using a standard PC mouse, keyboard or CCTV keyboard. The client application shall support area zoom and click to center functions for PTZ cameras if supported by the specific camera driver. Area zoom zooms into the rectangle drawn by mouse and click to center means clicking anywhere on the PTZ camera view centers the camera to that position
33	Client application shall be able to control pan-tilt-zoom, iris, focus, presets and dome patterns of the PTZ camera

34	Software should provide the ability to play a minimum of 32 video channels in time sync with each other. Software shall support exporting a multichannel clip with video, audio and text channel data
35	Any user can share layouts and should be visible to all users od same profile
36	Ability to Autocrop each camera view.
37	Should support Virtual Matrix option to build video walls and video matrixes, the matrix can be created by having a separate display server for each four monitors in the matrix, as well as an operator console server to manage the display servers.
38	Ability to Define a Virtual camera that focuses in the part of camera view be it live or playback. using Virtual Cameras one can view chosen parts of the full recorded Camera View in a Separate Window. View Specific Area of interest in a virtual camera and choose per virtual camera for zooming, View , Aspect Ratio and resolution. Virtual cameras may overlap each other. Atleast 30 such Virtual camera can be made from one single camera view.
39	Shall have visualized Video intelligence for the Virtual camera to Auto Zoom and track an object.
40	The device Station should have various symbol options to user to understand if the Camera is in below Conditions : Normal, Recording , No Signal , Not in use , Connecting and No Connection.
41	The Graphic User Interface shall be very easy for the user to monitor and deter. The User interface in one window shall have at least the following : Menu, Profile Control, Device Tree , Data & Time settings , Activity Setting , Play back control , time slider, Camera Tour and control , Alarm List , Different Plugin options , Different tab controls for cameras.
42	The camera toolbar shall be displayed when the mouse is moved over a camera or if a camera is selected with other means. If the mouse is not moved for some time, the camera toolbar disappears automatically. The camera toolbar shall contain atleast the following items. • Camera settings control • Export control • Image print control • Camera closing and duplication control • Two way audio control • View or virtual zoom control • highlight control • Image Control plugin control • 360 camera de-warping control (In case of 360 Cameras) • Other toolbar plugins
43	Alarm Indications: The Alarm shall be easily indicated In the device tree, and in Profile Maps, the camera which is associated to an alarm shall be highlighted in yellow / Red Color.

44	Alarm Filtering Option shall be there. It shall possible to “silence” alarms for a desired time period Ranging from 5 Minutes till 24 Hours or more. This is useful if alarms are unintentionally active all the time, e.g., due to adverse environmental conditions such as heavy wind, rain or snowfall
45	Each camera view should have Image Control Plugin and each camera view can be configured individually as per the condition. The Image Control plugin has various options to adjust the camera image.
a	Option to turn the image to black and white image
b	Edge highlight filter
c	Histogram filter (a form of contrast optimization filter)
d	Noise reduction filter
e	Image sharpening filter
f	De-interlace filter
g	Image flip (flips image along horizontal Axis)
h	Image mirror (mirrors image along vertical axis)
i	Brightness adjustment slider
j	Contrast adjustment slider
46	The Software shall have an easy to use 3D calibration tool where 3D calibration objects are matched to the actual camera viewing scene. The calibration parameters include camera height, camera viewing angle and camera tilt angle. (Picture of 3 D Calibration tool of the Software to be attached with the tender document as proof of the same)
47	*Evidence Export Solution* - The Software shall be able to create, export and share Incident by making clips from multiple cameras with labels, descriptions and comments. The Clips shall be played simultaneously or sequentially in desired order to give wholistic veiw about the incident and the evidence. the systems should combine the video clips from multiple cameras collected together, and then edit them into a movie that contains authenticity checked material and detailed descriptions of what is being shown on the videos. The Evidence solution makes it very easy for the viewer to follow and understand exactly what happened. The exported video should be saved in SEF (Secure Export Format) for secure non tamper file system with Password key which can be set to 20 Characters. The Client application should support dual password mode for each user.
48	*Advanced Activity Search* - The software should have the capability to have intelligent and advanced activity /event search detection methods of last 25 such instances in a given period of time which will enable user to search a particular portion in the entire video where the incident / theft / bomb was kept within couple of minutes. The Video of such event can be directly exported from here itself for further process
49	Any Android or IOS smart phones can be converted as a camera and integrated with the system software as and when required and the footage to be recorded. Static IP for the devices shall be provided by end user if opted for.

50	The Mobile Client Version shall be available in Android and IOS. The Mobile client shall have the below Minimum Feature list : - Grid of 4 cameras visible when a tablet device is used in a landscape mode. - Swiping gestures can be used to switch between camera grids and also with individual cameras to get to full screen mode. All system generated alarms. Easy date and time search for video footage, still images can be sent via email as JPEG files by a single tap, its PTZ control includes manual control, pre-set positions and camera tours, I/O controls, such as doors and lights, can be controlled by the Mobile Client and sites can be easily configured on the road.

Video Analytics	
Sr.No	**Required Parameter**
1	The video analytics (VA) shall be of global repute and shall be an inbuilt solution from the VMS manufacturer where the video analytics software is included in the basic VMS installation package and work as a windows service. The VA should run in the same Recorder as that of the VMS. VA licence key to be part of VMS Licence key to avoid complexities of multiple licenses.
2	The Video Analytics (VA) shall be designed to provide Intelligent Video Analysis for 24/7 surveillance with support for 3rd party devices
3	The VA configurator shall work as an independent windows application
4	The VA shall allow each camera to have 40 detection zones that are polygonal with a variable number of vertices so that any shape can be supported. Detection zone can also be a line, which can have one or many segments. The VA shall be flexible to use Rule based Analytics in any fixed camera in the project and shall provide with floating license for the particular server.
5	The VA configurator shall have easy to use graphical user interface with live alarms list for easy parameter fine tuning and feedback.
6	The VA alarms shall be recorded in the VMS similarly like other alarms, for example motion detection, audio detection and digital input alarms.
7	The VMS shall store the VA alarm video and image files for export
8	The VA shall support video from any camera supported by the VMS.
9	The VA shall support cameras using any of the video compression formats H.264/MPEG4/MJPEG.
10	The VMS shall support scheduling so that that VA alarms can be enabled or disabled for a certain period of time. The VA software shall be able to run atleast 4 different types of analytics in one single camera.
11	Calibration
	The video analytics shall have an easy to use 3D calibration tool where 3D calibration objects are matched to the actual camera viewing scene. The calibration parameters include camera height, camera viewing angle and camera tilt angle. (Picture of 3 D Calibration tool of the Software to be attached with the tender document as proof of the same)

12	The Presence filter detects when an object, person or vehicle is inside or crossing a zone or a line.
13	Camera Tampering
	Detects moving, defocusing or covering of the camera
14	Left Baggage/ Abandoned Baggage
	Detects and generates an alert highlighting Suspicious objects can be detected when carried into the scene and planted by a person as well as when dropped or thrown into the scene.
15	Enter and Exit Detection
	An “object entered” alarm is raised when an object crosses from the outside to the inside of a detection zone. Conversely, an “object exited” alarm is raised when an object crosses from the inside to the outside of a detection zone.
16	Stopping Detection
	Objects that are stopped inside a zone for longer than the defined amount of time will trigger the rule and raise an alarm.
17	Dwell detection
	Objects that dwell inside a zone for longer than the pre-defined amount of time will trigger the rule and raise an alarm.
18	Directional Detection
	Objects that travel in the configured direction (within the limits of the acceptance angle) through a zone or over a line trigger the rule and raise an alarm.
19	Object Classification
	VCA can perform object classification once the camera has been calibrated. Object classification is based on properties extracted from the object including object area and speed.
20	Objects Counting at least 40 counters linked to the detection rules, provide counting of all detection objects.
21	Camera shake cancellation –object tracker works even if the camera is on a swaying pole

4.13.2 Artificial Intelligence

Artificial Intelligence - AI Analytics	
S.No	**Required Parameter**
1	Video, Edge sensors based Analytics with Artificial intelligence and continuous learning are crucial for the safety envisaged, all analytics shall be edge based or cloud based or Server Based or a mix of all and will have the capability of continuous machine learning. The VMS, Video analytics and AI should be of same make for tight integrated system. The advantage of edge based analytics shall be to leverage the current AI technology available and help in incident based surveillance. The minimal functionality expected includes:
	A. Solid Waste Management/Vandalism related
	a) Graffiti and Vandalism detection
	b) Debris and Garbage detection
	c) Sweeping and cleaning of streets/bins before and after
	d) Garbage bin cleaned or not

	B. Traffic Management related
	1) Parking violation
	2) Over-Speeding vehicle detection
	3) Accident detection
	4) Helmet detection on two-wheeler
	5) Wrong way or illegal turn detection
	C. Citizens Safety related
	1) Detection and Recognize the pattern of demonstration and conflicts in crowd
	2) Detection and classification of human, animal and vehicle
	3) Loitering detection
	4) Person climbing barricade
	5) Person collapsing

4.13.3 NVR (Network Video Recorder):

S.No	Description
1.	The Network Video Recorder (NVR) will be connected via a Gigabit Ethernet network.
2.	NVR shall be of N+M configuration, M value will be decided during due-diligence
3.	All equipment shall be designed to provide a usable life of not less than 7 years.
4.	The NVRs shall have a self-diagnostic feature including disk status, CPU usage, motherboard temperature, network status and fan status.
5.	The NVRs shall be support interface using 10/100/1000BaseTX. It shall support a total 512 Mbps incoming badnwitdh. The NVR shall be powered using 100-240VAC/50Hz.
6.	The NVR shall support both Linux or Windows platform/or as per solution requirement.
7.	The NVR shall be capable of digitally signing stored video and digitally sign exported video to ensure chain of trust.
8.	The NVR shall have failover and redundancy built in with seamless playback without manual intervention.
9.	The NVR shall support a minimum of 200 recorded video streams and 20 playback and NVR shall support failover and recording redundancy built in seamless without manual intervention.
10.	All equipment shall be modularly upgradeable so that it does not need to be replaced in its entirety to increase memory capacity, to upgrade processing performance, or to reconfigure I/O options. NVR should support H.265 video compression.
11.	Normal state (non-alarm) recording configuration to provide for “Detection” as defined by and as follows: ▪ Resolution HD ▪ Normal Frame rate of 25 FPS
12.	Alarm state recording configuration to provide for “Recognition” as defined by ULC-317-1997 and as follows: ▪ Resolution of HD ▪ Frame rate of 25 FPS ▪ Alarm state recording of one track of audio at 32 Kbit ▪ quoted/proposed models should have EN/CE, FCC and UL certificate for NVR

4.14 Environmental Monitoring

Sl no	Monitor	Description	Parameter	Range / units
	Functional Specification			
	Environmental Sensor (ES)			
	Environmental Sensor will be connected on Smart Poles and location of ES would be Smart Pole locations.			
1.1	Air Quality Parameters	Chemical Parameters	NO2	at least 10ppm
1.2			CO	at least 1000 ppm
1.3			SO2	at least 20ppm
1.4			O3	at least 1000 ppb
1.5		Particulate Matter	PM 2.5	0 to 230 micro gms / cu.m
1.6			PM 10	0 to 450 micro gms / cu.m
2.1	Weather Parameters	Physical Properties	Temperature	0 to 60 Deg. C
2.2			Relative Humidity	at least 70%
2.3			Pressure	540-1100 Millibars
2.4		Other Properties	Light	at least 10,000 Lux
2.5			UV	at least 15 mW/ cm2
2.6		Chemical Parameters	CO2	at least 5000 ppm

3.1	Noise		Noise	at least 130 dB (A)
4		GPS	Yes	
5		GSM	Yes	Min. 2G compatible or better
6		Wi-fi	Yes	
7		Power	12 V , 2 A DC supply for ES	Option for solar power pack
7.1			12 V , 3 Amp DC or 230 V, 1 Amp AC	
	Physical Specifications			
1		Dimensions	Shall be customized based on requirement.	
2		Mounting	To be located in a housing, on a pole	
3		Construction	IP65	

4.15 Solid Waste Management Solution

4.15.1 Overview

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

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

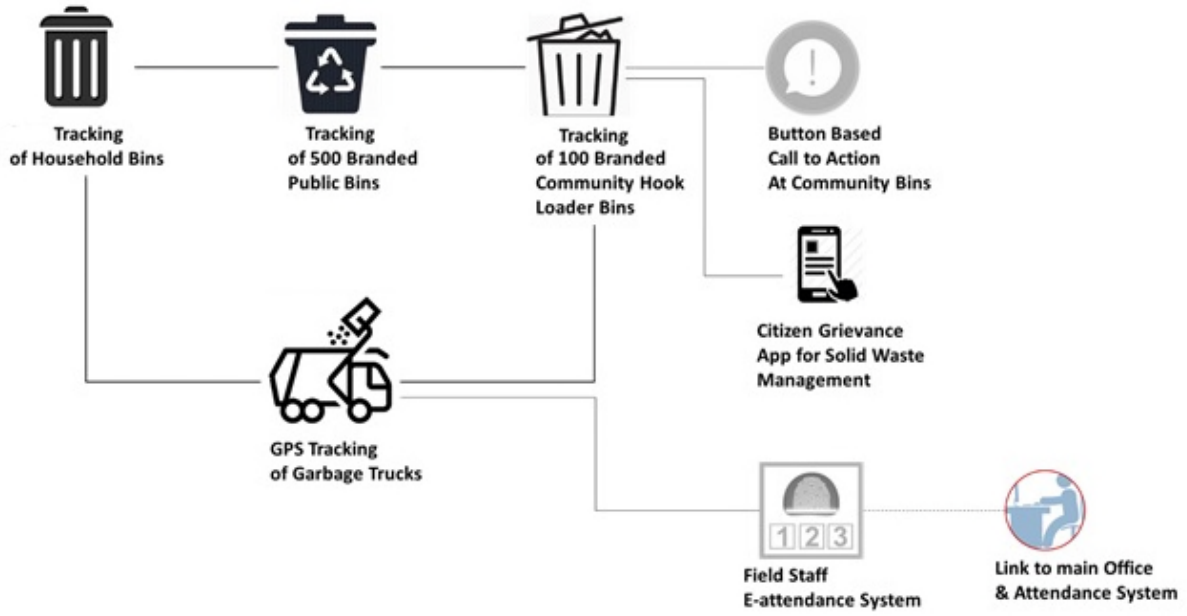
Currently, managing people responsible for the activity and proper utilization of assets/resources assigned to them has become a complex job for AMC. The main problems of existing solid waste collection process are:

a) Lack of information about collection time and area.
b) Lack of proper system for monitoring, tracking collection & transportation vehicles
c) Physical visit required to verify employee performance

d) Transfer of waste from primary collection to secondary collection is vehicle transfer and improper co-ordination leads to missed trips and garbage piling.
e) Lack of quick response to urgent cases like truck accident, breakdown, long time idling, etc.

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

a) Door to door collection tracking and monitoring
b) GIS Mapping of Commercial Establishment with Entity Type
c) RFID Tags/QR Code for door to door, waste tracking and monitoring. Primary objective of the project is to track location of waste pickup at each house-hold/commercial establishments and tipper vehicles movement.
d) Option to capture pictorial evidence with GPS Location and issue notification for each pickup.
e) Placing RFID tags/QR Code on each house-hold/Commercial Establishment/Dustbins from where waste need to be picked up.
f) Option for Route Creation over the Map
g) Route assignment/roaster management for route scheduling and assignment
h) Manage routes and vehicles dynamically through an automated system.
i) Route optimization which shall help in reduction of trip time, fuel saving and serving more locations
j) Reduce human intervention in monitoring process
k) Determine the Route Violation if any
l) Record & maintain history of vehicle routes, attended sites/missed sites/bins and other details
m) Reporting of vehicles, garbage collected and other SWM details to higher authorities from any location at any time
n) Monitor and track activities of field staff on daily basis
o) Real time management of missed garbage collection points
p) Ensure complete coverage of door to door and community collections
q) Option to send verification SMS/notification to registered mobile number for each household and collect response.



4.15.2 Project Intent

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

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

4.15.3 Scope of Work

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

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

a) Implementation of “Door to Door Collection Monitoring System”

- Supply and installation RFID tags/QR Code and GPRS Based RFID readers/Smart Phones.
- Design and integrate Door to Door Tracking and Monitoring System

- Registration of Each House Hold/Floor/Commercial Establishment for Master Data

b) MSI should provide Automatic Vehicle Locator solution to vehicles to track the complete traverse path round the clock with any state of movement or non-movement

c) MSI should provide GPS and Pictorial based attendance management system to the staff

d) MSI should install surveillance cameras at bulk waste generation/ collection points.

e) MSI shall provide an MIS system which shall be capable of recording details of daily waste collection, waste processed and waste disposed in terms of tonnage. Solution shall be automated with a computerized weigh bridge. Data from the weigh bridge shall be transmitted online to OCC.

f) Integrating data feed from waste disposal site (data feed access would be provided by DMC) like feeds from CCTV camera and Data from Weigh Bridge

g) Sizing of hardware, software and network devices required in DC/DR for using the Integrated SWM.

h) Supply & Installation of hardware (servers), software and network devices required in DC/DR for using the Integrated SWM.

i) Design, Development, Supply, and Deployment & Implementation of Web Based Application software integrated with GPS, RFID devices, QR Codes & Vehicle Tracking Management System (VTMS) and complaint management modules.

j) Mobile Apps for both Android & iOS for Citizens for complaint and Door to Door Solution and also integrate with Citizen App

k) Maintenance of RFID devices and other provided hardware and after warranty period including the replacement of devices in case of damage, new vehicle or any other change.

l) Maintenance of web based application/mobile apps for Integrated SWM, during and after warranty for a period of 5 years.

m) Real time management of missed garbage transfer

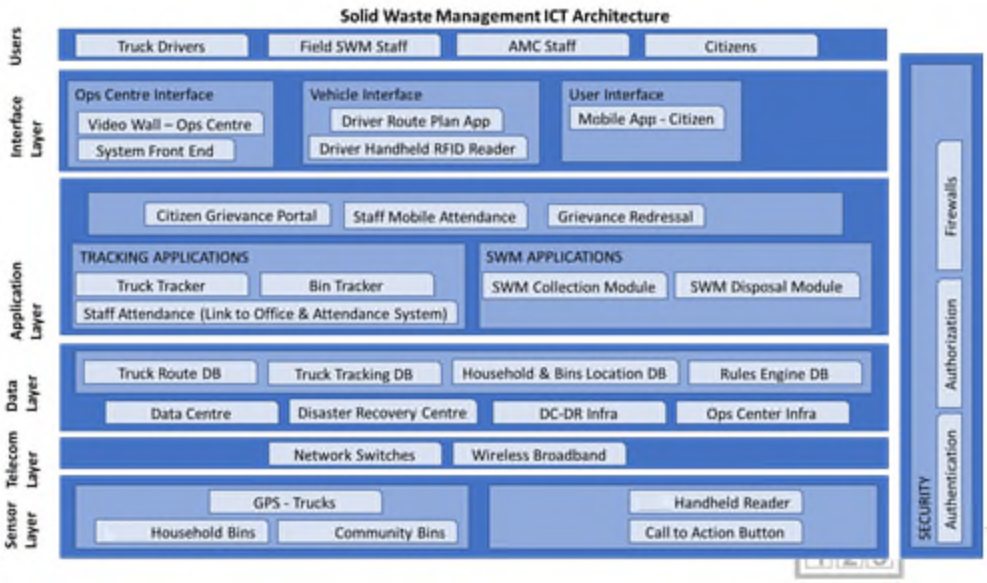
n) Daily report of Door-Door Collection efficiency combined with complaints raised by Public

o) Monitoring & Reporting Application - reports of vehicles, garbage collection status, bin status etc.

p) Provide resources for support, maintenance and administration of the system.

q) Integration of ISWM with City Operation Command Centre

r) Provide training to DSCL resources for operating the SWM system.



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

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

4.15.5 Functional Specifications

Automated Vehicle Tracking Management System

a) GPS tracking of waste pick up vehicle for real time tracking

b) System should help in co-ordination between primary and secondary collection vehicles for transferring dump

c) Route Optimization will help in reduction of trip time, fuel saving and serving more locations

d) System should ensure that complete coverage of door to door and community collections served by vehicles
e) Record history of vehicle routes, attended sites and other details
f) Monitoring & Reporting Application - reports of vehicles.
g) Ensure complete coverage of door to door and community collections served by vehicles
h) Alert / Alarm management for Ignition/Over speed/Power Cut and tempering
i) Solution should be integrated into the GIS map

Mobile GPS based Staff Attendance Management System

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

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

Mobile Application for Customers

MSI should integrate Citizen app provided to citizens/public which will help them raise complaint for following:

a) Garbage Pile on the roads
b) Missed Garbage Collection at residential, commercial, industrial and other areas
c) Crowd sourcing application for compliant registration and grievances
d) Request for Garbage Collection
e) Other issues like Street Sweeping and Blocked Nala/nali etc

Unified Dashboard View for Solid Waste Management

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

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

Infrastructure Solution - Field Devices

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

a) GPS Tracking System with all fittings & fixtures in all the vehicles
b) GPS based mobile attendance management.
c) CCTV Cameras at Waste Processing Site and at bulk waste generation points
d) RFID tags/QR Code at households /RFID tags/QR Code on collection vehicles
e) Automated Weigh bridge

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

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

Common Functional Requirements
Dashboard:

Dashboard Module should give a quick and easy view to know overall fleet status on real time basis. It should display status information of all vehicles i.e. Running, Idle or Standby. Dashboard view should provide following information:

- For each department, separate authentication based vehicle tracking module.
- Within department section, there shall be an aggregated view of all department specific vehicles, its location, movement and other real-time details shall be available.
- There should be a facility to club area specific and category specific vehicles in groups.
- Zone name, Ward Name, Vehicle No, Vehicle Type, Current Location & Last Updated Date & Time of each vehicle.
- It should give alert message if GPS device gets disconnected from a vehicle.
- Dashboard should have search parameter where different searches i.e. Vehicle Number wise, Zone & Ward wise, running / idle / standby vehicle wise and "No communication" wise searches can be done.
- Running Km and Idle KM Related parameters also required on daily basis
- It should also give an indication regarding running speed of vehicle i.e. Normal speed, Alarming speed and above Alarming speed.
- There should be a provision to see route followed by a vehicle on a GIS map.

Map Based Analysis:

Integration with:	**Functionality:**
▪ GIS ▪ Vehicle Tracking System	▪ Creating buffers along emergency site & working site. ▪ Creating & sending alerts in case SUB's reach particular level for vehicle movement, which can be shown on the map

Functional Requirements – SWM:

Area Details:

- Area information (Zone / Ward / Colony / Society)
- Population details
- Volume of Solid waste which includes Wet & Dry waste (recycled & non-recycled)
- Resources required
- Collection procedure (i.e. Primary: House to House & Secondary: Community Bin to Garbage transport centre or mix)

Garbage Collection Scheduling:

Integration with: ▪ **GIS** ▪ **Vehicle Tracking System**	**Functionality:** ▪ Assign SWM Vehicles to pick-up Garbage. Category wise assignment like A: Highly in demand, B: Medium, C: Low Demand. ▪ Assignment of dynamic routes using vehicle initial route and bins attended. ▪ Location-wise assignment of Sanitation Staff ▪ Scheduling of garbage collection and cleaning activities with the objective of maximizing citizen friendliness and optimum use of resources.

Primary Garbage Collection & Disposal:

Integration with: ▪ **Weigh Bridge**	**Functionality:** Record volume of garbage collected/disposed on daily basis.
Integration with: ▪ **Vehicle Tracking System**	**Functionality:** Keeping certain Checks as per environmental regulations, like minimum frequency of lifting garbage etc
Management Information System (MIS):	
▪ Monitor deployment of pickup trucks & personnel based on schedule originally drawn. ▪ Info on use of Transfer Stations / Quantity of garbage received ▪ Door to door collection, ward wise / Dashboard for all activities ▪ Reports of Ward Wise Weight Reports. / Any other custom report as per department	

4.15.6 Technical Specifications

GPS System

Item	Minimum Requirement Description	Compliance (Yes/No)
GPS Receiver	Minimum 16 channels	
GPS re-acquisition functionality	Cold start <= 42 Sec, Warm Start < 35 sec, Hot Start <= 2 Sec	
GPS Tracking Sensitivity	-165 dBmtyp	
GPS Velocity Accuracy	< 0.01 m/sec	
GPS Navigation Sensitivity	-148 dBmtyp	
GPS Navigation Update	1 Second	
GPS Data Format	Support WGS – 84	
GSM/GPRS Band	GSM/GPRS SMT quad band and UMTS (3G)	
GSM/GPRS Network Support	Support all GSM Network	
Data Acquisition and Transmission	Data packets shall have configurable fields - Unit ID, Latitude, Longitude, Speed, Time Stamp, Orientation, GPS fix, Alert Status.	

Data Acquisition and Transmission	Shall be configurable for Data Transmission at varying minimum time intervals of few seconds and minutes to a central computer application	
Data Acquisition and Transmission	Shall support GPS data storage atleast 10000 logs (based on string size) during non GPRS coverage area and forward the same when GPRS coverage is available. Shall be capable of storing 150 or more route geofences with facility to update route geofence master in the device over the air	
Data Acquisition and Transmission	Shall transmit data in SMS mode when GPRS is not available	
Micro Controller Module support for Interface	16 bit RISC architecture based Micro Controller system for interface with various sub systems	
Antennas	Built -in GPS and GSM Antenna.	
Audio Interface	16 Watts Audio Amplifiers 4 Loud Speaker (4 Watts each)	
Power Supply	Power Supply input support 7 V to 32 V DC battery and shall be powered by vehicle battery and not ignition	
Internal Battery Back Up	6-8 hours backup	
Environment	Shall be heat resistant, dust resistant and water / rain splash resistant, dustproof, shock proof and tamper proof. Shall have at least IP65 or higher protection classification Operate between 0°C to +55 °C	
Status LEDs	Power, GPS, GSM, VMU Status	
Alerts & Notifications	Shall be programmed to provide Alerts on power supply disconnect, speed violation, device tampering etc.	
Configuration	Shall support Over The Air (OTA) firmware upgrade and shall be remotely configured for the required GSM Service Provider, Server IP connection, GPS data Update Interval etc.	
Packaging & Accessories	Dimensions: 121mm (L) x 102mm (W) x 30mm (H) with power supply cable	
Rating	22 tracking / 66 acquisition minimum	
General Requirement	GPS tracking device should have adequate intelligence and programmability to run custom	

	edge applications and analytics on the edge device.	
General Requirement	GPS tracking device should have embedded storage and compute and should offer SDK/API for custom tools and application portability into the same.	
Device I/O	GPS tracking device should have minimum 3 digital input and One Analog input and One input for SOS	
RFID TAG		
Item	**Minimum Requirement Description**	**Compliance (Yes/No)/Page No**
Type	ABS, High Quality Engineering Plastic	
Supported Transponders	ISO18000-6C EPC Class 1 GEN2	
Frequency Range	ISM 865~928 MHz	
Operation Mode	Fixed Frequency or FHSS Software Programmable	
Memory capacity	Tag shall support ISO18000-6C protocol standard 2K Bits storage capacity, 1728 Bits (216bytes) writable user area; MR6730B metal supports EPC C1 GEN2 (ISO18000-6C), with 96Bits writable EPC Code area, 512Bits writable user area, and 32Bits password area, EPC 128 bit user 512 bit TID 96 bits.	
Reading Rate	Software Programmable, Average Reading per 64 Bits < 10ms	
Tags material	Metal material	
Reading Range	Shall be able to be calibrated (to be kept as 4 - 6 m max) based on the site visit	
Operation Temp	0°C to 60°C	
IP Classification	IP 68	
Weather	Heat, dust proof, UV resistant & sea water resistant	
Chemical Resistance	No physical or performance changes in -168 hour Motor oil exposure 168 hour Salt water	

	exposure (salinity 10%) 5 hrs Sulfuric acid (10 %Ph 2) 1 h Naoh (10 % Ph 14) exposure	

AVLS System

Item	Minimum Requirement Description	Compliance (Yes/No)/Page No
General Requirement	Each vehicle, using the GPS vehicle tracking (VTS) device, shall determine its precise location through GIS based GPS System and transmit the same to the City Operation Centre at defined intervals of time. The location shall be displayed on GIS based route maps at City Operation centre	
General Requirement	AVLS shall be able to give ETA at next bus stops in real time based on speed and distance measured. System shall update ETA at each bus stop on all PIS accordingly.	
General Requirement	System shall be able to compare the actual location of the vehicle / bus, at any given time, with its scheduled location	
General Requirement	System at the control rooms shall be able to calculate the time for the vehicle / bus to reach all subsequent stops along the route, factoring in the current vehicle / bus and any deviations from the schedule and reported traffic congestion enroute	
General Requirement	Shall provide inputs/feeds to Passenger Information System (PIS) with the real-time data to be displayed at various display units and announcement systems	
General Requirement	Information elements that need to be captured and transmitted to City Operation Centre at the minimum include longitude, latitude, and physical location enroute with date and time stamps, vehicle / bus number, route number, and Driver ID, etc.	
General Requirement	Shall provide these data on real time basis at pre-determined and configurable intervals (10 seconds) over GPRS/GSM network	

General Requirement	Tracking of vehicle / buses that deviate from the scheduled route based on definition of permitted geographic regions of operation	
General Requirement	Vehicle Fleet Summary Dashboard – Quick view on vehicle fleet performance	
General Requirement	Register a vehicle / bus on unscheduled route from backend on real time basis	
General Requirement	Application must have the functioning fort planning/scheduling/Rostering/Dispatching of any Bus using Software	
General Requirement	Option should be there on Driver Console to accept the route assigned by dispatch manager at which bus has to ply	
General Requirement	Real Time ETA based Trip Management showing trips in progress/completed trips and scheduled trip and Missed Stoppage Details etc	
General Requirement	Fare Collection Summary for Each Bus and Stoppage wise for the day	
General Requirement	Exception Recording/ Actions (Over-Speeding, Harsh Acceleration, Harsh Braking, Off-route Detection, unscheduled stoppage, Non-Stoppage at Bus stops/collection points, Trip Cancellation).	
General Requirement	Real-time Running Trip Line diagram of vehicle / buses on a particular route, for headway detection.	
General Requirement	Auto headway detection and notification.	
General Requirement	Applications Software shall have a facility to define the Masters.	
General Requirement	New routes shall be created in the application.	
General Requirement	Business rules engine for fare stages, fare structures, various routes etc. shall be configurable.	
General Requirement	Facility shall be provided to collate the transactional data received from Depots and Bus Stations. The transaction data shall be uploaded once every day for the previous day.	

General Requirement	Officials shall be able to access the application as per the pre-defined roles and responsibilities	
General Requirement	Application shall provide facility to query the data and generate the customized reports as per the requirements.	
General Requirement	System shall display the contact details of the bus driver / conductor so that the operation centre staff can communicate with them directly.	
General Requirement	Operation Centre operator shall be able to drill down to the exact location of the event by clicking on the alert and see the position of event drawn over the map along with driver, vehicle and standard description of event details related to the business rule.	
General Requirement	The system be able to integrate with the City IOP/City Operations Platform with all the available data like Location, route information, Vehicle telemetry information, Speed etc.	
General Requirement	The system should allow programmability, allowing actions to be triggered based on events. e.g. speed metric can trigger API call to GIS Maps pulling speed limit on the road based on GPS or GTFS location.	
General Requirement	The platform should offer an Application builder for developing custom Applications as needed and should support an Interactive Development Environment that can facilitate in-house expertise to develop widgets and create API extensions	

Sl. No.	Item	Minimum Requirement Description	Compliance (Yes/No) Page No
MDT.001	Processor	At least Dual core, 1 GHz or more	
MDT.002	Memory	RAM at least 1 GB or better	
MDT.003	Storage	At least 8 GB or higher	

MDT.004	Operating System	Android v 4.1 and above	
MDT.005	Network	2G bands: GSM 900 / 1800 / 1900 3G bands: HSDPA 900 / 2100 Speed: HSPA 14.4/5.76 Mbps GPRS: Yes EDGE: Yes SIM: Single or dual sim	
MDT.006	Display	Capacitive touchscreen, 16M colours Resolution: 480 x 800 pixels (~217 ppi pixel density)	
MDT.007	Generation	2G and 3G support	
MDT.009	GSM	Yes	
MDT.REQ .010	Screen size	minimum 4" with touch support	
MDT. 011	Camera & Video	at least 3MP Front & 5 MP rear with LED Flash (integrated) Geo-tagging, face/smile detection Video: Yes	
MDT. 012	Feature	Should work as Location Tracker device for Attendance Management System	
MDT. 013	Screen luminosity	Daylight readable	
MDT.014	Speakerphone	Hands free Support	
MDT. 015	Keyboard	Virtual on Screen	
MDT. 016	Communicatio n	GPS: Yes with GLONASS, WLAN: Wi-Fi 802.11 b/g/n, Wi-Fi Direct, hotspot, DLNA, Bluetooth: v4.0, A2DP, apt-X, USB: microUSB v2.0	
MDT. 017	Audio Playing Format	With 3.5 mm Jack MP3, wav files format etc.	
MDT. 018	Ports	Micro USB * 1 version 2.0 and above and same for charging and Headset port etc.	
MDT. 019	Power Supply	230V, 50 Hz AC Supply	
MDT. 020	Bluetooth	Yes	
MDT. 021	Battery	minimum 1500 mAh and above	
MDT. 022	Charger	Suitable charger shall be supplied, Built-in rechargeable battery pack/battery. USB Charger	
MDT. 023	Mobile Device Monitoring	Should support the ability to disable access to public App	

		Stores based on a policy configuration	
MDT.REQ.024	Mobile Device Monitoring	Should have configuration Policies to allow individual Components of the mobile device to be enabled or disabled.	

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

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

PTZCA.008	Auto adjustment & Remote Control	Colour, brightness, sharpness, contrast, white balance, exposure control, backlight compensation, Gain Control, Wide Dynamic Range	
PTZCA.009	Protocol	HTTP, HTTPS, FTP, RTSP, RTP, TCP, UDP, RTCP, DHCP, SNMP	
PTZCA.010	Security	Password Protection, IP Address filtering, User Access Log, HTTPS encryption	
PTZCA.011	Operating conditions	0 to 50°C	
PTZCA.012	Casing	NEMA 4X / IP-66 rated	
PTZCA.013	Certification	UL / CE / FCC / EN	
PTZCA.014	Auto Detection & Configuration	Camera should be automatically discovered & configured when connected to VMS or Network Switch, to set right network parameters for video stream on the network	
PTZCA.015	Activity detection	Camera should support User- definable alerts with configurable sensitivities and thresholds, email alert, HTTP notifications. Camera should support for IEEE 802.1X authentication	

4.16 Workflow and DMS

General Compliance

1 The system should be platform independent and should support both Linux and Windows platform. It should support both these platforms with or without virtualization.

2 The system shall support separate Document/Image server for better management of documents and store only metadata information in database.

3 Support open, scalable, Multi-tier architecture with each tier fully independent with support for clustering.

4 Compliance to workflow standards: BPMN, BPEL and WFMC.

5 Inter-operability - The systems must seamlessly integrate with any or all of the existing legacy and Core applications and shall support interface with other open-standard systems.

6 The system shall support multiple databases i.e. MS SQL, Oracle and Postgre SQL

7 DAK Management and File Management should be licensed module and should be compliant with Manual of office procedure published by DARPG. They should be available in OEM price list.

8 DMS, Workflow, DAK/Correspondence Management and File Management and Scanning component should be from a single OEM only.

Correspondence (DAK) and File Management System

1 DAK and File Management system should build using robust Enterprise Document Management and Business Process Management as a platform and should comply with the Manual of Office Procedure (MOP), published by the Department of Administrative Reforms and Public Grievances (DARPG). Correspondence and File Management System should be available in OEM price list. Please provide confirmation from OEM on letter head.
2 The system shall have a repository or predefined folder / area where all new correspondences (DAKs) are received after scanning. The system should be secure and should be tested for OWASP top ten vulnerabilities at one of the Govt./PSU organization. Please provide any documentary evidence.
3 The system shall have a facility to create Paper profile of a DAK in the repository, in case correspondences (DAKs) are not scanned.
4 The system shall have a facility to add correspondences (DAKs) in electronic format from local computer drive.
5 The system shall provide a facility to view correspondences (DAKs) on RHS and indexing fields on LHS.
6 The system shall have a facility to add a Note with a correspondences (DAKs). Using the tablets and mobile users should be able to access the Files and DAKs
7 The system shall have a facility to save the correspondences (DAKs) in an existing file.
8 The system shall have a facility to route the correspondences (DAKs) using workflow feature of a system.
9 The system shall support ad-hoc routing of a document
10 The system shall have a facility to prepare response and attach with the correspondences (DAKs) workflow
11 The system shall provide an interface to track & search the status of a correspondences (DAKs) in a workflow
12 The system shall have a facility to send the reminders.
13 The system shall have a facility to generate various reports w.r.t. correspondences (DAKs) workflow such as pending with users, pending since, elapsed time, initiated by, completed by etc.
14 The system shall have a facility to track a department where a correspondence (DAKs) is pending.
15 The system shall provide a advanced search interface for tracing & searching a correspondence (DAKs) based on dates, subject, pending with, completed by, pending since etc.

16 The system shall have a feature to recall a correspondence (DAKs) from other user. The system should be built using the Business Process Management framework.
17 The system should have facility to put the completed DAK in a new or an existing file.
18 The system should facilitate creation of a new electronic file in the system.
19 The system shall have a facility to create both main as well as part file.
20 File creation shall take at least File Number and File Subject as an input.
21 The system shall have a facility to save the file in the desired location folder.
22 The system shall also generate a Barcode number on successful creation of a file. This barcode can be pasted on a physical file for tracking, in case physical file is also used.
23 The system shall have facility to print barcode number of file at any point of time.
24 The system shall have facility to add documents in the File.
25 The system shall provide facility to view all letters/documents at the right hand side (RHS) of the folder with note-sheet on left hand side
26 The system shall provide facility to users to append their notes, which shall be automatically stamped with user name, date and time
27 The system shall provide facility to secure notes in File View
28 The system shall support the Whitehall view of the file. The system shall replicate the Present file handling in the same manner as followed i.e. electronic files shall give the same look and feel of Physical file with documents on the right hand side and green note sheet on the left hand side.
29 The system shall have an In-built Web based Text Editor with basic functionalities such as bold, alignment, font, color etc.
30 Solution should have the Green Note sheet.
31 System should differentiate between Administrative general files (Subject Files) and Administrative specific files (Special Files)
32 The system shall have a facility to create/open a new electronic subject file.
33 Subject File creation shall take at least File Number and File Subject as inputs.
34 The system shall have a facility to create both main as well as part file.
35 The system shall have a facility to save the file in the desired folder in the system.
36 The system shall also generate a Barcode number on successful creation of a file. This barcode can be pasted on a physical file for tracking, in case physical file is also used.
37 The system shall have facility to print barcode number of file at any point of time.
38 The system shall have facility to add documents in the File.
39 The system should have a facility to search a file on File number, file subject
40 The system should have a index table of all created files
41 The system should support creation of any types of special files such as employee files, property return file etc.
42 The system should have a provision to define searching attributes for each type of special file
43 The system should have a separate searching interface for each type of special file
44 The system shall provide facility to users to link the notes to any document, file and previous notes, so that corresponding objects can be directly opened from the note view
45 The system shall provide facility to users to append notes in the same paragraph
46 The system shall provide security on notes so that Noting/comments once written, signed and forwarded shall not be amendable by any user including originator, however if a new note has not been written, the user shall be able to modify the latest note, which he is writing.

47 The system shall provide facility to take print out of the noting for filing in paper folder as record
48 The system shall provide a facility to add new documents in the file by calling native application like Word, Excel etc. from the same interface.
49 The system shall provide facility to open multiple documents simultaneously.
50 The system shall have a facility to create a paper profile of a document in the file, in case document is not available in electronic form.
51 Using workflow feature of a system, user shall be able to route the file.
52 The system shall provide a feature to recall a File from other user
53 The system shall provide an interface to search the status of a file in a workflow.
54 The system shall provide a facility to track a department where a File is pending.
55 The system shall support the case file management
56 File view shall provide facility to view all documents inside file, Noting / commenting, Edit file properties.

Committee & Meeting Management:

1 The system should have the capability to constitute the committee with its members and convener details. It should be built using Business process management platform.
2 The system should have the capability to capture various details of the committee such as term of reference, tenure, committee members etc.
3 The system should have the capability to define the role of the each committee members.
4 The system should have the capability to define the committee members from the internal departments as well as external users along with required details.
5 The system should have the capability to define the message template for sending the notification to respective committee members.
6 The system should have the capability to create and saving the templates for different type of notification messages.
7 The system should have the capability to define the approval process for committee constituted.
8 The system should have the capability of User Inbox where committee members/approvers can view the pending request for approval.
9 The system should have the capability to attach the required documents with various committees constituted.
10 The system should have the capability to circulate the Office Memoranda with the respective committee members/stake holders having details about the committee.
11 The system should have the capability to define the meeting details such as Agenda, date, time, venue, priority etc along with the required documents.
12 The system should have the capability to link the members with meeting from the list of pre-approved committees.
13 The system should have the capability to define the approval workflow for Meeting scheduled.
14 The system should have the capability to define the Meeting invitation templates for sending the notifications to all the committee members.
15 The system should provide the calendar view having details about the meeting schedule on weekly/monthly basis.

16 The system should provide the capability to submit the response about their availability for the meeting scheduled.
17 The system should have the capability wherein convener can define the deadline of submitting the response of member's availability.
18 The system should have the capability to capture the Minutes of Meeting.
19 The system should have the capability to assign the actionable to the respective committee members.
20 The system should provide the capability to define the deadlines of submitting the response for defined actionable.
21 The system should provide the capability to designing the template for circulating the Minutes of Meeting (MOM).
22 The system should provide the capability to send the MOM notification through email.
23 The system should provide the capability to track the actionable assigned to the respective committee members. The system should be built using the Business Process Management framework.

RTI/Grievance Management:

1 The System shall provide facility to link cross-related documents like Application form and Grievance Re and reply sent etc. The system should be built using the Business Process Management framework.
2 The system should be able to automatically set a deadline and priority for the resolution of complaints based on the type of grievance as per the departmental policy.
3 The system should have capability to delegate responsibilities to an alternate user in the absence of the assigned user.
4 The system should allow the user who reviews the complaint to assign the task of redressing the grievance to another defined user from a list, and optionally also assign a criticality level.
5 The system should have capability to automatically escalate the complaint to higher authorities on passing of the deadline for the RTI request.
6 The system should have the capability to define the workflow for RTI Application, First Appeal and Second Appeal etc.
7 The system should have the capability to assign the RTI request to concerned department.
8 The system should have capability to set an extended deadline for pending grievances/RTI requests based on inputs received from higher authorities.
9 The system should have capability to inform the Citizen by email that the grievance has been redressed.
10 The system should automatically generate call back lists when complaint has been resolved
11 The system should have the capability to define & generate the RTI Response/Grievance Response Letter in a format from the system itself.

Court/Legal Case Management:

1 Should be able to create Court file including various court details such as Case no, Case Type, Date of Filing, Case details, Court Order details, Hearing date, Order date etc. The system should be built using the Business Process Management framework.
2 Should be able to Track court dates, hearing dates etc.
3 Should be able to provide alerts for the upcoming hearings.
4 Should be able to Cross-reference all dates for one case, one client, one attorney, a group, or the entire office.
5 Should have the capability to generate the Case Diary having complete details and history of the cases.
6 Should be able to provide a mechanism for analysis of work flow, case status, and types of cases opened and closed
7 Should be able to maintain an audit trail of entries and changes.
8 Should be able to capture note sheet with the court case files.

Legislative Query Processing:

1 The Legislative Query processing modules should be built using Enterprise Content Management & Business Process Management framework.
2 The system should have capability to allow the personnel to assign selected query to the department staff from a list and different query to different users.
3 The system should have capability to alert the department officials through email, dashboard alerts, and automated SMS messages with reminders on deadlines for query response before the due date.
4 The system should have capability to record/update/close the status of Legislative Question. Should be able to maintain an audit trail.
5 The system should have capability to reopen a query which was inappropriately addressed and closed.
6 System should be able to present the data analytics in graphical format such as Bar graphs, pie charts, line graphs etc. based on user requirements.
7 The system should have the capability to define & generate the Parliamentary Questionnaire Response Letter in a format from the system itself.

Document Management System

Document Scanning Features:

1 Should provide an integrated scanning engine with capability for centralized and decentralized Scanning & Document Capturing. The scanning and document management solution should be from same OEM so as to provide an integrated solution right from capture to archival of documents
2 The scanning solution should have the capability to capture the document through mobile devices.
3 The mobile based document capture application and scanning solution should be from the same OEM.
4 Should have a well-defined capture module for support of document processing, validation, index building, and image enhancements.
5 "Should be able to support the capture of digital records of at least the following formats:
· Emails and attachments
· OCR documents
· Images - .tiff, jpeg, gif, PDF etc."
6 The proposed solution should provide for automatic correction of parameters like format/ compression not proper, skew, wrong orientation, error in automatic cropping, punch hole marks etc. during scanning. The scanning solution should provide support for automatic document quality analysis so that any bad quality document doesn't get uploaded to the repository. There should be an independent software quality check service available as part of overall scanning solution which can be used to audit scanned documents for resolution, format/ compression, orientation etc.
7 Support all the special image enhancement functionality offered by the scanner through the driver interface.
8 Solution shall support Bulk Import of image and electronic documents

9 Should have capability of automatic segregation of documents/records based on Barcode, Blank page, fixed page and auto Form recognition
10 Should have the capability of scanning on Linux platform.
11 Provide Image processing libraries that support image enhancements such as changing contrast, zoom in/out, cleaning etc. and other imaging features like compression and extraction etc.
12 The software solution should include the Rubber band feature for the extraction of the data using OCR technology so that user can mark a zone on image at runtime during scanning stage & map the extracted data with the indexing field.
13 The mobile capture should support image compression, B/w conversion from color images, G4 compression for B&W, JPEG for color and gray scale, multiple page document capture, auto cropping, auto orientation, perspective correction, noise removal and geo capture.

Architecture & Scalability:

1 System should be platform independent and should support both Linux and Windows for application server
2 Solution should have been built using server side java and J2EE technologies.
3 Solution should be multi-tier, web-based solution (having web-based front-end for users and as well as for system administrative functions) having centralized database, web and application server with support for clustering
4 The system should store only index information in database while images should be stored in separate file server.
5 Solution should be compliant to ODMA, WebDav open source standards.

Archival of Electronic documents:

1 The System shall support categorization of documents in folders-subfolders just like windows interface. There should not be any limit on the number of folder and levels of sub folder. The system shall support multiple databases i.e. MS SQL, Oracle and PostgreSQL.
2 The System shall provide facility to link cross-related documents like Application form and Field report, Grievance and reply sent etc.
3 The system shall provide search facility to in the same interface, so that users are able to search the documents to be linked
4 The system shall support versioning of documents with facility to write version comments
5 The system shall allow Locking of documents for editing and importing it back into the system through check-in/Check-out features
6 Repository should be format agnostic.
7 System should support configuration of verification processes for different business types. It should be able to handle multi-user environment for processing files related to different business types. While processing a file, all the data and images for each transaction should be displayed to processing users and processing users should be allowed to accept, reject or send the files for review

Document View:

1 The System shall support Applet for viewing Image documents- No third party viewers should be there for viewing of scanned images. Please specify if third party applets are used and the licensing terms together with cost implication
2 Even for multi page document. The download and view should be page by page. System should include mobile app for accessing documents.
3 The system shall facilitate zoom-in/zoom-out, zoom percentage and Zoom lens to zoom in on a part of image and other image operations like Invert, rotate etc.
4 Support archival & view of PDF/A format documents (open ISO standard for long term archival of documents)
5 Document view shall have the provision to draw a line, insert arrows etc over image document.
6 The system should support viewing and rendering of PDF/A documents in inbuilt viewer.
7 Document view shall have the provision to highlight or hide certain text by drawing line rectangle and solid rectangle.
8 The System shall support for viewing documents in native application.
9 The system shall provide facility of putting text, graphic and image annotations on scanned document pages.
10 The system should have mobile application for retrieval and archiving of documents

Annotations:

1 The Image applet shall support comprehensive annotation features like highlighting, marking text, underlining putting sticky notes on documents, and support for text and image stamps etc.
2 The system shall support automatic stamping of annotations with user name, date and time of putting annotations.
3 The system shall provide facility for securing annotations for selective users.
4 The system shall store annotations as separate file and at no time, the original image shall be changed. The system shall provide facility of taking print outs with or without annotations

Indexing:

1 The System shall provide facility to index folders, files and documents on user-defined indexes like department, ministry, file number, year etc.
2 The system shall facilitate manual and automatic indexing using OCR functionality or from other applications
3 The System shall support Automatic full text indexing for Text search.

Search and Retrieval:

1 The system shall provide extensive search facility to retrieve documents or Folders/Files
2 The system shall support saving of search queries and search results

3 The system shall support search for documents or folders on document or folder on profile information such as name, created, modified or accessed times, keywords, owner etc.

Security & User Management:

1 The Document management system shall support definition of Users, Groups and Roles relation in the system
2 The system shall support access permissions on Folders, documents and object level
3 The system shall support multiple levels of access rights (Delete/ Edit/ View/ Print/ Copy or Download).
4 System shall support for application based rights
5 The system shall support system privileges like Create/Delete Users, Define indexes etc.
6 The system shall support secure login id and passwords for each user and passwords shall be stored in encrypted format in database
7 The system shall have a facility to define password policy with extensive password validations like passwords must be of minimum 8 characters, shall be alphanumeric, locking of user-id after three un-successful attempts, password expiry, password history so that passwords are not same as previous passwords etc.
8 The system shall provide LDAP support for integrating with directory services and shall support single sign on
9 The system shall support Extensive Audit-trails at document, Folder and for highest levels for each action done by particular user with user name, date and time
10 The System shall support integration with database-based authentication.
11 The system shall support integration with PKI infrastructure as well as bio-metric solution for enhanced security.

Administration
1 The system shall support web-based administration module for the complete management of system.
2 The Admin module shall support Users/Groups/Role definition and granting Access Rights to them and set password expiries
3 The Admin module shall provide easy to use interface for Index structure definition that can be used by different users.
4 The Admin module shall provide interface for purging old audit trail and do selective logging i.e. select the system or application features for, which the audit trails have to be generated.
5 The Admin module shall provide facility to take complete and incremental backups and shall be able to integrate with third party backup solutions.

Reports and Audit Trails Features:

1 The System shall support extensive Reports and audit trails and shall also provide data points and facility to design new reports
2 The system shall support Extensive Audit-trails at user, Folder and Cabinet levels
3 The system shall provide facility to generate Audit trails on separate actions, and between specific date/times

4 The system shall support extensive reporting facility at document, folder and user level. Please specify all inbuilt reports available in the system and also provide effort estimates for new Custom reports to be designed

5 The System shall have audit trail to maintain history of all transactions performed on the system.

6 The system shall give flexibility to administrator to do selective logging i.e. suspend and resume audit trail generation for specific system and user activities.

7 The application shall log all the actions done by individual users with user name, date and time and the administrator shall be able to generate detailed audit logs and history of the process instance.

Reminders and Alarms

1 The system should have the capability to set automatic reminders and alarms to concerned users.

Integration and Web Services

1 Should be based on open standards and have API support for data import & export.

2 The System shall provide support to invocation of external programs to perform activities of a process like legacy application screen for data entry.

3 The System shall support integration based on standards such as XML

4 The System shall support message-based collaboration based on protocols such as HTTP, FTP and SMTP.

5 The System shall support integration with Email Servers.

6 The System shall provide fully functional APIs for Integration.

7 The System shall support Web based interfaces.

Record Management System

1 The system should be certified to Record Management standard like DoD 5015.02 or equivalent standard.

2 Solution should include Records Management component to comply with regulatory and legal policies for long-term archival of content.

3 Solution should manage lifecycle of documents through record retention, storage, retrieval and destruction policies.

4 Solution should support managing and tracking of physical location of documents

5 Solution should have facility to export / import electronic record with metadata in XML format

6 Solution should provide the configurable capability of record classification as per the record keeping structure (File Plan) of department.

7 Solution should have a provision to define physical location of record management facility

8 Solution should have a facility to define disposition schedule / policies for record

9 Solution should provide the capability for only authorized individuals to view, create, edit, and delete disposition schedule components of record categories. The complete schedules would be as per the organizational policies.

10 Solution should have a provision to move & track a record among users within office/across locations

11 When record is moved out of the facility, system should have a capability to capture the transport / courier detail

12 "Solution should provide report on the Records in the selected file plan component such as such as number of records present, number of record folder, Record creation date, etc.

- Report on activities of the selected user
- Report on the Request/Return activities
- Report on overdue items
- Report on items borrowed
- Reports on records, whose retention period are getting over in specified time
- Reports on disposition schedule

BUSINESS PROCESS MANAGEMENT SYSTEM (WORKFLOW ENGINE):

1 "The system shall facilitate re-engineering of processes and act as a platform for building specific application and have a workflow engine to support different types of document routing mechanism including:
Sequential routing -Tasks are to be performed one after the other in a sequence
Parallel routing - Tasks can be performed in parallel by splitting the tasks among multiple users and then merging as single composite work item. The system shall support conditional merging of multiple parallel activities i.e. Response from mandatory parallel work stages before it can be forwarded to next stage
Rule based routing - One or another task is to be performed, depending on predefined rules
Ad-hoc routing - Changing the routing sequence by authorized personnel"

2 Compliance to workflow standards: BPMN, BPEL and WFMC.

3 Support for registering and configuring third party applications in port let like view.

1. Process Designing

a. Graphical Route Designer

1 The workflow management system shall support Inbuilt Graphical workflow designer for modelling complex Business Processes using drag and drop facilities.

2 The Process designer shall provide intuitive interface for designing complex rules and conditions for workflow routing.

3 The interface shall be easy to use so that Process owners can change the business process as and when required without any programming knowledge.

4 The system shall enable process designers to design multiple sub-processes. This includes mapping of the existing process instance to the newly created process instance as per mapping defined in the route.

5 The workflow management system development environment shall provide easy navigation to choose sub-processes as required to be invoked from within a process.

6 Facility to copy and paste work stages along with all its properties.

7 Facility to define documents viewed and to be attached at individual stages.

8 The Process designer shall support multiple Introduction stages for introducing different document types from different acquisition sources
9 Facility to define multiple archive stages for archive selected documents and indexes in underlying Document management system at any stage of workflow process.
10 The system shall provide facility to define hold stages so that a particular instance or the workflow can be kept on hold for specified interval on the basis of pre-defined condition. The system shall also provide facility to define conditions for resuming the instance from hold stage.
11 The system shall allow process designers to design properties for each work stage like default document view, form view or Exception view etc.
12 The system shall allow users to define entry-level settings like Increase of priority or sending an email trigger on the basis of pre-defined conditions or setting up particular variable or property etc.
13 The workflow management system shall support the definition of roles and allow many-to-many relationships between users and roles to be defined.
14 Support for creating adhoc tasks at runtime and assigning to users

b. Inbuilt Form Designer

1 The system shall provide inbuilt facility to design Custom forms that can be attached at one or more stages of workflow.
2 The Form designer interface shall support facility to define text boxes, Combo boxes, radio buttons, Drop down etc.
3 The system shall provide facility to define variables in the process or in external database tables, which can be linked to fields defined in the form for efficient data entry.
4 The system shall provide facility to define zones at forms and images, so that relevant part of the image is highlighted for Image assisted data entry.
5 The system shall support field level calculations at form level
6 Facility to use scripts for defining field level validations

c. Inbuilt Exceptions

1 The system shall provide facility to define exceptions at individual stages, which shall dynamically change the route on execution.
2 The system shall facility to give rights to raise and clear exceptions at different stages of the process with user comments.
3 The system should have inbuilt Rule Engine for defining rules.
4 Facility to raise triggers on the basis of exceptions.
5 Facility to raise automatic exceptions on the basis of pre defined conditions.
6 The system shall track all the exceptions raised in the course of process and shall maintain history of that with user name, date, time and comments.
7 The system shall clearly differentiate process instances with and without exception

d. Inbuilt Triggers

1 The system shall provide facility to define custom triggers like Emails, Word template or launching executable etc. on predefined conditions
2 The system shall provide facility to define custom templates for the triggers with static and dynamic data.

3 The system shall provide facility to generate event based triggers for automatically sending mails/ fax, generating responses, invoking data form for data entry, communicating from external systems.

4 The workflow management system shall have email notification to user when the user is not logged on to the workflow management system. Upon receiving the email, the user shall be able to click on the URL in the email to automatically launch the Workflow management system and present the user with the task to act on.

2. Process Monitoring and Reporting

1 The workflow management system shall be able to keep track of the work item status, the date/time the jobs are started and ended, the creation and archival date of the documents.

2 The workflow management system shall provide graphical and tabular tools to view progress of each individual process

3 System shall provide a facility to configure dashboard for individuals for e.g. dashboard for director, dashboard for secretary, dash board for Additional director etc

4 No customization should be required to create dashboard, User should be able to configure dashboard without any coding.

5 There should not be any limit on the number of reports that can be created

6 User shall be able to drill down in a report for specific information analysis

7 "The workflow management system shall support the generation of statistical and management reports like:

• Number of pending files
• Time taken to complete each task
• Process History Report
• User Performance Report
• Average Process Time Report
• Participant Report
• Participant Processing Time Report
• Process Definition Summary Report
• Exception Details Report
• Expired Work item Report
• Diversion Report"

8 The workflow management system shall support the generation of performance comparison reports.

9 The workflow management system shall support users drill down from a higher level view of business processes to lower level details.

10 The workflow management system shall support statistical reports like Total turnaround time and delay report for complete process or specific work stages

11 The workflow management system shall support definition of new customized reports based on exposed data points.

12 The workflow management system shall also provide dashboard interface for online reporting of various processes. The interface shall give a flexibility to toggle between graphical and tabular view and tile different windows in the same interface

13 The system should include administration module to configure the user, groups, queue related to a process. The system should allow user to set their display settings according to the individual preferences and company policies. Users can customize their themes, resize components, and configure single /multi-column views. It should have navigation container to display the list of all component instances associated with the view of a user.

3. User Management and Security

1 The workflow management system shall support integration with Lightweight Directory Access Protocol (LDAP) for domain level authentication and single sign on.

2 The workflow management system shall support integration with database-based authentication.

3 The workflow management system shall be capable of giving access rights to users/groups on work stages, documents, forms and also to the data fields.

4 The workflow management system shall support extensive password validations i.e locking of user account after specified number of unsuccessful login attempts, password history, password expiry, passwords must be alphanumeric and of minimum character length etc.

5 The workflow management system shall support SSL, HTTPS and session timeouts.

4.17 Enterprise GIS

Scope of Work

- Base Map Creation
- Incorporation of Existing GIS Data
- Collection of Existing GIS Data

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

- Town Planning Schemes showing proposed land use zoning, transport network and sites designated for various public purposes.
- Maps showing administrative boundaries ward boundaries, census boundaries, slum boundaries.
- Revenue Maps showing Cadastral Boundaries.
- Soft copy Maps / drawings of utilities like solid waste disposal, roads along with the data available with other Concerned Department.
- Location of State and Central Government offices, railways and highways, police stations, primary &high schools, colleges, universities, primary health centers, hospitals, banks, theatres etc. also need to be located on the maps through field verification.
- All the details that Municipal Corporation/ Smart City desires to include.

- Data validation and gap analysis

o Selected Bidder will conduct QA QC and check the Qty , Quality, Accuracy, source and reliability of the collected data from Municipal Corporation / Smart City , whether the data (spatial or non-spatial) is recent or accurate enough to be used and not obsolete. Ad come with detail Gap analysis Report.

o Positional Accuracy Selected Bidder will check whether the positional accuracy of the existing data available with Municipal Corporation / Smart City is in sync with the Satellite Imagery provided by Municipal Corporation / Smart City . Selected Bidder will prepare base map using the available and fetched data and validation of the same will be carried out by the authorized officials of Municipal Corporation/ Smart City. In case of Field Measurement Books, they are to be built and super imposed on the Base Maps.

- Accuracy Requirement: The 10% of GCPs will be randomly selected as sample for the accuracy of .3 Mtrs. On the data and see whether data fits on the projection of baseman incase data doesn't fit Municipal Corporation/ Smart City will provide data which can be used.
- Reliability: Selected Bidder will check from the available legacy data with Municipal Corporation, whether the data (spatial or non-spatial) is recent or accurate enough to be used and not obsolete. In case data is rejected Municipal Corporation / Smart City will be responsible to provide rectified data.
- Attribute Validity: Selected Bidder will validate attribute data accuracy, whether the data accurate enough to be used and not obsolete.
- Procurement of High Resolution Satellite Imagery

o The selected bidder has to procure and supply ortho rectified having .3 Mt or better resolution latest satellite imagery

o Only procured imagery shall be used for the preparation of Base Maps, data from alternative online sources such as Google Earth / Google Maps is strictly prohibited as this is strictly against the usage policies of the respective services.

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

- DGPS Survey and Geo referencing and Post Processing of Satellite Imagery

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

o For Geo-referencing the Bidder needs to take the Ground Control Points (GCPs). GCPs are basically taken as a road intersection points, Building Corners, Permanent Locations etc. Bidder shall generate the Grid of 1 x 1 Sq. Km. on the Satellite Image and collect appropriate No of GCPS per sheet. GCPs need to be collected using DGPS. The locations identified on the image and real ground should be verified with the Authorized Representative appointed by the Corporation. The data should have following

▪ Projection: Universal Transverse Mercator (UTM), Spheroid: WGS 84, Zone: 43N. Observation time for DGPS instruments has to be minimum 12 (Twelve) Hours at Base Station and minimum 30 Min Thirty Minutes at each GCP using DGPS.

▪ The horizontal accuracy of GCPs should be 0.1-0.3 meters. 5% of GCPs would be randomly selected as sample for the accuracy. If the incorrectness in accuracy found in any sample, the entire work shall be rejected and shall be required to rework.

- Creation of Data Model

Data Model for storing the spatial & Non-Spatial data shall be decided by the Municipal Corporation / Smart City in consultation with the successful Bidder/SI in accordance with the National Large Scale mapping Policy.". Bidder will modify the data model and update the same with the help of detailed round of discussion with each concerned Municipal Corporation / Smart City department officials. Bdder will understand existing data model of Municipal Corporation / Smart City and will use proper tools to create the data model like CASE tools and UML etc. The final data model will be approved by the Municipal Corporation / Smart City and before proceeding further the data model will be finalized.

- Digitization of Satellite Imagery.

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

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

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

o Bidder will then take sufficient number of Ground Control Points (GCPs) collected through Differential Global Positioning System (DGPS) survey. Bidder will prepare an up-to-date large-scale base map (Scale 1:2000) of all the wards/zones of City using satellite imageries and then will prepare a new Database using the existing Database available with Municipal Corporation / Smart City , as unified Geo-spatial Data with infrastructure details.

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

- Creation of Utility Data from Paper / CAD Drawings

o Bidder will digitize Geo reference existing Paper/Cad Drawing in GIS

o Incorporating TP and DP in GIS

o Bidder wills Incorporate Geo reference existing TP and DP in GIS

- Final Base Map Preparation

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

o The layer list would be exhaustive taking into consideration of the features to be captured, the attributes will added etc., The layer list and the database layers would be created using programs, appropriately. All the data captured would be checked and validated using custom built routines for its accuracy and logical correctness. The rigorous QC process of

bidder would help in achieving accurate feature capturing, required accuracy in coding and classification.

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

- Data Migration

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

COTS GIS and Image Processing Software

Bidder will provide three licenses of COTS Based Standard Desktop GIS and Image Processing Software for Data Creation/Updating and Change Deduction and Image Classification

General Features	Compliance Yes/NO
Multiple Document Interface (MDI)	
Project, View and Layer Management	
Geo-Linked Multiple Views	
Well known Raster, Vector and Tabular file formats support	
On the Fly Map Projection Transformation	
Large set of Library for Projection & Geographic Coordinate System	
Advance Map Navigation and Visualization	
Seamless data handling using ORDBMS	
Identification and Measurement Tools	
Customizable GUI	
Extensive Map Composition Tool	
Raster and Vector Catalogue	
GIS Features	
Advance Drawing and Editing	
Topology Creation	
Edge Matching and Rubber Sheeting	
Geometric Correction	

Database Management	
Query Builder for Simple and Complex Query	
Legend Creator for thematic mapping	
A large library of symbols	
Rule Based Labeling and Annotation	
Geo-processing and Overlay Analysis	
Vector to Raster	
Advanced Report Generation with wizard	
Image Processing Features	
Image Enhancement and Filtering	
Image Analysis Tools	
Image Geo-referencing	
Image Extraction and Mosaicking	
Atmospheric and Radiometric Correction	
Image Transformation	
Image Classification	
Advance Segmentation	
Advanced Change Detection	
Raster To Vector	
Band Arithmetic and Linear Algebraic	
Advanced Module	
Network Analysis	
Defining Network Rules	
Add Network Location	
Remove Network Location	
Find Shortest and Optimum Path	
Location Analysis	
Multi Location Analysis	
Service Area	
Dynamic Segmentation	

Hyper-spectral Tools	
Internal Average Relative Reflectance (IARR)	
Auto IARR	
Log and Auto Log Residuals	
Normalize	
Rescale	
Spectrum Average	
Signal to Noise	
Mean per Pixel	
3D Modeling	
Terrain Extraction	
Flythrough & Walkthrough Creation	
Drape Raster, Vector and 3D Object	
Line of Sight and Radio Line of Sight	
View Shed Analysis	
Stereo Viewing	
Environmental Effect Like Fog, Fire, Cloud, Sun, etc	
Particle emitter	
Save Image & Animation [*.avi]	
Raster GIS Analysis	
Spatial Analysis	
Distance Tools:	
Math Tools	
Conditional Tools	
Extraction Tools	
Local	
Generalization	
Multivariate	
Neighborhood	
Weighted Overlay	

Terrain Analysis	
DEM to Contour and DEM from Point and Contour Line	
Slope and Aspect	
Hill Shade and Topographic Normalize	
Cut & Fill Analysis	
View Shed, Route Indivisibility and Line of Sight	
Best Path	
Area/Volume Calculation	
Hypsometry	
Semi Variance	
Surface Specification Points	
Anaglyph	
Global Positioning System	
Interface with GPS device	
GPS Tracking and Navigation	
Extract feature using GPS	
Simulate GPS file	
GPS data validation	
GPS error correction	
Satellite sky-view	
Speed and Bearing Indication	
Way-Path generation and storing	
Geo-fencing	
Different File formats support	
Export to KML/KMZ	
Hydrology Tools	
Fill	
Flow Direction	
Flow Accumulation	
Flow Length	

Sink	
Stream	
Stream Feature	
Stream Link	
Stream Order	
Basin	
Watershed	
Tracking Analysis	
Simulate and analyze time-based data	
Report on patterns related to time and defined rules.	
Monitoring of mobile resources	
Analyse patterns of movement	
Neural Network Classification	
Supervised	
Unsupervised	

Supply of COTS Enterprise GIS and Image Processing Server Software Platform

Bidder will supply Enterprise COTS based GIS and Image Processing Server platform which will install on at least 16 Core Hardware Server.

Sl no	Technical Specification	Compliance/Page Number
1	The proposed software should have functions of GIS and Image Processing along with advance functions such as network analysis, terrain analysis, 3D analysis, change analysis, etc.	
2	GIS Software must allow authority to implement a centrally managed GIS providing the advantage of lower cost of ownership through single, centrally managed, focused GIS applications (such as a Web application) that can be scalable to support multiple users and saves the cost of installing and administering desktop applications on each user's machine.	
3	Platform for GIS Application Software should be able to operate on Windows	

4	ODBC compliance enabling interface with RDBMS like Oracle, SQL server, Access etc. should be available.	
5	GUI shall be highly user friendly, self-explanatory and eye catching. It shall provide the sample example wherever it seeks user input and also preserve the history of the inputs. GUI can be made good looking and beautiful by making use of good color scheme and putting functions indicative image (drawing) on button.	
6	The proposed GIS software could be any Industry standard COTS GIS platform and should be easy to handle, operate, maintain & also train the authority staff/end users.	
7	The customized software for authority should have simple user interface both for departmental users as well as for citizens with easy navigation and querying facility.	
8	On-line help shall be provided at all functions and tools.	
9	The proposed software should be OGC compliant and follow the interoperability.	
10	The software should support OGC Services such as WMS, WFS, WCS, CSW, INSPIRE, etc along with GML, KML, etc.	
11	The software should support all types of raster formats and services like ERDAS IMAGINE, ENVI, PIX, DTED, DEM, CEOS, JPEG, JP2, PNG, GeoTIFF, & Web Coverage Service (WCS, OGC standard), Web Map Service (WMS), OGC standard.	
12	Should be able to support broad range of clients including browsers, desktops, Mobile Handsets, Palmtops, Tough books, etc.	
13	GIS Functions	
14	The proposed software should support multiple document interface (MDI), User should be able to create multiple views in single project.	
15	The application framework of the software should be such that it should have Dockable/Floating Toolbars, Dockable and Auto Hiding Windows, Unicode	
16	Support for Multilanguage Attributes, Drag and Drop to Rearrange Tools/Toolbars, Create New Toolbars or Menus without Programming, Extend the Applications with Add-ins built with .NET, Java, or Python, Build New GIS Components with .NET or Java or other development platforms.	
17	The proposed software should have capability to create layer as per the data model defined by the authority. User should be able create table structure as per the requirement.	

18	The software should have provision for definition of map projection system and geodetic datum to set all the maps in a common projection and scale.	
19	It should have facility to create custom projection using 3 to 7 parameters.	
20	It should have the facility to display multiple projection coordinates on map click.	
21	The software should provide facility to click on any feature of the map and return a select set of attributes for feature i.e. Identify tool along with pop-up.	
22	Software should have rich geo-processing functions such buffer generation, clip, erase, intersection, dissolve, union, polyline to polygon, etc. It should have facility to perform the spatial intersection analysis like plot area with buffer zone to calculate road-widening impact on adjacent land.	
23	The Software should be able to import / export data from / to various formats like .dwg, ,dxf, .dgn, .shp (shape files), coverage file, .mif (MapInfo), .mdb (GeoMedia), .gml, .kml, .gpx. , Geo PDF GeoJSON, interlis, GeoRSS, SqlLite etc.	
24	The proposed software should have function to import / export tabular data such as .xlsx, .csv, .dbf, etc.	
25	Support of IFC object for BIM applications.	
26	Support 3 D data	
27	Integrated GPS module for desktop and mobile GIS.	
28	Support of Coordinate Geometry (COGO) description for GIS objects creation and store in GIS database.	
29	Facility to define joins between the two tables (graphic / non-graphic) of the database to get integrated information in the table and perform GIS analysis.	
30	The system should provide facility to exchange the GIS Data with other platform applications like Microsoft Word, and Excel to use GIS data and generate reports like graph and charts.	
31	Software should have rich display and navigation tools. It should have zoom in, zoom out, fixed zoom in, fixed zoom out, pan, real time pan, bookmark, Geo link multiple views, swipe, flicker, search by location, cross hair, cursor location value, numeric dump, query cursor etc. It should have support of continuous panning i.e. real time pan.	
32	Software should allow the user to perform undo / redo operations during edits.	

33	The software should have module for geo-referencing of vector and raster data.	
34	Facility to capture the geometry from the layout maps, Building maps by maintaining the coincident geometry i.e. when a new polygon is captured simply by selecting an existing polygon to digitize the common boundary thereby ensuring no slivers or gaps between adjacent area features like parcels.	
35	The software should provide a complete set of drawing & editing tools in order to enable the user to Draw & Modify any or parts of various geographical objects (point, line and polygon) on the map.	
36	The software should have topology creation tool to remove the topological errors from vector data.	
37	The software should have the ability to add data from internet or intranet users to the existing map data so that data from other sources.	
38	The software should allow user to create layers or shortcuts to geographic data that store symbology for displaying features.	
39	A rich legend creation tool should be required in proposed application for thematic mapping. User should apply color and symbology using the attribute attached with the layer based on single, quantile and unique values functions.	
40	A rich annotation tool should be available such as add label, edit label, move label, rotate label, remove all label, etc.	
41	The software should have module of Dynamic Labelling and Rule based Labelling.	
42	The software should have a provision of hyper linking the GIS feature as well as its attribute fields with existing documents, URLs, Images, drawing files or scanned maps related to that feature.	
43	Software should have versioning capability for history tracking.	
44	Query builder tool should be available with the software to perform simple and complex queries.	
45	The customized application should provide the user facility to make dynamic queries on GIS GUI. The application should allow users to store and retrieve standard queries used by them in day to day operation.	
46	Software should have various query tools for queries based on attributes, location, etc.	
47	Software should have map composition / layout tool for printing spatial data at different scales and at adjustable print quality.	

48	Software should allow users to export results to various file formats like EMF, BMP, TIFF, JPEG, PDF, etc.	
49	Image Processing Functions	
50	The proposed software should support HRSI (High Resolution Satellite Imagery) and low resolution satellite images (panchromatic & multispectral) such as IKONOS, Quick bird, Geoeye, Worldview, CARTOSAT, EROS, LISS-IV, LISS-III, AWIFS, RISAT-1, KALPANA-1, INSAT3A, INSAT3D, PROVA-V, etc..	
51	The software should have capability to process optical satellite data as well as microwave image data.	
52	The software should be capable to process and visualize the stereo pair data. It should be able to create DEM from stereo pair and perform ortho-rectification.	
53	The software should support images with More than 8 bits, 11 bit, 16 bits, and 24 bits per band.	
54	The software should support image format such .tif, geotiff, .img, .pix, .hdr, .h4, .h5, DTED, DEM, CEOS, .bmp, .jpeg, etc.	
55	The software should be also support LiDAR data file format such as *.las, *.isd, *.pcg etc…	
56	The software should have projection transformation tool to reproject the image from one projection to other projection system.	
57	Image extraction module should be available in the proposed software which can be performed by defining the extent, inquire box and polygon layer.	
58	The software should have module for image mosaicing and splitting.	
59	Geometric Correction and atmospheric correct module should be available to remove the geometric distortion in the image and atmospheric anomalies such as haze.	
60	It should have Layer stacking to create composite image from a number of band of the satellite imageries.	
61	The software should have image enhancement module to enhance the imageries. It should have enhancement algorithm such as	
62	Linear, Logarithmic, Histogram Equalize, Histogram Matching, Density Slice, Gaussian, Squire root, Tone Balancing	
63	The software should have Image filtering algorithm such as	
64	Convolution, Texture, Adaptive, Crisp, Laplacian, Statistical, FFT, etc.	

65	The software should have image transformation module such Vegetation Index, Principal Component Analysis (PCA), Inverse PCA, Pan sharpening, Wavelet fusion, etc.	
66	The software should have Natural Color image generation module using NIR, Red and Green band of high resolution multispectral image data. This module should have capability to stretch the natural color image into 8 bit.	
67	Proposed software should have image classification modules such as supervised and unsupervised classification along with image segmentation.	
68	The software should be capable to process the temporal or time series image data. The software should provide change detection module such as: Basic Change Detection Advance Change Detection Auto Change Detection	
69	The advance change detection module should be capable to ingest multiple input images to find the change. It also handles the multi resolution satellite image along with mis-registration. It should supports various methods of advance change detection such as single band differencing, cross correlation, Image regression, Image ratio-ing, PCA, Change Vector Analysis (CVA), Magnitude Differencing, Vegetation Index Differencing, Tasseled Cap, Chi-Square, Unsupervised Change Detection, etc.	
70	The change detection module should have capability of Object Library Creation for Object Identification and Automatic Feature Extraction (AFE).	
71	The software should have functions like Linear Algebraic Combination, Change resolution, Bit Conversion, proximity analysis, etc.	
72	The software should have function called Dynamic threshold for analyzing change detection using image. This function is used to categorize the pixels in input image based on the threshold value.	
73	The software should have raster catalog and vector catalog tool for raster and vector data management.	
74	The software should have network analysis module to find the shortest and Optimum path using the topologically corrected road network.	
75	The software should have tools for terrain analysis and 3D analysis. The module should be able to create slope/aspect, hillshade, elevation profile, topographic normalize, line of sight, viewshed analysis.	
76	The software should have algorithm for surface generation such as Linear, IDW and Krigging.	

77	Software should support fully automatic and semi-automatic raster to vector conversion tools.	
78	OGC Certified	
79	User Management Tools Add User and Assign Rights	
80	Map Tools Vector and Raster Data Support (Display) Zoom In Zoom Out Zoom to Extent Previous Next ViewView Pan Zoom to box Book Mark Layer Visibility on/off	
81	Measure Tool Measure Distance Measure Area	
82	Advanced Tools Select Tool Unselect Identification Buffer Get XY coordinates Find XY coordinates Labelling	
83	Query Tools Basic Query Feature Query (Spatial and Non Spatial) Advance Query	
84	Spatial Editing Tools Feature Creation Add Feature Edit Feature Delete feature	
85	Non Spatial Editing Tools Attribute Information Editing	
86	Geo-processing	
87	Network Analysis	
88	Real Time Data Support and	
89	Online Spatial Data Creation and Updation Support	
90	Should support internet, intranet, cloud	
91	Multiuser data editing	
92	Data Analysis Look up Table Update	
93	Image Enhancement – Linear, Gaussian, Logarithmic, Density slice, Square Root, Histogram Equalize ,Histogram Matching	
94	Tone Balancing	
95	Image Filtering ,Texture ,Adaptive, Crisp, Statistical, Convolution	
96	Image Classification Unsupervised Classification	
97	Supervised Classification, Threshold , Generate Statistics of ROI/ Create Signature File, Post Classification Smoothing	
98	Contingency Matrix , Signature Reparability, PCT Edit	
99	Scatter Plot ,Class Information, Fuzzy Classification	
100	Fuzzy Convolution ,Segmentation	
101	Change Detection - Cut and Fill Analysis	

102	Conversion Tools	
103	It should have display, navigation, measurement, layer management, draw/edit and GPS functions.	
104	The mobile GIS/GPS application should be able to display the vector data with color and symbology.	
105	User should be able the ingest point, line, polygon and image theme in mobile GIS application.	
106	The application should have functions such as draw point/line/polygon features, attribute editing and delete point/line/polygon features.	
107	The GPS tool of the application should be able to collect point, line and polygon features.	
108	The application should have tools such as query builder, identify, find feature using attribute value, clear selection/refresh and find feature by location.	
109	The mobile application user interface should be customizable as per user requirement.	
110	Should have support for the smart phones and tablet devices with GPS Support. It should have support for	
111	Enterprise GIS Function	
112	The GIS server should be based on a Services Oriented Architecture (SOA).	
113	Should support Java /VB Script, .Net etc. and other latest technologies.	
114	OGC certification and capability to serve and consume OGC complied web services including WMS, WFS, WCS, CSW, INSPIRE, etc.	
115	Should be based on 64 bit architecture or better.	
116	Should support Windows/Linux platform.	
117	Should be able to support broad range of clients including Interoperability and browsers, desktops, Mobile Handsets.	
118	Should support unlimited number of Editing and viewing clients. It should also allow multiuser editing with Advanced Editing Functionalities.	
119	Should support standard Web server/application server like IIS, Apache, Tomcat, Oracle HTTP server, etc.	
120	Should supports unlimited Desktop client connection. Desktop GIS applications with the capability to consume WMS/ WFS services should be able to connect and use data from the server.	

121	Should be capable of maintaining data history, version management and conflict detection / resolution.	
122	Should have geo-processing framework, geo-processing core analysis functionalities, spatial and statistics analysis functionalities.	
123	Should have capability of centrally managed data, models, tools, maps and applications.	
124	Should have the capability to link documents like Adobe pdf, word/power-point JPEG, GIF, PNG, DTED and TIFF files etc to map features.	
125	Should support database check in–check out/replication functionalities hence maintaining the parent child relationship of Master Database.	
126	Should have open access to extensive GIS capabilities so as to enable organizations to publish and share geographic data(2D&3D),maps, analysis tools, Manipulate data, 3D models etc.	
127	The publisher should have capability to publish the project/data on GIS server and enable OGC services such as WMS, WFS, WCS and CSW in the data layer.	
128	All the Geo-processing and Image processing function such as buffer creation, clip, erase, image enhancement, image filtering, Vegetation Indices Calculation, Linear Algebraic Combination, Band Math, change detection, image extraction, mosaicing, etc should be performed at server end by sending the request using the web client and should enable the WMS service to display the processed data on web.	
129	Application Server must support Time aware data for Trends / Time Series Analysis. Application Server must support network and perform Routing analysis, Service Area Analysis, and Tracking Analysis.	
130	Should support for GML, RSS (Real Simple Syndication) and KML/KMZ (Keyhole Markup Language).	
131	The server should have in built map caching capability.	
132	It should provide imagery access quickly after acquisition with dynamic mosaicing and on- the-fly processing.	
133	Should support standard Web server/application server	
134	Should have Web Application Functionalities like pan, zoom, identifying features on a map, feature based hyperlink, measure distance, overview window, find place, query attribute, search attribute, editing and geo processing task.	
135	The software should allow visualization of data in 2D, 3D in web as well as desktop application.	

136	Control user access and credentials to data by assigning roles.	
137	Logging records all transactions including log-ins, searches, downloads, uploads, edits, and deletions.	
138	Should support Single sign-on, authentication module.	
139	Should support SSL and signed certificates to ensure complete security from browser to server.	
140	Should enable a secure, private sharing of confidential data that can be deployed on private network to promote collaboration on maps and applications within the organization.	
141	Should provide a web publishing wizard so that registered users can publish websites without coding/programming.	
142	Should be able to create and manage groups to control publishing the data and its services on Data store/workspaces.	

Design and Development of Enterprise Web GIS Portal

Bidder will Design and Develop web GIS application using COTS Base Enterprise GIS platform. This application will cater to the viewing, analysing, & utilizing the Geographic Information needs for Smart City Command Control System

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

- Will be based on COTS Base Enterprise GIS Platform
- OGC Open Geospatial data standards compliant
- Existing Server, Client, Web, Mobile / Tablets to be supported
- Application will be open to integrate additional functionalities in future
- Visualization of data e.g. Land Parcel Data DEM on Satellite Image
- will support multiple relational database connections
- Shall have query based results
- Application will have facility of Historical data analysis for Land parcel information, property tax information, building information using time series
- Will support distributed transaction. This allows multiple users to edit the map data at a same time
- Application will support DBMS spatial index and R- tree index for better system performance
- Creation of server clusters with load balancing and fail-over functionality will be supported
- Application will support data compression and asynchronous map view, static& dynamic cache.
- Application will have facility to configure additional menus for future functionality
- User authorization and authentication should be GUI based
- Application will have the facility to monitor application operations and status: Logged in user status, server load, data access status

- Application will have the facility to create custom GUI without business customization through designated application the selected bidder is expected to follow the complete SDLC for the development of the GIS application.
- Proposed/Developed GIS Application software will follow National Spatial Data Infrastructure (NSDI) Meta standards and should be compatible with National Urban Information System (NUIS) Scheme. Tightly integrate the spatial data with the existing system at Smart City.

4.18 City WiFi

Seamless WiFi connectivity is required throughput the Dehradun Municipal area to run the Dehradun one Application.

1. Solution & Architecture Overview

1.1	The wireless LAN solution shall be based on IEEE 802.11 and shall be WFA certified for Data and Voice.	**Compliance/Page Number**
1.2	The wireless LAN solution shall propose a distributed control function (no centralized controller) with inherent support for redundancy, elimination of traffic bottlenecks and lowered latency.	
1.3	The wireless LAN solution shall rely on a distributed and L2 only data plane.	
1.4	The wireless LAN solution shall be able to be deployed in mono-site deployment with Access Points spread over a single broadcast domain (VLAN) and operating in a common RF environment and multi-site deployment with Access Points spread over multiple broadcast domains (VLAN) that may operate in different RF environment. For both deployment types, the solution shall offer advanced features like Intrusion Detection/Prevention or a Captive Portal to manage guest's connection without additional third-party components.	
1.5	The wireless LAN solution shall propose a centralized management function, irrespective of the deployment model.	
1.6	The wireless LAN solution shall scale atleast minimum 4000 Access Points and thousands of users while guarantee ease of deployment and expansion (to be described).	
1.7	The deployment model shall rely on a licensing model that is as simple as possible, with one license per AP including all functions (basic or advanced) handled by the AP.	
1.9	The mono site deployment shall allow an easy migration to multisite deployment (Minimum 4000 AP) when needed.	
1.10	The wireless LAN solution shall have been designed with scalability in mind to allow the additional, minimum 2000 APs limit to be extended in the future (to be described) without requiring new equipment or deployment design change.	

2. Access Control, Authentication and Encryption

2.1	The wireless LAN solution shall support MAC based authentication.	
2.2	The wireless LAN solution shall support 802.1x based authentication.	
2.3	The WLAN solution shall include a built-in RADIUS server for 802.1x and MAC authentication that shall not be proposed as a separate product.	
2.4	The built-in RADIUS server shall be able to interface with an external authentication server (Radius, LDAP, Active Directory): Free Radius, Microsoft NPS Radius Server, Microsoft AD, Open LDAP…	
2.5	The built-in RADIUS server shall support at least following EAP types: EAP-PEAP, EAP-GTC, EAP-TLS, EAP-TTLS.	
2.6	The wireless LAN solution shall have the ability to utilize RADIUS attributes to assign each authenticated user/device to a specific ROLE. A role defines a VLAN and enforces security and QoS through the use of role-based ACLs and QoS policies that can be directly integrated with the roles defined within existing authentication servers.	
2.7	The wireless LAN solution shall support following link layer encryption standards: WPA2_AES, WPA2_TKIP, WPA_AES, WPA_TKIP, DYNAMIC_WEP, WPA_PSK_AES, WPA_PSK_TKIP, WPA_PSK_AES_TKIP, WPA2_PSK_AES, WPA2_PSK_TKIP.	
2.8	The wireless LAN solution shall support following 802.1x supplicants: Windows 7, 10, MAC OS, IOS, Android, Chromebook…	
2.9	Irrespective of the deployment model, the wireless LAN solution shall propose a “Guest” management solution based on an embedded and built-in Captive Portal providing web based authentication for guests and visitors.	
2.10	The Guests Captive Portal included in the wireless LAN solution shall allow a customizable look & feel.	
2.11	The Guest management solution shall allow, at least, following authentication methods: Username & Password Access Code Simple Term & Condition acceptance	
2.12	The Guest management solution shall allow non-IT staff (e.g., a receptionist) to create temporary guest accounts.	
2.13	For a multisite deployment scenario, the WLAN solution shall allow guest self-registration and employee sponsored access.	
2.14	The licensing model of the Guest management solution shall be based on the number of devices.	
2.15	The Guest management solution shall allow setting a validity period for an authenticated device, in order to avoid entering credentials each time a guest access the network.	
2.16	The WLAN solution shall implement strict guests traffic isolation.	

2.17	The WLAN solution shall support BYOD and be able to provide device onboarding that is as simple as possible and without requiring additional third party components.	
2.18	The on-boarding process of employee devices shall be based on employee corporate accounts.	
2.19	The BYOD application shall allow setting the validity period for the device, and the maximum number of devices per account.	
2.20	The licensing model of the BYOD application shall be based on the number of on-boarded devices.	

3. RF Management

3.1	The WLAN solution shall allow automatic and/or manual RF management (channel and power).	
3.2	The WLAN solution shall support Short Guard Interval.	
3.3	The WLAN solution shall be smart enough to guide a new client to the optimal band/channel (2.4GHz/5GHz) considering, at a given time, both the number of associated clients on each band, and the medium utilization.	
3.4	If no band/channel (2.4GHz/5GHz) is overloaded (high medium utilization) or crowded (high client count), an AP shall by default guide a new client to the 5GHz band.	
3.5	Even if the 5GHz band is not overloaded but is crowded (high client count), an AP shall guide a new client to the 2.4GHz band.	
3.6	If a band/channel (2.4GHz/5GHz) is overloaded (high medium utilization) and even if it is not crowded, an AP shall guide a new client to the less loaded band/channel.	
3.7	If all bands/channels (2.4GHz/5GHz) are overloaded (high medium utilization) and no band/channel is crowded, an AP shall guide a new client to the 5GHz band.	
3.8	If all bands/channels (2.4GHz/5GHz) are overloaded (high medium utilization) and the 5GHz is crowded, an AP shall guide a new client to the 2.4GHz band.	
3.9	When a new client discovers multiple APs to associate to, the new client shall be guided to the AP that has the fewest associated clients, thus allowing smart/dynamic load balancing.	
3.10	The WLAN solution shall deny connection to an AP when the signal of the client becomes too weak and disconnect a client when the signal becomes too weak.	
3.11	The WLAN solution shall propose APs that have the ability to scan the air in order to provide interfering/rogue APs and wireless attacks detection, and shall not rely on dedicated scanning equipment.	
3.12	The scanning function of the APs shall not impact active voice or video calls (SIP and H.323).	

4. Intrusion Detection and Prevention

4.1	The WLAN solution have WIDS/WIPS capabilities with no additional and dedicated equipment nor additional license.	
4.2	The WLAN solution shall be able to identify Interfering APs.	
4.3	The WLAN solution shall be able to identify and contain Rogue APs.	
4.4	The WLAN solution shall allow the definition of flexible policies to classify an AP as a Rogue AP.	
4.5	The WLAN solution shall allow the definition of flexible AP attacks detection policies.	
4.6	The WLAN solution shall allow the definition of flexible client attacks detection policies.	
4.7	The WLAN solution shall be able to blacklist a WLAN client, either manually or automatically after a client attack has been detected.	
4.8	The WLAN solution shall allow to configure a blacklist duration.	
4.9	The WLAN solution shall allow to configure an authentication failure times threshold.	

5. Quality of Service

5.1	The WLAN solution shall offer WLAN Access Points that shall support fine-tuned Quality of Service (QoS) allowing following actions based on the identity of the connecting user: ACL based (source/destination IP address and TCP/UDP ports) permit/deny decision QoS priority marking and queuing	
5.2	The wireless LAN solution shall comply with the 802.11e WMM standard and shall allow for custom QoS tag (802.1p/DSCP) to WMM queue mapping.	
5.3	The WLAN solution shall have traffic *Deep Packet Inspection* (DPI) capabilities allowing an administrator to take control of applications (even if they all run on top of the HTTP or HTTPs protocols), including not only blocking applications, but also allowing to prioritize and rate-limit applications.	
5.4	The wireless LAN solution shall be able to define and guarantee bandwidth based on the SSID. It shall also be to define and guarantee bandwidth based on the user/device role.	
5.5	The WLAN solution shall allow to set the maximum number of clients per band/radio and per AP for a specific SSID.	

5.6	The wireless LAN solution shall propose broadcast traffic optimization mechanisms (including Broadcast filtering and Broadcast/Multicast Key rotation).	
5.7	Leveraging its IGMP snooping capabilities, the wireless LAN solution shall be able to optimize multicast traffic by converting multicast traffic to unicast traffic.	
5.8	For a multisite deployment scenario, Multicast optimization shall stop on high load.	
5.9	The wireless LAN solution shall propose the WMM *Automatic Power Save delivery* (APSD) feature to allow clients conserve battery life.	
5.10	The wireless LAN solution shall by default identify Voice and Video (SIP and H323) calls and provide appropriate treatment.	

6. Mobility

6.1	The WLAN solution shall support Layer 2 roaming capabilities across APs with no special client-side software required.	
6.2	The WLAN solution shall support Layer 3 roaming across APs with no special client side software required.	
6.3	The WLAN solution shall support both *Opportunistic Key Caching* (802.11k).	
6.4	The WLAN solution shall comply to the 802.11r standard.	

7. Management

7.1	The wireless LAN solution shall propose a centralized management function based on an embedded and secure WEB GUI, irrespective of the deployment model.	
7.2	The proposed solution should be premise based and not cloud based	
7.3	If the centralized management function requires the deployment of a dedicated application, this one shall be in the form of a Virtual Appliance that can be installed on top of any of following hypervisors: VMware ESXi, Microsoft HyperV and Oracle VirtualBox.	
7.4	Centralized management function shall be able to handle wired equipment (switches) management for a “unified management” approach.	
7.5	The WLAN solution shall be able to automatically discover new APs added to the network.	
7.6	WLAN solution shall be able to blacklist a WLAN client, either manually or automatically after a client attack has been detected.	
7.7	The centralized management function shall allow to display the physical topology of the network.	

7.8	The centralized management function shall allow per equipment configuration and software backup and restore, and bulk backup and restore.	
7.9	The centralized management function shall allow access to all wIPS/wIDS features.	
7.10	The centralized management function shall offer, on the basis of an application signature file, insight at application layer (e.g. *facebook.com*, *youtube.com*, *salesforce.com*…) even if the applications run on top of the HTTP or HTTPs protocols. It shall also allow control of those applications.	
7.11	The centralized management function shall allow to display the Wi-Fi coverage quality within a given area (“Heat Map”).	
7.12	The centralized management function shall allow, before deployment, to determine optimal placement of Access Points (APs) in a location (RF Planning).	
7.13	The centralized management function shall be collocated with the Guest and BYOD management applications.	

8. Access Points Specific Requirements

8.1	The WLAN solution shall propose a 802.11ac wave2 MU-MIMO outdoor ruggedized dual-radio AP Access Point.	
8.2	The outdoor ruggedized Access Point shall have integrated omni-directional antennas or may be equipped with external antennas.	
8.3	The outdoor ruggedized Access Point shall support atleast 16 SSIDs (8 per radio).	
8.4	The outdoor ruggedized Access Point shall offer atleast 1733Mbps throughput on the 5Ghz band and atleast 400Mbps throughput on the 2.4GHz band.	
8.5	The outdoor ruggedized Access Point shall support atleast 512 clients.	
8.6	The outdoor ruggedized Access Point shall have two (2) 1Gb Ethernet port.	
8.7	Roaming Parameters supported shall be L2 Roaming Fast BSS Transition (802.11r Roaming) Radio Resource Management (802.11k) BSS Transition Management (802.11v)	
8.8	The outdoor ruggedized Access Point shall propose *Deep Packet Inspection* (DPI) capabilities providing real-time classification of flows at the application level.	
8.9	The outdoor ruggedized Access Point shall be IP66/67 certified.	
8.10	The outdoor ruggedized Access Point shall support persistent moisture and precipitation, and high and low temperatures: -40°C to 65°C	
8.11	The outdoor ruggedized Access Point shall support 802.3af/at PoE with 40W maximum consumption.	
8.12	The MTBF for the outdoor ruggedized Access Point shall be at least 525600h (60 Years).	

8.13	The outdoor ruggedized Access Point shall propose a Factory reset button.	
8.14	The outdoor ruggedized Access Point shall propose a console port.	
8.15	Operating temperature must be -40°C to 65°C (-40°F to +149°F) "Chassis rating: IP67; Wind resistance: atleast 100 MPH sustained winds / at 165 MPH wind gusts" Humidity must be 10% to 90% non-condensing. CE & RoHS, REACH, WEEE, CB Scheme Safety, NRTL FCC and IC approval and certificates, EN 60601-1-2 EMC requirements for the Medical Directive 93/42/EEC Wi-Fi Alliance (WFA) certified 802.11a/b/g/n/ac	

4.19 Non-IT Requirements, Specifications & Office Interior Spaces

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

General Standards:

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

• Development of ergonomic reports for the DICCC covering Human Factors Engineering (HFE), ISO9241 (Ergonomic requirements for office work with visual display terminals - VDTs) and ISO11064 (Ergonomic Design of Control Centres)

• The proposed interior material should meet to basic control room norms, including but not limited to:

- ASTM E84 or equivalent fire norms,
- High scratch resistant surfaces,
- Seismic zone compliance, and Green Guard passed Desk for ensuring safe environment for operators.

Civil and Architectural Work

False Ceiling:

Metal false ceiling with powder coated 0.5mm thick hot dipped galvanised steel tiles 595 x 595 mm with regular edge (10mm) suitable for 25mm grid supported on suitable powder coated galvanised steel grid as per manufacturer specification. The same shall be inclusive of cut outs for lighting, AC grills, Fire detectors, nozzles, etc.

Minimum 12 mm thick fire line Gypsum false ceiling and lighting troughs 300 mm as per design including 100 mm high cornices as lighting pelmets on G.I. frame work, in G.I. vertical supports at every 450mm c/c and horizontal runners at every 900mm c/c self-taping metal screws to proper line and level. The same shall be inclusive of making holes and required framing for fixing electrical fixtures, A.C. grills etc. GI vertical supports to be anchored to slab by means of anchor fasteners.

Furniture and Fixture:

Workstation size of min. 18” depth made with 1.5mm thick laminate of standard make over 18mm thick commercial board complete with wooden beading including cutting holes & fixing of cable manager etc. complete with polish. Edges shall be factory post-formed. The desk shall have the necessary drawers, keyboard trays, cabinets etc. along with sliding / opening as per approved design with quality drawer slides, hinges, locks etc. All workstations, cabins should be as per industry best practices and standards.

Providing & making of storage unit with 18 mm thick MDF board along with 1.5 mm approved laminate colour outside and 2 coat of enamel paint inside the storage of size 1'6"x1'6"x2'4". The same should be provided with all the required accessories including the handle, lock, sliding channel and necessary hardware, etc. complete with polish

An enclosure for gas cylinder of Shutters and Partitions along with wooden support and 18 mm thick MDF board along with 1.5 mm approved laminate colour outside and 2 coat of enamel paint inside the shutter. The same should be provided with all the required accessories including the handle, lock, loaded hinges, tower bolt and necessary hardware etc. complete with French polish.

Partitions (wherever required as per approved drawing)

Full height partition wall of 125 mm thick fire line gyp-board partition using 12.5 mm thick double fire line gyp-board on both sides with GI steel metal vertical stud frame of size min. 75 mm fixed in the floor and ceiling channels of 75 mm wide to provide a strong partition. Glass wool insulation inside shall be provided as required. Fixing is by self-tapping screw with vertical studs being at 610 mm intervals. The same should be inclusive of making cut-outs for switch board, sockets, grill etc. It shall also include preparing the surface smoothly and all as per manufacture’s specification etc. finally finishing with one coat of approved brand of fire resistant coating. Glazing including the framework of 4" x 2" powder coated aluminium section complete (in areas like partition between server room & other auxiliary areas).

Fire Rated Wire Glass minimum 6 mm thick for all glazing in the partition wall complete. (External windows not included in this). All doors should be minimum 1200 mm (4 ft.) wide.

Flooring (wherever required as per approved drawing)

MSI shall procure and install a raised floor to match the floor height and room aesthetic in accordance with the approved final layout and design. MSI shall consider standard parameters for developing the final height, width, point of load, and uniform distribution load of the raised floor for the rooms based on type of furniture and overall load.

MSI shall ensure the following features and parameters areconsidered while designing and commissioning the raised floor:

1. Point of Load (PoL) shall be considered 20% more than the actual load
2. Uniform Distribution Load shall be calculated according to the final Point of Load
3. Noise-proof, Fireproof
4. Maintenance window for easy access to under the raised floor
5. Separate electrical and data cable tray under the raised floor
6. Face of floor tiles shall conform to the aesthetic part of the approved design

7. MSI shall perform load test and noise test of the constructed raised floor.

The MSI shall complete the following requirements for the raised flooring panels:

- Floor shall be designed for standard load conforming to BIS 875-1987.
- Panels shall be made up of 18-gauge steel of 600 mm × 600 mm size treated for corrosion and coated with epoxy conductive paint (minimum thickness 50 Micron).
- Raised flooring covering shall be antistatic, high- pressure laminate, two (2) mm thick in approved shade and color with PVC trim edge. It shall not make any noise while walking on it or moving equipment. Load and stress tests on floor panels shall be performed as part of acceptance testing.

Air Conditioning and Natural Convection

For Data Centre -

Precision remote control and manual operated air conditioning system shall be exclusively installed to maintain the required temperature in the data center server farm area. The A/C shall be capable of providing sensible cooling capacities at ambient temperature and humidity with adequate air flow. Air conditioner shall be linked to secondary power supply as well to prevent them from shutting down in case of power outage

Painting

Provide and apply Fire retardant paint of pre-approved make and shade to give an even shade over a primer coat as per manufacturers' recommendations after applying painting putty to level and plumb and finishing with 2 coats of fire retardant paint. Base coating shall be as per manufacturer's recommendation for coverage of paint, For all vertical Plain surface and fire line gyp-board ceiling.

Use approved fire retardant coating on all vertical surfaces, furniture etc. as per manufacturer's specification.

PVC conduit:

The conduits for all systems shall be high impact rigid PVC heavy-duty type and shall comply with I.E.E regulations for non- metallic conduit 1.6 mm thick as per IS 9537/1983. All sections of conduit and relevant boxes shall be properly cleaned and glued using appropriate epoxy resin glue and the proper connecting pieces, like conduit fittings such as Mild Steel and should be so installed that they can remain accessible for existing cable or the installing of the additional cables.

No conduit less than 20mm external diameter shall be used. Conduit runs shall be so arranged that the cables connected to separate main circuits shall be enclosed in separate conduits, and that all lead and return wire of each circuit shall be run to the same circuit.

All conduits shall be smooth in bore, true in size and all ends where conduits are cut shall be carefully made true and all sharp edges trimmed. All joints between lengths of conduit or between conduit and fittings boxes shall be pushed firmly together and glued properly.

Wiring

PVC insulated copper conductor cable shall be used for sub circuit runs from the distribution boards to the points and shall be pulled into conduits. Looping system of wring shall be used, wires shall not be jointed. No reduction of strands is permitted at terminations.

Wherever wiring is run through trunking or raceways, the wires emerging from individual distributions shall be bunched together with cable straps at required regular intervals. Identification ferrules indication the circuit and D.B. number shall be where required

Where, single phase circuits are supplied from a three phase and a neutral distribution board, no conduit shall contain wiring fed from more than one phase in any one room in the premises, where all or part of the electrical load consists of lights, fans and/or other single phase current consuming devices, all shall be connected to the same phase of the supply.

Circuits fed from distinct sources of supply or from different distribution boards or M.C.B.s shall not be bunched in one conduit. In large areas and other situations where the load is divided between two or three phases, no two single-phase switches connected to difference phase shall be mounted within two meters of each other.

All splicing shall be done by means of terminal blocks or connectors and no twisting connection between conductors shall be allowed. Metal clad sockets shall be of die cast non-corroding zinc alloy and deeply recessed contact tubes. Visible scraping type earth terminal shall be provided. Socket shall have push on protective cap.

Balancing of circuits in three phases installed shall be arranged before installation is taken up. Unless otherwise specified not more than ten light points shall be grouped on one circuit and the load per circuit shall not exceed 1000 watts.

Cable Work

Cable ducts should be of such dimension that the cables laid in it do not touch one another. If found necessary the cable shall be fixed with clamps on the walls of the duct. Cables shall be laid on the walls/on the trays as required using suitable clamping/ fixing arrangement as required. Cables shall be neatly arranged on the trays in such manner that a criss-crossing is avoided and final take off to switch gear is easily facilitated. Cable shall be laid as per the IS standard

All cables will be identified close to their termination point by cable number as per circuit schedule. Cable numbers should be properly punched. For trip circuit identification additional red ferrules are to be used only in the switch gear / control panels, cables shall be supported so as to prevent appreciable sagging. In general distance between supports shall not be greater than 600mm for horizontal run and 750mm for vertical run.

Each section of the rising mains shall be provided with suitable wall straps so that same the can be mounted on the wall.

Whenever the rising mains pass through the floor they shall be provided with a built-in fire proof barrier so that this barrier restricts the spread of fire through the rising mains from one section to the other adjacent section.

Neoprene rubber gaskets shall be provided between the covers

and channel to satisfy the operating conditions imposed by temperature weathering, durability etc.

Necessary earthling arrangement shall be made alongside the rising mains enclosure by Mean of a GI strip of adequate size bolted to each section and shall be earthed at both ends. The rising mains enclosure shall be bolted type.

The space between data and power cabling should be as per standards and there should not be any criss-cross wiring of the two, in order to avoid any interference, or corruption of data.

Fire Detection and Control Mechanism

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

- Should proactively alert incase there is a possibility of a electrical fire (short circuit or over current)
- The system should have the capability to integrate with different makes of fire alarm systems in the DCs and provide the alarms generated by the system on the centralized Dashboard.
- The system should be able to plan and process a proper evacuation plan incase of fire
- Trigger Audio and Visual alarm
- Co-relate with the nearest camera in the site with the zone of the FAS.
- Switching ON of lights on the evacuation pathway.

Rodent Repellent System

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

Access Control System

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

#	**Description**
1.	Controlled Entries to defined access points
2.	Controlled exits from defined access points

3.	Controlled entries and exits for visitors
4.	Configurable system for user defined access policy for each access point
5.	Record, report and archive each and every activity (permission granted and / or rejected) for each access point.
6.	User defined reporting and log formats
7.	Fail safe operation in case of no-power condition and abnormal condition such as fire, theft, intrusion, loss of access control, etc.
8.	Day, Date, Time and duration based access rights should be user configurable for each access point and for each user.
	One user can have different policy / access rights for different access points.

DG Set

Sl no	Parameter	Minimum Specifications
1.	General	Auto Starting DG Set Mounted on a common based frame with AVM (Anti-Vibration) pads, residential silencer with exhaust piping, complete conforming to ISO 8528 specifications and CPCB certified for emissions. KVA rating as per the requirement.
2.	Capacity	250 KVA
3.	Fuel	High Speed Diesel (HSD) With 30 Ltr. Tank Capacity or better. It should be sufficient and suitable for containing fuel for 12 hours continuous operation, Complete with level indicator, fuel inlet and outlet, air vent, drain plug, inlet arrangement for direct filling and set of fuel hoses for inlet and return.
4.	Power Factor	0.8
5.	Engine	Engine should support electric auto start, water cooled, multi cylinder, maximum 1500 rpm with electronic/manual governor and electrical starting arrangement complete with battery, 4 stroke multiple cylinders/single and diesel operated conforming to BS 5514/ ISO 3046/ IS 10002
6.	Alternator	Self-exciting, self-regulating type alternator rated at 0.8 PF or better, 415 Volts, 3 Phase, 4 wires, 50 cycles/sec, 1500 RPM, conforming to IS 4722/ BS 5000, Windings of 100% Copper, class H insulation, Protection as per IP 23.
7.	AMF (Auto Main Failure) Panel	AMF Panel fitted inside the enclosure, with the following meters/indicators: ▪ Incoming and outgoing voltage ▪ Current in all phases ▪ Frequency ▪ KVA and power factor ▪ Time indication for hours/ minutes of operation ▪ Fuel Level in field tank, low fuel indication ▪ Emergency Stop button ▪ Auto/Manual/Test selector switch ▪ MCCB/Circuit breaker for short-circuit and overload protection ▪ Control Fuses

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

4.20 ICT Software Components for Data Center:

4.20.1 Enterprise Database

Sl no	Description
1.	Database License should be un-restricted and perpetual, to prevent any noncompliance in an event of customization & integration.
2.	Databases shall support multi-hardware platform.
3.	RDBMS should support Unicode with Indian Language support
4.	RDBMS should have spatial capability and should be capable of storing vector (2D, 3D), raster data as well as the metadata.
5.	Database shall provide standard SQL Tool for accessing the database. The tool should be able to monitor, maintain and manage the database instance, objects, and packages.
6.	Database shall have built-in backup and recovery tool, which can support the online backup.
7.	RDBMS should support of seamless data transformation from on premise to public cloud and from public cloud to on premise.
8.	Database shall be able to provide database level storage management mechanism, which should enable the availability by means of creating redundancy, automatically balance the data files across the available disks, i/o balancing across the available disks for the database for performance, availability and management.
9.	Database shall support for central storage of data with multiple instances of database in a clustered environment access the single /multiple database.
10.	Database shall be able to provide database level storage management mechanism, which should enable the availability by means of creating redundancy, automatically balance the data files across the available disks, i/o balancing across the available disks for the database for performance, availability and management.

Sl no	Description
11.	Should be an enterprise class database with the ability to support connection pooling, load sharing and load balancing when the load on the application increases
12.	Database shall have built-in DR solution to replicate the changes happening in the database across DR site with an option to run real time or near real-time reports from the DR site without stopping the recovery mechanism.
13.	Ability to recover the node on fly or with limited timelines with-out Unloading/ reloading data.
14.	RDBMS should provide continuous availability features to address hardware failures, instance failures, human errors like accidental deletion of data, tables etc.
15.	Database shall provide native functionality to store and retrieve XML, Images and Text data types.
16.	Database shall provide native functionality to store XML, within the database and support search, query functionalities.
17.	RDBMS should support spatial data types.
18.	Database shall have Active-Passive or Active-Active failover clustering with objectives of scalability and high availability.
19.	Database shall provide control data access down to the row-level so that multiple users with varying access privileges can share the data within the same physical database.
20.	Database shall be having built-in provision to Administer database / database clusters, Monitor performance, Maintain database, Backup and recovery, Recovery management, Disaster recovery management.
21.	Database shall be having native auditing capabilities for the database.
22.	Database shall be having built-in provision to Administer database / database clusters, Monitor performance, Maintain database, Backup and recovery, Recovery management, Disaster recovery management.
23.	Availability of recovery/restart facilities of the DBMS.
24.	Automated recovery/restart features provided that do not require programmer involvement or system reruns.
25.	Program restart should be provided from the point of failure.
26.	RDMS should have the ability to manage recovery/restart facilities to reduce system overhead.
27.	Provides extra utilities to back up the databases by faster means than record by record retrieval.
28.	The database should provide controls over who, when, where and how applications, data and databases can be accessed.
29.	RDBMS should be possible to prevent privileged IT users such as DBAs and administrators from accessing and modifying the data.
30.	The database should provide multi-factor authentication based controls and policies preferably taking account of application context etc.
31.	Should provide adequate auditing trail facility. Audit trail should also be maintained at database level for any changes made in database and it should be ensured that these audit trails cannot be manipulated by anyone including super users and DBAs.
32.	System should record the date and time stamp for all records generation/modification.

Sl no	Description
33.	Solution should offer spatial analytic functions for data mining applications, such as binning, spatial correlation, co-location mining, spatial clustering, and location prospecting

4.20.2 Enterprise Backup Software

Sl no	Description
1.	The proposed Backup Solution should be available on various OS platforms such as Windows, Linux etc. and be capable of supporting SAN based backup / restore from various platforms including Linux, Windows etc.
2.	The solution should offer centralized, web-based administration with a single view of all back up servers
3.	The proposed backup solution should allow creating tape clone facility after the backup process.
4.	Scheduled unattended backup using policy-based management for all Server and OS platforms
5.	The proposed Backup Solution has in-built frequency and calendar based scheduling system.
6.	The software should support on-line backup and restore of various applications and Databases
7.	The backup software should be capable of having multiple back-up sessions simultaneously
8.	The proposed backup solution should be capable of taking back up of SAN environment as well as LAN based backup.
9.	The backup software should support different types of backup such as Full back up, Incremental back up, Differential back up, Selective back up, Point in Time back up and Progressive Incremental back up and snapshots
10.	The backup software should support different types of user interface such as GUI, Web- based interface
11.	The proposed Backup Solution has in-built media management and supports cross platform Device & Media sharing in SAN environment.
12.	Backup Software is able to rebuild the Backup Database/Catalogue from tapes in the event of catalogue loss/corruption.
13.	The proposed Backup Solution has online backup solution for different type of Databases such as Oracle, MS SQL, MySQL and Sybase / DB2 etc. on various OS.
14.	Backup Solution shall be able to copy data across firewall.
15.	The backup software must also be capable of reorganizing the data onto tapes within the library by migrating data from one set of tapes into another, so that the space available is utilized to the maximum. The software must be capable of setting this utilization threshold for tapes

Sl no	Description
16.	The backup software should be able to support versioning and should be applicable to individual backed up objects.

4.20.3 Directory Services

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

4.21 Network Backbone and Internet Connectivity

4.21.1 Overview

Pan city network backbone and internet connectivity is an important components of the project and needs very careful attention in assessment, planning and implementation. It is important not only to ensure that the required connectivity is reliable, secure and supports the required SLA parameters of Latency, Jitter, Packet Loss and Performance. City wide network is essentially intended to provide a high-speed network connectivity for supporting all existing and future smart solutions. The project objectives broadly are as follows:

- To provide inexpensive and pervasive connectivity all across the city
- To boost digital inclusion among departments and citizens
- To provide 24*7 uninterrupted connectivity across the city
- To establish a medium for quick data gathering from multiple sources and faster decision making
- To act as a channel for integration of all the city services
- To enable the government to have advanced communication products/platforms and better security and surveillance systems

The proposed smart city solution will involve city wide network coverage across various locations in DSCL. Dehradun smart city will offer various smart services to its citizens. To provide these services in an uninterrupted and effective manner a robust network is required to be deployed. Network needs to be planned to meet the all the network requirements for currently services envisaged, scalability and future requirement. DSCL intends to provide connectivity under at locations like; municipal offices, Bus depots, traffic junctions, parks, fire establishments, police stations, urban health centers, schools etc. MSI would be required to create a single network i.e. city wide network for the smooth functioning of all solutions. Successful bidder is required to integrate city wide network with Data center (DC), Disaster recovery (DR) and Command Control & Communication Center (DICCC).

DSCL intends to procure Leased Circuits & Internet Bandwidth for the city wide network under the Dehradun smart city Project. The successful bidder is required to terminate the desired Leased circuits and Internet Bandwidth at the locations specified.

A Service Level Agreement will be signed with the successful bidder. As bidder, will be responsible for smooth functioning of the entire network connectivity, availability of sufficient quantities of all the critical components will be taken care of by the bidder to maintain the guaranteed uptime. Bidders are requested to take into consideration the equipment's required at each location for providing connectivity while quoting for the tender.

Full Duplex Bandwidth as Per Schedule of Requirement has to be provisioned and implemented by the Service Provider. Service Provider has to keep provision of giving burstable Bandwidth & the rates will be as per finalized rates. Service Provider has to arrange fiber & other last mile equipment accordingly including media convertors wherever required.

4.21.2 Scope of work

The detailed scope of work for MSI for providing of pan city network backbone is given below:

Bandwidth Provisioning

MSI shall implement the solution in and provision the network bandwidth as per details given below. MSI shall be responsible for upgrading its infrastructure, including the last mile, to meet the requirements of the DSCL, at no additional cost to the DSCL. The network & bandwidth should meet following requirements:

- DSCL may order an increase/decrease/termination/withdrawal in bandwidth, which bidder shall take into account.
- The network should be capable of providing Bandwidth on Demand for planned as well as for unplanned activities.
- MSI should provide the bandwidth for intranet & internet.

Internet Bandwidth at DICCC, Data Center and all field locations

DSCL is procuring bulk internet bandwidth for the requirement of various locations throughout the city. MSI is required to terminate these links at the desired locations defined as per the price bid format of this RFP.

Redundancy

- As a measure of redundancy remote locations, DICCC, DC & between DC & DR site connected through Leased Circuits should have redundancy in place to meet necessary SLA requirements.
- Location-wise Bandwidth requirements is given in Annexure A & B.

Rate Contract

- DSCL is procuring leased circuits to be delivered at various locations spread across the Dehradun city.
- Looking at the scalability and future requirement discovery of prices shall be valid for the period contract duration under the Rate Contract as per price bid.
- It has been observed that there is a considerable price reduction in cost of Domestic and Internet bandwidth during last few years. Hence, DSCL will review the prices at end of every year and MSI is required to match the prevailing market prices as per TRAI regulations.
- Adding new location – whenever a new location is decided to be added by the DSCL, an order will be placed with MSI at the contracted price. MSI shall carry out site-survey at new location for feasibility of location over wired connectivity. MSI would be required to implement and commission the location within 2 weeks from the date of work order.

Technical Specifications

a. Leased circuit:

- The bandwidth must be provisioned on Optical Fiber Media. No other last mile media type is acceptable.
- Latency from point A to point B should not exceed 20 ms.
- The bandwidth supplied should be symmetric, dedicated 1:1 with 100% throughput.
- Up time guarantee must be 99.5 %
- MSI must deliver this bandwidth on a fiber optic cable network at the respective locations.
- All costs to connect the links to last mile node of SCADL has to be borne by MSI. DSCL will not pay or reimburse any last mile of extra work cost.
- MSI has to use the IP addressing schema provided by the SCADL.

b. Internet Bandwidth

- The bandwidth must be provisioned on Optic Fiber media only. No other last mile media type is acceptable.
- DSCL is procuring bulk internet bandwidth (as per the Price bid) for the requirement of various locations throughout the city. However, successful MSI is required to terminate these links at the desired locations.
- Latency to Google, Yahoo and NIXI peering should not exceed 200 ms.
- The bandwidth should be dedicated 1:1 with 100% throughput.
- Up time guarantee must be 99.7%
- Provider must have minimum two sources of Internet Gateway bandwidth input.
- MSI must deliver this bandwidth on Gigabit Ethernet optically or electrically which will be taken as input.
- MSI must deliver the required bandwidth on a fiber optic cable network at the desired locations.
- All costs to connect the link to the last mile node has to be borne by MSI. DSCL will not pay or reimburse any last mile of extra work cost.

Following Minimum bandwidth requirement to be provisioned at the locations indicative number of locations are following.

Sl No	Bandwidth Requirement	Indicative Quantity	Connectivity/Bandwidth
1	DC	2	MPLS/800Mbps
2	DC to DR	1	MPLS/400Mbps
3	End Location	50	MPLS/2Mbps
4	DC Internet	2	Internet/200Mbps

4.22 Web Portal and Mobile Application

Overview

At the core of the stakeholder's service experience will be citizen portal of DSCL which will be a gateway to citizens, tourists and businesses for disseminating information and engagement. It will be accessed by citizens, investors and corporates alike and shall provide factual and attractive information to investors. The portal should clearly communicate a sense of 'identity' at first glance. The Portal will have an intuitive user interface for rendering various services and providing role based access to various systems in use. Through the Portal, any user can seek information, request for services, and status check on service request, lodge an incident/complaint and provide suggestions. Portal shall exhibit enriched info graphics on various parameters of smart solutions.

Portal should serve as a cutting-edge communication tool that clearly conveys its mission, vision, offerings and purpose. The site shall help prospects and citizens to better understand and engage with the DSCL's mission. Portal shall be a useful tool for the target audience, while being visually appealing, user-friendly, and state-of-the-art. It must allow easy navigation. Portal must have an attractive mix of text, images, audio and video.

The portal should:

- increase traffic and visitor engagement through architecture, design, and other features such as social media integration
- help visitors easily understand the corporation's mission and obtain information about DSCL's offerings
- deliver content concisely and clearly; includes dynamic information

The portal should have links to log-in for visitors (through APIs of Gmail/Facebook etc.) and employees. This log in shall redirect the user to the portal with rights to view or update content as per user status. The home page shall be clean and visually compelling that quickly conveys to the visitor, corporation's mission and what the DSCL does. This shall include dynamic 'Call-Outs' which highlight what's new on the website as well as information sliders. The portal should primarily be available in Hindi & English.

Mobile enablement framework will be deployed for DSCL, which deals with both rendering the portal in mobile devices through necessary UI components as well as making native mobile apps for mobile platforms i.e. Android, iOS, Windows. App shall be available on App store (iOS), Google play store (Android) etc. for freely downloadable for interested stakeholders.

Refer subsequent section for minimum functional and technical requirement specifications.

4.22.1 ERP

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

Functional and Technical Requirements:

a. Architecture

- Centralized Server Architecture (n-tier architecture with web enabled user interface)
- The presentation logic should be decoupled from the business components logic
- Data access layer should be on RDBMS platform. Backend RDBMS should be of latest proven version of leading RDBMS.
- Single Database (No Heterogeneous Database to be allowed as part of the proposed solution.

b. User Interfaces

- The solution proposed should be Unicode compliant. Authority envisages requirements for both English and regional language for Data Entry, Display, Input and Output
- Single Sign-on (for all the users) for accessing all the modules
- Any data entry needs to be carried out only once and further it should be made available as often as necessary to all the systems by providing pre-fill feature
- All modules should be homogeneous with respect to Keyboard use, screen layout and menu operations with Graphic User Interface (GUI) support
- GUI Form Administration should support
- Changing fields or tab labels
- Hiding fields or tabs.
- Changing the position or size of field or labels
- Adding restrictions like mandatory or not
- Setting default value in a field
- Changing list of value (LOV) contents
- Capability to setup logic to trap conditions to pop messages in response to conditions like logical data entry errors, certain conditions etc.
- Ability to provide various configurable parameters down to the end user level so that the user screens can have different functionality for a given user.
- Disparate information can be consolidated from a number of systems as required to produce reports and carry out ad hoc analysis and reporting

c. Access & Data Security

- Role based authentication for accessing various functionalities of different modules with encrypted passwords. Access Rights can be given to Individual Users or Groups
- Flexibility to define separate Role and Designation to the users. Upon transfers of officers / employees, applications / letters / complaints pending with the employee shall remain to the role and new employee will be able to take action on these applications / letters / complaints.
- User rights to various forms should be Create New Record, View existing Record or
- Edit existing record.
- System should be able to capture exceptions to detect frauds / mistakes
- An audit trail of changes to data in the system should be maintained to identify the users responsible for the modification. There should be a facility to create reports on audit logs

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

- User – self registration and first time password change prompt.
- System would allow user to login and avail services from any of the modules.
- System would allow user to view any Service information from Departments displayed on Web portal.
- During user id creation system would ask for Security question for any password reset request by user in future.
- System would prompt user to create password as per security policy.
- Alphanumeric passwords would be asked.
- System would ask user to create a transaction password to be used for performing any financial transaction with the concerned departments or while making any changes in the profile.
- During user id creation, system would ask user to furnish all personal details like
  - Name
  - Gender
  - Age
  - Address
  - Phone no.
  - Email id
  - Occupation
  - Family details
  - PAN/License/Passport/Voter Registration No./UID No. or any other Id proof details.
- System would prompt user to login using user id and password created and verify them.
- On successful password match, system would allow the user to login to the portal and allow him to access his/her profile. On unsuccessful password match, System would generate password error message and ask user to enter correct password in order to login to his/her profile.
- System would allow user to edit his/her personal details like Name, Address etc.

- System would display the service related information/Instructions to fill up requested details in the entry forms like applicable fee and documents to be attached/submitted along with application request.
- For CCC Operator, system would initially allow CCC operators to login using their login ids and passwords as given by System administrator. After first time login by all CCC operators the system would ask them to change their password (alphanumeric) as per the security policy.
- After successfully changing the password and verifying the same on to the system, CCC operator would get access to all the modules, can accept and insert details of the requests received by the citizens for specific modules.
- System would display instructions to CCC operators at the time of inserting details in the request form for various applications.

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

- Employees Information System having unique Employee ID
- Payroll Package
- Leave Monitoring System
- Biometric based Attendance System
- Employee Performance Monitoring System, etc.

A. Profile Management:

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

B. Security

Based on ISO 27001/BS 7799 standards, user access to the system must be through a single sign on process, which should involve specification of a user Identification, a password and the applications displayed must be as per the user profile and authority. The system should al low user to change his/her password based on a given time frame as well as give the user the option to change his password at any time. The system should disable the User profile after five unsuccessful log-on attempts. The system should be able to log successful and failed attempts to the system. This section highlights the security architecture proposed for the e-Municipality system:

I. General Requirements

i. Information, hardware and software would be secured to both internal and external parties (such as through password encryption).

ii. The security measures adopted should be of wide range and of high quality, to create confidence in the systems security and integrity. The system should be protected against

deliberate or accidental misuse that might cause a loss of confidence in it or loss or inconvenience to one or more of its users.

iii. System level and application level authentication between portal and between applications within portal, if any, to ensure against security attacks

There should be four levels of security considerations as described below:

a. Key Security Considerations at the User level:

(i) User authentication

(ii) Role based access to services, transactions and data

b. Key Security Considerations at the Network/ Transport level:

(i) Network Link Encryption (IPSEC)

(ii) Encrypted HTTP session using SSL (HTTPS)

c. Key Security Consideration at the Infrastructure Level:

(i) Firewall to filter unauthorized sessions/traffic

(ii) Intrusion Prevention System to detect/ prevent unauthorized activities and

sessions

d. Key Security Considerations at the Application & Database level:

(i) Secure storage of user credentials

(ii) Server–to-Server communication encryption

(iii) Secured/ encrypted storage of data/ data elements in the Database & DB Backups

(iv) Comprehensive logging & audit trail of sessions and transactions

Unified Messaging system:

SMS: The Web-Portal shall have facility to send SMS to Mobile number of a citizen which was provided while requesting certain information or service. The SMS shall be auto-generated based on the information or service requested on occurrence of its change of status. All the application needs to be integrated with SMS gateway.

E-mail: The Web-Portal shall have facility to send e-mails to

o The e-mail address of a citizen, provided while requesting certain information or service.
o The e-mail shall be auto-generated based on the information or service requested on occurrence of its change of status.
o Reporting Officials maintaining the hierarchy, in cases of delay (as per the Citizens' Charter) in providing services.

Workflow Management System:

Workflow Management System would serve as an integrated functionality across all the departmental modules to receive and process the request / applications received via any of

the service delivery channels. Each request/application should be processed via workflow engine mechanism. I.e. each of the application should be routed to the respective department official's activity dashboard. WMS should also have a facility of delegation of powers.

Workflow management system should be compliant to workflow standards: BPMN, BPEL and WFMC

RTI Management module based on Business Process Management platform with the following features:

• Ability to record incoming RTI queries into the system.

• Ability to upload the documents along with the queries.

• Ability to route the RTI queries to different department users.

• Ability to send the response of the queries to the Applicant who had filed the RTI.

• Ability to reopen old RTI request in case of First and Second RTI Appeal.

A] Citizen Service Module:

- Citizen Help Desk
- Facility to lodge New Complaints, Check Status
- Facility to check citizen data, Bill Dues, Application Status,
- Payment Status, Renewal Status, Certificates issuance
- Inter & Intranet
- Citizen Charter MSC, Authority

B] Application Acceptance & Delivery of Outputs

- Department-wise categorization
- Allow system to accept service specific inputs
- Capture of Mobile No. of Applicant
- Re-submission of rejected application after compliance
- Check-list for documents to be submitted along-with application
- Define citizen charter (list of the officers & duration for service delivery) Authority
- Fees to be accepted Accounts
- Generate Token of Application acceptance
- Rejection Note in case of inadequate application
- Delivery of the output through CCC / Internet / KIOSK
- SMS alert to applicant upon decision SMS Gateway

C] Payment Acceptance

- Property Tax
- Accounts,
- Departmental
- Modules,
- Property Tax
- Water Tax
- Professional Tax
- Vehicle Tax
- License
- All Departmental Services
- Tender Document Fees
- Any other

D] Citizen Services (General) [Such services won't have any department specific functionality. CCC module, by using Workflow Management System should be able to deliver these services]

- Marriage Certificate
- NOCs for other govt. departments
- Booking of various Corporation premises such as Halls,
- Community Halls, Open air theatre, Amphitheatre, Auditorium,
- Ground, Party Plot, etc.,
- Issue of health license for shop having area
- Any other services

E] Marriage Registration Sub-Module

- Design of Forms & Database for the Marriage Registration
- Functionality
- Capture of Thumb Impressions of the Applicants & Witnesses
- Capture of the Photograph of the Applicants & Witnesses
- Scrutiny of the Applications

F] Professional Tax

- Enrolment and Registry Enrolment of firms. (PEC & PRC) Property Tax, GIS
- Details of firms along with their contact details, address, etc. Property Tax, GIS
- Outstanding Professional Tax details for different firms. Property Tax, GIS

G] Vehicle Tax

- Capturing Vehicle details such as Engine No/ Chassis no,
- Capturing type of Vehicle for collection of taxes.
- Capturing details of the Vehicle owner (Name, Address, Contact details, etc.)

H] MIS

- SMS alert to applicant upon decision
- Services Statistics, CCC / KIOSK, Department-wise
- Officer-wise list of services pending HRMS, WMS
- Marriage Registration periodic / statistical reports
- Professional Tax collection / outstanding report
- Interest calculation for outstanding Professional tax
- Defaulter list for Professional Tax payment GIS
- Property Tax collection report
- Report containing license issued details and payment
- collected for the same.
- Vehicle Tax collection report

I] Additional Functional Scope after validation

- RTI
- Issuing License : Gumasta License, Hawker's License, Health license etc

These are the module to be the part of ERP system to provide service delivery the system will be flexible to scale up and configure the solutions and modules as and when required based on city requirement for governance and service delivery.

4.22.2 Web Portal

Functional and Technical Requirements of Web Portal

Sl no	Description
1.	**Home Page** A clean, visually compelling home page that quickly conveys to the visitor, the DSCL's mission and what DSCL does. It will include (but not limited to) the following information either directly or linked through other pages: ▪ About DSCL; Corporation, Message from the CMD, Board of Directors, Shareholding pattern, Organogram & Key Personnel ▪ City Profile

Sl no	Description
	▪ Master Plan ▪ Investment opportunities ▪ Key statistics ▪ Tourist Locations ▪ GIS map of the City ▪ Photo Gallery ▪ Online Services listing (e-governance services) ▪ Opportunities; Tenders, Careers, Empanelment, Training ▪ Downloads ▪ Links to Facebook, twitter etc. ▪ FAQs ▪ Feedback ▪ Contact Us ▪ Search ▪ News & Updates ▪ Log in ▪ Privacy Policy, Disclaimer, Visitors count, Important links, Site map
2.	**Branding:** Clearly communicates a sense of 'identity' at first glance.
3.	**Visual appeal:** The site must have an attractive mix of text, images, audio and video.
4.	**Fast Loading Pages:** Optimization of web pages for a faster browsing experience with compatibility with key industry browsers and platforms.
5.	**Responsive Design:** The site must be mobile-optimized through responsive design methods. Therefore, it should detect that a mobile device is being used and present the user with the mobile version first. The user should be able to switch to the desktop version and adjust resolution and format accordingly.
6.	**Bilingual** The portal shall be available in Hindi & English and Unicode complaint.
7.	**Simple and clear navigation:** The site should be easy to navigate. Information should be grouped and presented in a logical manner and require no more than three levels of "drill down" for the user to find the desired information thus creating a clean, clear, easy and satisfying user experience. This should include drop down menus, so that the visitor can easily find what they are looking for with a few clicks of the mouse.
8.	**Search Tools:** Provide search capabilities using key words or phrasing that will provide access to content from throughout the site. Additionally, make it possible to download historical and recent data whereby the user can define his/her preference. Platform should allow users to search content of the portal easily and quickly without the need of high speed bandwidth.
9.	**Important Links:** Links should be placed within the portal to allow individuals to contact institutions affiliated with the DSCL and access to the portal as well the respective departments/agencies/corporations/ministries.
10.	**Easy access to Key performance indicators (Infographics):** Seamless presentation of dashboard data to provide continuously updated graphs and charts.
11.	**News/Update feed:** Constant and dynamic update feed on portal home page. Displays announcements and notifications for new content additions on front page of portal.

Sl no	Description
12.	**Calendar and bookings:** A dynamic calendar that displays events as well as filters for searching events and booking any available venues/functions.
13.	**Contact Form:** Provides a web-based contact form with anti-spam controls and shall allow stakeholders to track the status of request at any point of time, if any.
14.	**e-Mails**: automatically send follow-up emails to our stakeholders (subscribers) if they visited a specific web page, or completed some specific task (e.g. survey) on the website.
15.	**Social Media Engagement Tools:** New tools to improve interaction with social media.
16.	**Search Engine Optimization (SEO):** Portal availability using common search engines to ensure it is optimized using SEO.
17.	**Search capability:** Portal should provide search engine with advanced full-text search capabilities.
18.	**Compatibility:** Site must be compatible with common operating platforms including Google Chrome, Microsoft® Internet Explorer 8.0 or higher, Microsoft Edge, Mozilla Firefox, and Safari 5.0 or higher.
19.	**Mobile Access**: Portal must be "responsively designed" to accommodate mobile users. This also includes accommodations for slower, cellular internet connections. This includes compatibility with iOS, Android and other industry standard platforms.
20.	**Settings:** Portal must not require plug-ins as a default.
21.	**Performance:** Portal must be able to handle multimedia (video) with high performance.
22.	**HTML Compliance:** Full compliance with HTML 5.0 or higher.
23.	**GIS:** web GIS view of Dehradun Smart City depicting information through various layers would be shown to stakeholders; showing occupied and vacant land parcels, access to information on industries, residential properties, education & health facilities, transportation etc.
24.	**Security:** Portal shall be secure against hacking and other vulnerable activities.
25.	**Content Management System:** ✓ shall have Content Management System to update the content on the Portal which shall have minimum following capabilities: ▪ Content Authoring ▪ Content Publishing ▪ Content Delivery ▪ Content Storage Management ▪ Content Archival ✓ Separation of content from presentation, which allows authors to focus on content rather than web design. ✓ Content storage management of all types of content; text graphic, audio, video etc.
26.	**Integration with other applications:** Different existing and future applications/modules shall have to be seamlessly integrated with the portal. It is envisaged that GIS and the proposed systems shall work in an integrated manner to allow DSCL to extract maximum benefits from the system.
27.	**Design and Construction**

Sl no	Description
	▪ Work closely with the DSCL at each stage of the design to identify user needs and corresponding user interface requirements, workflows, and functionalities ▪ Ensure integration of all elements including content, information format, compatibility with software platforms used by DSCL and standards for content management ▪ Platform should allow easy integration of multimedia products and user-friendly administrator interface ▪ Create wireframes, storyboards and prototypes to propose options for implementation. Provide five (5) template designs for review to select a concept ▪ Concepts should reflect the DSCL's identity, nature and purpose ▪ Develop corresponding user interface components (web templates, style sheets, scripts, images, dashboards, social media interfaces) as needed ▪ Use simple, cost-effective techniques to test designs with representatives of target audience prior to launch of portal ▪ Submit the final concept to DSCL for review prior to 'going live' ▪ Secure the existing portal prior to transitioning to the new platform ▪ Keep a full backup of the portal through the currency of the Project ▪ Manage all upgrades and updates on the website including content update in an efficient and integrated manner ▪ Portal design shall support easy upgrades and updates on content without the need to redo the base design.

4.22.3 Mobile App

With rapidly increasing levels of mobile penetration and continuous improvement in bandwidth, and requirements of accessibility and citizen convenience, it has been envisaged to offer information dissemination to stakeholders over mobile devices. There shall be a strong interfaces, technologies, applications etc. for mobile devices. In order to maximize citizen convenience and bring about business process improvements, the successful MSI shall continuously innovate, upgrade and incorporate such new technologies that emerge new avenues.

Functional and Technical Requirements of Mobile App

Sl no	Description
1	Mobile app should mirror the portal and be adapted for optimum viewing on multiple operating systems and device sizes. However the actual application layout design for both mobile and web is the responsibility of MSI.
2	Mobile app must be based on latest HTML 5 and above.
3	Mobile app shall be native on Android, iOS and Windows platform.
4	Mobile app should be in Hindi & English.
5	Mobile app should be capable of showcasing enriched infographics to its stakeholders.
6	Mobile app shall be designed in such a manner that it shall address the following key issues:

Sl no	Description
	▪ Caching: Caching unnecessary data on a device that has limited resources ▪ Communication: Failing to protect sensitive data over any carrier ▪ Data Access: Failing to implement data-access mechanisms that work with intermittent connectivity
7	Mobile app shall be integrated with main core solution proposed. There shall be facility to PUSH through and PULL through mechanism to get and receive information using SMS service.
8	Mobile app shall provide critical data such as user identification and location information including latitude, longitude and altitude.
9	The mobile app shall have the ability to take and transmit, pictures and videos in real time along with geo-tags from the device.
10	Mobile app should have capability of - ▪ Image compression, B/w conversion from color images ▪ Auto cropping, Auto orientation, perspective correction, geo capture ▪ Image capture setting (camera resolution, image type)
11	Mobile app shall have the ability to push information to the mobile app as well as post bulletins and resources on the mobile app through API's.
12	Platform will provide a report generating tool, which can be used to generate customized reports at any level.
13	Platform should allow for a graphical interface to view the summary data in MIS reports. This would include trend graphs, graphs indicating how much of the target has been met etc.

4.23 Scope of Integration

MSI has to integrate all the existing and upcoming solutions available in city with respect to uses cases and the effective decision management perspective as mentioned below but not limited to:

Existing Solutions:

- Smart Lighting
- ICT Enabled Solid Waste Management
- Intelligent Transportation System
- E-Challan System
- Smart Education
- Smart Health Management System

Future Solutions:

- SCADA for Water
- SCADA for Energy
- Intelligent Transportation System
- E-Challan System
- Public Bike Sharing
- Smart Water Supply System

5 Project Governance and Change Management

5.1 Project Management and Governance

5.1.1 Project Management Office (PMO)

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

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

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

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

i. Module development status
ii. Testing results
iii. IT infrastructure procurement and deployment status
iv. Status of setting up/procuring of the Helpdesk, DC hosting
v. Any other issues that either party wishes to add to the agenda.

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

5.1.2 Helpdesk and Facilities Management Services

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

MSI shall setup a central helpdesk dedicated (i.e. on premise) for the Project. This helpdesk would be operational upon implementation of the Project. Providing helpdesk/support services from a shared facility of any other party/provider is not permitted.

Functional requirements of the helpdesk management system, fully integrated with the

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

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

Sl no	Resources
1.	Operators
2.	Program Manager
3.	Solution Architect
4.	IoT Expert
5.	Command Control & Communication Centre Expert
6.	Database Expert
7.	Security Expert
8.	System Admin
9.	Network Expert
10.	GIS Expert

Note: Numbers provided for staff providing 24*7 support is excluding relievers.

5.1.3 Steering Committee

- The Steering Committee will consist of senior stakeholders from DSCL, its nominated agencies and MSI. MSI will nominate its Smart City vertical head to be a part of the Project Steering Committee
- MSI shall participate in monthly Steering Committee meetings and update Steering Committee on Project progress, Risk parameters (if any), Resource deployment and plan, immediate tasks, and any obstacles in project. The Steering committee meeting will be a forum for seeking and getting approval for project decisions on major changes etc.
- All relevant records of proceedings of Steering Committee should be maintained, updated, tracked and shared with the Steering Committee and Project Management Office by MSI.
- During the development and implementation phase of the project, it is expected that there will be at least fortnightly Steering Committee meetings. During the O&M phase, the meetings will be held at least once a quarter.
- Other than the planned meetings, in exceptional cases, DSCL may call for a Steering Committee meeting with prior notice to MSI.

5.1.4 Project Monitoring and Reporting

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

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

5.1.5 Risk and Issue management

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

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

- MSI shall monitor, report, and update the project risk profile. The risks should be discussed with DSCL and a mitigation plan be identified during the project review/status meetings. The Risk and Issue management should form an agenda for the Project Steering Committee meetings as and when required.

5.1.6 Governance procedures

MSI shall document the agreed structures in a procedures manual.

5.1.7 Planning and Scheduling

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

The project plan should include the following:

1. The project break up into logical phases and sub-phases;

2. Activities making up the sub-phases and phases;

3. Components in each phase with milestones;

4. The milestone dates are decided by DSCL in this RFP. MSI cannot change any of the milestone completion dates. MSI can only propose the internal task deadlines while keeping the overall end dates the same. MSI may suggest improvement in project dates without changing the end dates of each activity.

5. Key milestones and deliverables along with their dates including those related to delivery and installation of hardware and software;

6. Start date and end date for each activity;

7. The dependencies among activities;
8. Resources to be assigned to each activity;
9. Dependency on DSCL

5.1.8 License Metering / Management

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

5.2 Manpower Deployment

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

Sl no	Type of Resource	Minimum Quantity	Minimum Deployment during Implementation phase	Minimum Deployment during O & M phase
1.	Team Leader-cum-Program Manager	1	100%	100%
2.	Solution Architect	1	80%	Onsite Support to Project team on need basis
3.	IoT Expert	1	60%	Onsite Support to Project team on need basis
4.	Command and Control Expert	1	80%	Onsite Support to Project team on need basis
5.	ITMS Expert	1	50%	Onsite Support to Project team on need basis
6.	Database Expert	1	80%	100%
7.	Security Expert	1	60%	Onsite Support to Project team on need basis
8.	Systems Administrator	1	50%	100%
9.	Network Administrator	1	50%	100%
10.	GIS Expert	1	80%	100%

11.	Software Lead	1	80%	100%
12.	Quality Assurance/Testing	As required	As required	As required
13.	Programmer	As required	As required	As required
14.	Mobile App Developer	As required	As required	As required

Apart from the above mentioned manpower, MSI is required to provide suitable manpower to monitor the data feeds at command Centre and support DSCL in operationalization of the project. Total number of operators required for the project is 30 in three shifts. DSCL reserves the right to increase or decrease the number of operators. The exact role of these personnel and their responsibilities would be defined and monitored by DSCL and respective departmental personnel. MSI shall be required to provide such manpower meeting following requirements:

1. All such manpower shall be minimum graduate pass

2. All such manpower shall be without any criminal background / record.

3. DSCL reserves the right to carry out background check of the personnel proposed on the Project for verification of criminal record, at the beginning of deployment or during deployment.

4. MSI shall have to replace any person, if not found suitable for the job.

5. All the manpower shall have to undergo training from MSI for at least 15 working days on the working of project. Training should also cover dos & don'ts and will have few sessions from DSCL officers on right approaches for monitoring the feeds & providing feedback to DSCL, Traffic Police and other associated government agencies.

6. Each person shall have to undergo compulsory 1 day training every month

7. Operational Manpower shall work in 3 shifts, with no person being made to see the feeds for more than 8 hours at a stretch.

Detail operational guideline document, standard operating procedure, governance and oversight plan shall be prepared by MSI during implementation which shall specify detail responsibilities of these resources and their do's & don'ts.

The supervisors required for operationalization of the project will be provided by DSCL, as per requirements.

5.3 Change Management & Control

5.3.1 Change Orders / Alterations / Variations

a. MSI agrees that the requirements given in the Bidding Documents are minimum requirements and are only indicative. The vendor would need to etch out the details at the time of preparing the design document prior to actual implementation. It shall be the responsibility of MSI to meet all the requirements of technical specifications contained in the RFP and any upward revisions and/or additions of quantities, specifications sizes given in the Bidding Documents required to be made during execution of the works, shall not constitute a

change order and shall be carried out without a change order and shall be carried out without any time and cost effect to Purchaser.

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

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

5.3.2 Change Order

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

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

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

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

e. Within ten (10) working days of receiving the comments from the Purchaser or the drawings, specification, purchase requisitions and other documents submitted by MSI for approval, MSI shall respond in writing, which item(s) of the Comments is/are potential changes(s) in the Scope of work of the RFP document covered in the Contract and shall advise a date by which change order (if applicable) will be submitted to the Purchaser.

5.4 Exit Management

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

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

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

5.4.1 Cooperation and Provision of Information

During the exit management period:

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

b. Promptly on reasonable request by the DSCL, MSI shall provide access to and copies of all information held or controlled by them which they have prepared or maintained in accordance with this agreement relating to any material aspect of the services (whether provided by MSI or sub-contractors appointed by MSI). The DSCL shall be entitled to copy of all such information. Such information shall include details pertaining to the services rendered and other performance data. MSI shall permit the DSCL or its nominated agencies to have reasonable access to its employees and facilities, to understand the methods of delivery of the services employed by MSI and to assist appropriate knowledge transfer.

5.4.2 Confidential Information, Security and Data

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

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

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

5.4.3 Transfer of Certain Agreements

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

replacement services by the DSCL or its nominated agency or its Replacement MSI.

5.4.4 General Obligations of MSI

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

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

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

5.4.5 Exit Management Plan

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

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

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

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

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

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

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

g. Payments during the Exit Management period shall be made in accordance with the

Terms of Payment Schedule.

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

6 Project Implementation Schedule, Deliverables and Payment Terms

6.1 Project Implementation Schedule and Deliverables Payment Schedule

T = 14 Days from Issue of LOI or LOA

Note:- All the payments against different mile stones shall be done only after the approval of respective mile stones from the authorities.

Sl no	Milestones	Deliverables	Timelines (in months)
1	**Project Implementation Phase**		**T + 10 months**
1.1	Project Inception Report	Detailed site survey report including infrastructure requirement analysis, hardware deployment plan, recommended action plan to address the gaps, budget estimates for addressing the gaps uncovered during the survey, phase wise location distribution etc. Detailed Project Plan including resource deployment, Communication plan, Risk management plan, Information Security and Business Continuity, Sensitization & Training Plan, Operations management plan etc.	T + 1 months
1.2	Requirement Study • Command and Control Centre (DICCC) including Data Centre • City IT Network Infrastructure. • Intelligent Traffic Management System (ITMS) • Environmental Monitoring System • City Web Portal & Mobile App • Enterprise GIS	Architecture and design for DICCC, City IT Network and Data Centre including Data Centre Architecture, Network Architecture, Security architecture etc. approval of FRS, SRS including Solution Architecture, Application Design Documents (HLD & LLD) of the proposed system, HLD & LDD should be prepared by OEM Integration report for external applications also to be approved.	T + 2 months

Sl no	Milestones	Deliverables	Timelines (in months)
	• City Wi-Fi • City Surveillance • Transit Management System • Integration of DICCC platform with existing & under-development external Systems/ Applications as per scope		
1.3	**Phase I: Go-Live** **a.** Design, supply, installation, commissioning including interior civil work, hardware, system software, network equipment, bandwidth procurement	1. Site Completion/readiness Report 2. Delivery Acceptance Reports from DSCL/authorized entity 3. Installation & Commissioning Reports 4. Software Licenses details requirement	T + 3 months
1.3	**Phase II: Go-Live** • Operationalization of Command Control & Communication Centre along with DC and DR • City IT Network Infrastructure – pan city availability of secure network for all proposed edge devices & sensors. Guidelines issued by MoUD for cyber security requirement should be adhered to for designing network for sensor & Wi-Fi traffic • GIS – Supply, installation, data migration, training & operationalization of enterprise GIS system for the city • City web-portal – Design, development, content writing, training & deployment of city web portal	1) Site Completion/readiness Report 2) Delivery Acceptance Reports from DSCL/authorized entity 3) Installation & Commissioning Reports 4) UAT/FAT and Go Live Certificate from DSCL/authorized entity 5) Training Content & Completion Certificate 6) Security Audit Certificate from Cert-In/STQC for Data Centre and Applications	T+7 Months

Sl no	Milestones	Deliverables	Timelines (in months)
	• ITMS – Supply, installation, commissioning, training and operationalization of ITSM components (ANPR, RLVD, SVDS, ATCS, PA, ECB) at 30% of total identified locations • Wi-Fi - Supply, installation, commissioning, training & operationalization of City Wi-Fi at 50% of total identified locations • Environmental Sensors - Supply, installation, commissioning, training & operationalization of Environmental sensors at sensors • Variable Messaging Board - Supply, installation, commissioning, training & operationalization of Variable Messaging Boards at 50% of total identified locations • City Surveillance - Supply, installation, commissioning, training & operationalization of Cameras at 50% of total identified locations • Transit Management - Supply, installation, commissioning, training & operationalization of Transit Management System		
1.4	**Phase III: Go-Live** • ITMS – Supply, installation, commissioning, training and operationalization of ITSM components (ANPR, RLVD, SVDS, ATCS, PA, ECB) at	1. Site Completion/readiness Report 2. Delivery Acceptance Reports from DSCL/authorized entity 3. Installation & Commissioning Reports 4. Software Licenses details	T + 9 months

Sl no	Milestones	Deliverables	Timelines (in months)
	remaining 70% of total identified locations • Wi-Fi - Supply, installation, commissioning, training & operationalization of City Wi-Fi at 50% of total identified locations • Variable Messaging Board - Supply, installation, commissioning, training & operationalization of Variable Messaging Boards at remaining 50% of total identified locations • Mobile App – Design, development, delivery, training & installation of mobile app in android & iOS for identified services & integration with existing services of DSCL • City Surveillance - Supply, installation, commissioning, training & operationalization of Cameras at 50% of total identified locations •	5. UAT/FAT and Go Live Certificate from DSCL/authorized entity 6. Availability of Mobile App on Play Store & Apple App Store 7. Training Content & Completion Certificate	
1.5	**Phase IV: Integration & Project Final Go-Live** Integration with external applications (existing & proposed)- ▪ Smart Lighting ▪ ICT Enabled Solid Waste Management ▪ Intelligent Transportation System ▪ E-Challan System ▪ Smart Water Supply System ▪ Smart Education ▪ Smart Health Management System	1. UAT/FAT and Go Live Certificate from DSCL/authorized entity 2. Training Content & Completion Certificate 3. Security Audit Certificate from Cert-In/STQC 4. Source code of portal, Mobile App & customized applications	**T + 10 months = T1**

Sl no	Milestones	Deliverables	Timelines (in months)
	▪ E-Gov		
2	**Project Operation & Maintenance Phase**		**T1 + 60 months**
2.1	Operation & Maintenance	• Monthly & Quarterly SLA Reports • Adhoc Reports	T1 + 60 Months

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

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

6.2 Payment Schedule

The total payment shall be paid in two part (i) Capex (70% of total bid value) (ii) Opex (30% of total bid value). The further breakup of Capex and Opex shall be as under:

Sl no	Milestones	Timelines	Payment
	Capex (70%)		
1.	Requirement study	T + 2 Months	10% of capex value
2.	Phase I : Go Live	T + 3 Months	15% of capex value
3.	Phase II : Go Live	T + 7 Months	30% of capex value
4.	Phase III : Go Live	T + 9 Months	25% of capex value
5.	Phase IV : Integration & Project Final Go-Live	T1 = T + 10 months	20% of capex value
	Opex (30%)		
6.	Project Operations & Maintenance phase for a period of 60 months from the date of Final Go Live	T1 + 60 Months	OPEX will be paid in twenty (20) equal quarterly instalments spread across 5 years Post Final Go-Live

Note 1: If successful bidder requests for Mobilization advance, following conditions shall be applicable –

a. Mobilization advance can be maximum of 10% of capex value

b. Mobilization advance shall be released only after receipt of Bank Guarantee of 100% of the requested amount

c. Mobilization advance shall be interest bearing and PLR rate of interest shall be payable to DSCL by the successful bidder
d. Mobilization advance shall be adjusted by Phase III of project implementation (T + 10 months)

Note 2:
a. All payments to the Systems Integrator shall be made upon submission of invoices along with necessary approval certificates from DSCL
b. The above payments are subject to meeting of SLA's failing which the appropriate deductions as mentioned in the Volume III of this RFP

7 Annexure

7.1 Annexure I: Bill of Material

Mentioned below is the indicative Bill of Material for each proposed project component, however the below quoted numbers are indicative only and MSI is required to access the exact requirement, location wise, for all the proposed solution components and shall accordingly propose and size the hardware and software infrastructure requirement to meet the RFP specifications and project objectives and SLA. Bidder should meet the specification given in RFP, any deviation with RFP specification would not be accepted. Bidder should add any additional item required as part of solution.

S.No	Line Item	Unit of Measurement	Indicative Quantity
	Data Center		
1.	Integrated Command and Control software and solution	Set	1
2.	Enterprise Service Bus with API Integration	Set	1
3.	Internet Router	Nos.	2
4.	Data Center Next Generation Firewall	Nos.	2
5.	Internet Firewall	Nos.	2
6.	Core Router	Nos.	2
7.	Core Switch	Nos.	2
8.	TOR/Distribution Switch	Nos.	4
9.	Anti-APT	Nos.	2
10.	End Point Detection and Response	Set	1
11.	SIEM	Set	1
12.	Server Load balancer	Nos.	2
13.	Link Load Balancer	Nos.	2
14.	DDoS	Nos.	2
15.	WAF	Nos.	2
16.	Key Management	Set	1
17.	Data Security	Set	1
18.	Secure Email Gateway	Set	1
19.	Secure Web Gateway	Set	1
20.	WebSite and File Monitoring Solution	Set	1
21.	EMS	Set	1

22.	Endpoint Security	Set	1
23.	HCI infrastructure	Set	As per requirement
24.	Non-HCI infrastructure	Set	As per requirement
25.	Video Wall, Controller and Management Software	Set	1
26.	Video Conferencing solution	Set	1
27.	IP Telephony with Citizen Centric Services	Set	1
28.	Analytics VMS and Video Analytics	Set	1
29.	Network Video Recorder	Set	1
30.	Integrated Data Center Infrastructure	Set	1
31.	10 KVA UPS	Nos.	2
32.	Site Preparation Cost	Lumpsum	1
33.	**Field Equipment**		
34.	DCPS	Nos.	As per requirement
35.	Field Junction Box	Nos.	As per requirement
36.	Camera Poles	Nos.	As per requirement
	Other Items		
37.	Workstation	Nos.	30
38.	Desktop for Help Desk	Nos.	5
39.	PAS	Nos.	5
40.	Multifunctional Device	Nos.	2
	Disaster Recovery		
41.	DR as a service with 50 % Capacity of DC	Lumpsum	1
42.	DR Management Software	Set	1
43.	DC - DR bandwidth	Set	1
	ATCS		
44.	ATCS Software and Solution	Set	1
45.	ATCS Traffic signal controller	Nos.	49
46.	4D Radar traffic Detector	Nos.	174
47.	Countdown timer	Nos.	180
48.	Traffic Light Aspects – Red	Nos.	515
49.	Traffic Light Aspects – Green	Nos.	1030
50.	Traffic Light Aspects – Amber	Nos.	515
51.	Pedestrian countdown timer with red and green lamp	Nos.	360
52.	Disabled Friendly Audio Tactile Device	Nos.	360

53.	Cantilever pole with mounting structure and junction box along foundation (Min Qty. MSI has to do Survey)	Nos.	115
54.	Straight pole with Mounting Structure with poles, junction boxes along with foundation (Min Qty MSI has to do Survey)		160
55.	Network Switch Ruggedized, and civil work	Nos.	49
	ITMS		
56.	ITMS - ANPR Software and Solution	Set	1
57.	ITMS - RLVD Software and solution	Set	1
58.	ITMS - SVD (Instant and Average Speed) software and solution	Set	1
59.	ITMS – TARS & E Challan solution	Set	1
60.	ITMS - PA Software and solution	Set	1
61.	ITMS - ECB management software and solution	Set	1
62.	ITMS - Variable Message Software and solution	Set	1
63.	ITMS – Traffic Monitoring & Management System	Set	1
64.	Smart Traffic Sensor A	Nos	28
65.	ANPR Systems for critical sites in the city	Nos	30
66.	Traffic Sensors B for Smart road and mobility	Nos	40
	RLVD		
67.	Red Light Violation Detection (RLVD) sensors	Per leg	58
68.	Camera with ANPR capability	No.	209
69.	Local processing unit	No.	35
70.	Mounting structure with pole, junction boxes etc.	Set	As per requirement
71.	Network Switch Ruggedized	No.	As per requirement
	SVD		
72.	Speed Detection System for covering 2 lanes in one direction with complete subcomponents including ANPR camera, sensors, wide angle evidence camera, IR illuminator, non-intrusive speed	Instant Speed No of Lanes	60
73.		Average Speed No of lanes	20
74.	SVD for dangerous junction		20
75.	Sensor, with cabling & mounting		
76.	infrastructure as required		
	Surveillance System		
77.	Outdoor Fixed Box Camera + IR Illuminator	No.	245
78.	Bullet Cameras + IR Illuminator	No.	150

79.	Outdoor PTZ Camera + IR Illuminator	No.	35
80.	Dome Cameras + IR Illuminator	No.	40
81.	ANPR Camera for Borders	No.	28
82.	Hand held units for E challan & TARS	Nos	150
83.	**PA System**		
84.	Public Address System – IP based PA with speakers	No.	24
85.	UPS (required capacity)	No.	As per requirement
86.	Mounting structures with pole etc.	No.	As per requirement
	Variable Message Sign		
87.	VMS board including VMS controller size 3000mm*1500mm*200 mm (minimum) with complete hardware and accessories as required + Mounting structure for VMS including UPS facility as per specifications	No.	50
88.	UPS (required capacity)	No.	As per requirement
89.	Mounting structures with pole etc.	No.	As per requirement
	ECB		
90.	ECB system	No.	35
91.	UPS (required capacity)	No.	As per requirement
92.	Mounting structure with pole etc.	No.	As per requirement
93.	Junction boxes for ITMS solution	No.	As per requirement
94.	Power cables	Meter	As per requirement
	Environmental Sensors		
95.	Environment sensors	No.	50
	Last Mile Connectivity and Bandwidth		
96.	24 Core Optical Cable based last mile connectivity	As required to cover pan city	As required to cover pan city
97.	Aggregate bandwidth at DC	As required to cover pan city	As required to cover pan city
98.	Leased Circuit Bandwidth	As required to cover pan city	As required to cover pan city
	Helpdesk		
99.	Hand Set	No.	5
100.	Head Set	No.	5
101.	Voice Logger	No.	1
102.	Soft telephone	No.	5
103.	Desktops	No.	5
104.	Officer Furniture and Revolving Chair	Lot	5

105.	**City Wi-Fi**		
106.	Access Point	No.	300
107.	Wi-fi Management/Controller		
108.	Network Switch Ruggedized	No.	As per requirement
109.	Junction Box	No.	As per requirement
110.	Online UPS – 1 KVA (in case bidder proposes solar power, required items should be mentioned in the technical proposal)	No.	As per requirement
	City Portal		
111.	City Portal	Set	1
112.	Mobile Application	Set	1
113.	Enterprise GIS	Unit	1
	Other Software		
114.	Enterprise database	Set	1
115.	ERP	Set	1
116.	Backup Software	Set	1
117.	Work-Flow and DMS solution	Set	1
118.	Directory Services		
	Power Backup		
119.	Diesel Genset	Unit	1
	Manpower		
120.	Manpower as per the RFP	No.	1
	Solid Waste Management		
121.	RFID Reader (With Controller)	No	30
122.	RFID Tags	No	25000
123.	Application Server Supply &Installation for data centre hosting	Set	1
124.	Database Server Supply & Installation for data centre hosting	Set	1
125.	RDBMS Supply & Installation for data centre hosting	Set	1
126.	Bin Level Sensors	No	500
127.	Solution Cost including License cost if any	Set	1
128.	VTMS (Vehicle Tracking and Monitoring system) solution cost including License cost if any	Lot	1
129.	GPS Devices (for new Vehicles)		30
130.	Citizens' App Development & integration Cost	Set	1
131.	Biometric Face Recognition Device	No	4
	Transit Management System (VTS)		
132.	GPS/OBU for Buses	Nos	1
133.	GPS for E-Rickshaws	Nos	1

134.	4G (or above) enabled SIM Cards	Nos	1
135.	Any other Hardware or Software required to meet the requirements (Bidder to list individual items and provide costing).	Nos	1
136.	Transit Management System Software	Set	1
	Smart Bus Shelter/ Depots		
137.	19" size of PIS display at Bus Shelters/stops + UPS	Nos	72
138.	55" size of PIS display at Bus Depots + UPS	Nos	2
139.	Fixed Box Camera	Nos	72
140.	ECB/ Panic Button	Nos	72
141.	VMD board (at Bus Shelters including VMS controller) size 960mm*960mm*200 mm (minimum) with complete hardware and accessories as required including UPS facility as per specifications	Nos	72
	4G (or above) enabled SIM Cards	Nos	72

7.2 Annexure II: DICCC Design Consideration

7.2.1 Key Design Considerations

Key design considerations taken into account are as follows –

- Designed for 24x7 online availability of application.
- Scalable solution on open protocols; no propriety devices/ applications
- API based architecture for Integration with other web applications and Mobile applications. Key guiding principles considered for building the integrated solution are the following:

o Continuous adoption of rapidly evolving Technology - Technology evolves too fast and Government projects similar to Smart City with its long procurement cycles do not align naturally to adapt to this trend. Also, any changes to existing implementations require contract changes, new RFP (Request for Proposal), etc. Hence the entire system would be built to be open (standards, open API, plug-n-play capabilities), components coupled loosely to allow changes in sub-system level without affecting other parts, architected to work completely within a heterogeneous compute, storage, and multi-vendor environment.

o Selection of best solution at best rate as and when required - Large integrated systems of Smart City operations should be designed to get best cost and performance advantages of natural technology curve (constant increase of speed and decrease of cost) and still aligned

to open procurement practices of the Government. For this to happen, architecture should be open and vendor neutral, use commodity hardware, and designed for horizontal scale. This allows buying of commodity compute, storage, etc. only when needed at best price.

o Distributed Access and Multi-channel service delivery -With high penetration of mobile devices and very large percentage of internet usage using mobile devices, it is imperative that the Smart City applications provide multiple channels of service delivery to its stakeholders. An important consideration is that the access devices and their screen capabilities (including browser variations) are numerous and constantly evolve. Hence, it is imperative to design the system such that the ecosystem of Smart City-integrated mobile apps also evolves.

o Security and privacy of data - Security and privacy of data within the integrated Project will be foundational keeping in view of the sensitivity of data and critical nature of the infrastructure envisioned to be built for Smart City operations. Security and privacy of data should be fundamental in design of the system without sacrificing utility of the system. When creating a system of this scale, it is imperative that handling of the sensitivity and criticality of data are not afterthoughts, but designed into the strategy of the system from day one.

o Provision of a Sustainable, Scalable Solution - The motive of the technological enhancements to provide a system that would be sustainable for the next few years. The expectation is that the system should sustain at least 5 years from GO-Live. The solution would be done keeping in mind the scalability of the system. The simplified procurement processes and ease of compliance is expected to lead to huge growth in contract's base. Every component of DSCL system needs to scale horizontally to very large volume of data.

The Application Software will have the capability to scale up to tomorrow's requirements like given below:

• Managing the entire Property Life Cycle (Data Collaboration between various govt. departmental systems)

• Maintaining Information on Citizen Life Cycle (Right from Birth to Marriage, Health, Education, Driving License, Interactions with DSCL)

• API Approach- DSCL has decided to adopt Open API as the guiding paradigm to achieve the above goals. Though DSCL system would develop a portal but that would not be the only way for interacting with the DSCL system as the stakeholders via his choice of third party applications, which will provide all user interfaces and convenience via desktop, mobile, other interfaces, will be able to interact with the DSCL system. These applications will connect with the DSCL system via secure DSCL system APIs. This architectural approach has been taken as the UI based integration through a ubiquitous web portal requires manual interaction and does not fit most consumption scenarios. The following benefits are envisaged from API based integration,

o Consumption across technologies and platforms(mobile, tablets, desktops, etc.) based on the individual requirements

o Automated upload and download of data

o Ability to adapt to changing taxation and other business rules and end user usage models

o Integration with customer software (GIS, Accounting systems).

• Business Rule Driven Approach-All configurations including policy decisions, business

parameters, rules, etc. shall be captured in a central place within the system. The system shall provide facility to the decision makers to add new or edit/delete existing policies or make changes with appropriate permission control and audit trace. Managing these in a central repository ensures only once source of truth is used across many application servers and reduces issues of inconsistent application behavior. Decoupling of the business parameters/rules/master data from the rest of the solution architecture and making them configurable allows for a great deal of flexibility.

- Data Distribution Service-As a future roadmap it is envisaged that the functionalities provided by the DSCL Project should be available as services that could be offered to other stakeholders on request. Keeping this in mind the system shall be able to provide data on subscription-publication basis. The organization of the information exchange between modules is fundamental to publish-subscribe (PS) systems. The PS model connects anonymous information producers (publishers) with information consumers (subscribers). The overall distributed application (the PS system) is composed of processes. The goal of the DDS architecture is to facilitate efficient distribution of data in a distributed system. Participant using DDS can ‘read’ or ‘write’ data efficiently and naturally with a typed interface. Underneath, the DDS middleware will distribute the data so that each reading participant can access the ‘most current’ values.

Guiding Architecture Principle

The IT architecture principles defined in this section are the underlying general rules and guidelines that will drive the subsequent development, use and maintenance of architectural standards, frameworks and future state target architecture.

DSCL system will be built on the following core principles:

Platform Approach

It is critical that a platform based approach is taken for any large scale application development, to ensure adequate focus and resources on issues related to scalability, security and data management. Building an application platform with reusable components or frameworks across the application suite provides a mechanism to abstract all necessary common features into a single layer. Hence the DICCC system is envisaged as a faceless system with 100% API driven architecture at the core of it. DSCL portal will be one such application on top of these APIs, rather than being fused into the platform as a monolithic system.

Open APIs designed to be used form the core design mechanism to ensure openness, multi-user ecosystem, specific vendor/system independence, and most importantly providing tax payers and other ecosystem players with choice of using innovative applications on various devices (mobile, tablet, etc.) that are built on top of these APIs.

Openness

Adoption of open API, open standards and wherever prudent open source products are of paramount importance for the system. This will ensure the system to be lightweight, scalable and secure. Openness comes from use of open standards and creating vendor neutral APIs and interfaces for all components. All the APIs will be stateless. Data access must be always through APIs, no application will access data directly from the storage layer or data access layer. For every internal data access also (access between various modules) there will be APIs and no direct access will be there.

Data as an enterprise asset

Information is a high value asset to be leveraged across the organization to improve performance and decision making. Accurate information would ensure effective decision making and improved performance.

Effective and careful data management is of high importance and top priority should be placed on ensuring where data resides, that its accuracy can be relied upon, and it can obtained when and where needed in adherence to The National Data Sharing and Accessibility Policy (NDSAP)

Different types of datasets generated both in geospatial and non-spatial form are supposed to be classified as shareable data and non-shareable data. Data management encompasses the systems and processes that ensure data integrity, data storage and security, including metadata, data security and access registers. The principles on which data sharing and accessibility need to be based include: Openness, Flexibility, Transparency, Quality, Security and Machine readable.

Performance

A best of breed solution using the leading technologies of the domain should be proposed in the solution ensuring the highest levels of performance. It will also ensure that the performance of various modules should be independent of each other to enhance the overall performance and also in case of disaster, performance of one module should not impact the performance other modules.

The solution should be designed in a manner that the following can be achieved:

- Modular design to distribute the appropriate system functions on web and app server
- Increase in-memory Operations (use static operations)
- Reduce number of I/O operations and N/w calls using selective caching
- Dedicated schemas for each function making them independent and avoiding delays due to other function accessing the same schema.
- Solution should provide measurable and acceptable performance requirements for users, for different connectivity bandwidths.
- The solution should provide optimal and high performance Portal Solution satisfying response time for slow Internet connections and different browsers.

Scalability

The component in the architecture will be capable of being scaled up to more user requests or handling more no. of input resources in various modules. Even inclusion of additional application functionalities can be catered to by upgrading the software editions with minimal effort.

The design of the system to consider future proofing the systems for volume handling requirements

- The application functions to be divided logically and developed as Modular solution.
- The system should be able to scale horizontally & vertically.
- Data Volume- Ability to support at least 20 % projected volume growth (year on year) in content post system implementation & content migration.

- Functionality – Ability to extend functionality of the solution without significant impact to the existing functional components and infrastructure.

- Loose coupling through layered modular design and messaging - The architecture would promote modular design and layered approach with clear division of responsibility and separation of concerns at the data storage, service and integration layer in order to achieve desired interoperability without any affinity to platforms, programming languages and network technologies. The architecture has to be scalable, maintainable and flexible for modular expansion as more citizen and business services are provided through the Project. Each of the logical layers would be loosely coupled with its adjacent layers

- Data partitioning and parallel processing - Project functionality naturally lends itself for massive parallel and distributed system. For linear scaling, it is essential that entire system is architected to work in parallel within and across machines with appropriate data and system partitioning. Choice of appropriate data sources such as RDBMS, Hadoop, NoSQL data stores, distributed file systems; etc. must be made to ensure there is absolutely no “single point of bottleneck” in the entire system including at the database and system level to scale linearly using commodity hardware.

- Horizontal scale for compute, Network and storage – Project architecture must be such that all components including compute, network and storage must scale horizontally to ensure that additional resources (compute, storage, network etc.) can be added as and when needed to achieve required scale.

No Vendor lock-in and Replace-ability

Specific OEM products may only be used when necessary to achieve scale, performance and reliability. Every such OEM component/service/product/framework/SI pre-existing product or work must be wrapped in a vendor neutral API so that at any time the OEM product can be replaced without affecting rest of the system. In addition, there must be at least 2 independent OEM products available using same standard before it can be used to ensure system is not locked in to single vendor implementation.

Security

The security services will cover the user profile management, authentication and authorization aspects of security control. This service run across all the layers since service components from different layers will interact with the security components. All public contents should be made available to all users without authentication. The service will authenticate users and allows access to other features of the envisaged application for which the user is entitled to.

The system should be designed to provide the appropriate security levels commiserate with the domain of operation. Also the system will ensure data confidentiality and data integrity.

The application system should have the following

- A secure solution should be provided at the hardware infrastructure level, software level, and access level.

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

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

- Appropriate mechanisms, protocols, and algorithms necessary to protect sensitive and confirmation data and information both during communication and storage should be implemented.
- Data security policies and standards to be developed and adopted across the Smart City departments and systems
- In order to adequately provide access to secured information, security needs must be identified and developed at the data level. Database design must consider and incorporate data integrity requirements.
- Role based access for all the stake holders envisaged to access and use the system
- Appropriate authentication mechanism adhering to industry good practice of Password Policies etc.
- Ability to adopt other authentication mechanism such as Electronic Signature Certificates
- Authorization validity to be ensured for the users providing the Data to the system. Data should be accepted only from the entity authorized
- Data should be visible only to the authorized entity
- Audit trails and Audit logging mechanism to be built in the system to ensure that user action can be established and can investigated if any can be aided(e.g. Logging of IP Address etc.)
- Data alterations etc. through unauthorized channel should be prevented.
- Industry good practice for coding of application so as to ensure sustenance to the Application Vulnerability Assessment

System must implement various measures to achieve this including mechanisms to ensure security of procurement data, spanning from strong end-to-end encryption of sensitive data, use of strong PKI national standards encryption, use of HSM (Hardware Security Module) appliances, physical security, access control, network security, stringent audit mechanism, 24x7 monitoring, and measures such as data partitioning and data encryption.

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

User Interface

The architecture and application solutions to be designed should promote simplicity and ease of use to the end users while still meeting business requirements. It should provide a simpler and more cost-effective solution. Reduces development time and makes the solution easier to maintain when changes in requirements occur.

This will be accomplished by the implementation of rich User Interfaces along with its integration with the DMS, Relational Data Store, Messaging and other external applications.

- Efficient and layout design are the key considerations that enhance usability which should be factored in while designing the application. Standard and consistent usability criteria must be defined. An intuitive, user friendly, well-articulated navigation method for the

applications greatly enhances the usability of the application.

- Effective information dissemination
- Enhanced functionalities including personalized delivery of content, collaboration and enriching GUI features
- The load time for all web page user interfaces must satisfy both the following response time targets on 1 mbps connection:

o 3 sec for welcome page

o 5 sec for static pages

o 10 sec for dynamic pages

- Ability to perform a simple search within 10 seconds on 1 mbps connectivity and a complex search (combining four terms) within 15 seconds regardless of the storage capacity or number of files and records on the system.
- Mobile Application Platform

o Applications and services including all appropriate channels such as SMS/USSD/IVRS and development of corresponding mobile applications to the applications and services leveraging the Mobile Service Delivery Gateway (MSDG) and Mobile App Store.

o Application platform should support the following smart phone mobile OS (Android 4.0 and above, iOS 4, 5 and above, Windows Phone OS 8.0 and above, Mobile Web App)

o Support the target packaging components like (Mobile Website, Hybrid App, Native App, Web App and Application Development, Eclipse tooling platforms)

o Support the ability to write code once and deploy on multiple mobile operating systems

o Support integration with native device API

o Support utilization of all native device features

o Support development of applications in a common programing language

o Support integration with mobile vendor SDKs for app development and testing

o Support HTML5, CSS3, JS features for smartphone devices

o Support common protocol adapters for connection to back office systems (i.e. HTTP, HTTPS, SOAP, XML for format)

o Support JSON to XML or provide XHTML message transformations

o Support multi-lingual and language internalization

o Support encrypted messaging between server and client components

Reliability

This is a very crucial system and data are of high sensitivity, the data transfer and data management should be reliable to keep the confidence of the stakeholders. The system should have appropriate measures to ensure processing reliability for the data received or accessed through the application.

It may be necessary to mainly ensure the following

- Prevent processing of duplicate incoming files/data
- Unauthorized alteration to the Data uploaded in the DSCL system should be prevented
- Ensure minimum data loss (expected zero data loss)

Manageability

It is essential that the application architecture handles different failures properly; be it a hardware failure, network outage, or software crashes. The system must be resilient to failures and have the ability to restart, and make human intervention minimal.

All layers of the system such as application, infrastructure must be managed through automation and proactive alerting rather than using 100's of people manually managing.

The entire application must be architected in such a way that every component of the system is monitored in a non-intrusive fashion (without affecting the performance or functionality of that component) and business metrics are published in a near real-time fashion. This allows data centre operators to be alerted proactively in the event of system issues and highlight these issues on a Network Operations Centre (NoC) at a granular level. The solution should be envisaged to utilize various tools and technologies for management and monitoring services. There should be management and monitoring tools to maintain the SLAs.

Availability

The solution design and deployment architecture will ensure that the application can be deployed in a centralized environment offering system High Availability and failover.

The solution should meet the following availability requirements

- Load Balanced across two or more Web Server avoiding single point of failure
- Deployment of multiple application instances should be possible
- Distributed or load balanced implementation of application to ensure that availability of services is not compromised at any failure instance.
- DC and DR infra network uptime should be 99.95%

SLA driven solution

Data from connected smart devices to be readily available (real-time), aggregated, classified and stored, so as not to delay the business processes of monitoring and decision making, and will enable appropriate timely sharing across the Smart City organization.

Readily available and consumed device data will facilitate timely access of analytics reports at every level and department of the Smart City and provide timely analysis of data as well as monitoring of KPIs through SLAs resulting in effective service delivery and improved decision making.

Integration Architecture

This section recommends the proposed integration architecture aligning with the overarching architectural principles.

The following are the integration specifications for the various integration scenarios -

Real-time integration

All the Smart City applications will be deployed in the Data Centre while any external application of the Smart City ecosystem will reside in outside premises.

The need for an OPC Unified Architecture (OPC- UA) is felt that will facilitate DSCL in defining an enterprise integration platform. An OPC platform will help in data exchange across applications in real-time mode (both synchronous and asynchronous), promote loose coupling with ease of maintenance and change, facilitate rapid composition of complex services, achieve scalability through modularity, and improved business visibility.

The OPC UA architecture is a service-oriented architecture (SOA) and is based on different logical levels. It is an architectural style that allows the integration of heterogeneous applications & users into flexible service delivery architecture. Discrete business functions contained in enterprise applications could be organized as layers of interoperable, standards-based shared "services" that can be combined, reused, discovered and leveraged by other applications and processes.

The following are the various integration modes and techniques that could be leveraged –

- OPC Base Services are abstract method descriptions, which are protocol independent and provide the basis for OPC UA functionality. The transport layer puts these methods into a protocol, which means it serializes/deserializes the data and transmits it over the network. Two protocols are specified for this purpose. One is a binary TCP protocol, optimized for high performance and the second is Web service-oriented

- SOAP web service based interfacing technique will be leveraged as the real-time point to point synchronous integration mode with external or third party systems. The following integration points could be considered for SOAP web service based interfacing -

o Payment gateway of the authorized banks to enable authorized users make financial transactions for the Smart City services availed by them. This should support a unified interface to integrate with all Payment Service Providers using web services over secured protocols.

o SMS application, acting as the SMS Gateway, will make use of APIs for SMS communication to GSM network using the GSM modem, which can be both event-driven as well as time- driven. The API will be exposed to initiate the broadcasting or alert notification.

o Social Media Apps and NoSQL data stores to exchange photos, videos and message feeds, based on interactions with Citizens and Business as well as comments/posts to inform stakeholders

o IVR/Customer Support solution with ERP and Transactional Data Repository to exchange citizen and business demographic, registration and payment data as well as transactional data related to citizen services and municipal operations.

- Message based interfacing technique will be leveraged for real-time asynchronous integration mode. The following integration points could be considered for message based interfacing -

o Central LDAP with ERP to synchronize member and employee user registration data

o Payment solution and ERP to exchange payment data for tracking of beneficiary’s

payment transactions against different services (citizen, workers, transporter, vendor), master data (employee, vendor/supplier, location, facilities, price table)

o Employee attendance data with ERP (HR Module) to capture data pertaining to employee location and attendance

o Departmental applications with ERP (Asset Management module) to exchange data for procurement and maintenance of any assets or infrastructure items for each department.

o Municipal operations application with ERP (Material Management module) to capture materials related transaction and inventory data for public works

o Other government applications with Smart City application to exchange data for government procurement, public health schemes, welfare schemes, citizen health, etc.

- RESTful API service based interfacing technique will be leveraged for the following integration areas-

o Access and use of various services provided by the different departments for citizens and business community will be done through a RESTful, stateless API layer.

o Access and use of various internal functions related to operations and administration of Smart City for departmental and DSCL employees will be done through a RESTful, stateless API layer

- Data integration in batch mode will be through ETL. The following integration points could be considered for ETL based data integration -

o Initial data migration to cleanse, validate and load the data extracted from source systems into target tables

o Data load from all the individual transactional systems like ERP, Grievance Redressal to central enterprise data warehouse solution for aggregation, mining, dashboard reporting and analytics.

Process Integration layer of the DSCL solution will automate complex business processes or provide unified access to information that is scattered across many systems. Process Integration will provide a clean separation between the definition of the process in the process model, the execution of the process in the process manager, and the implementation of the individual functions in the applications. This separation will allow the application functions to be reused in many different processes.

An enterprise service bus (ESB) is a software architecture model used for designing and implementing the interaction and communication between mutually interacting software applications in Service Oriented Architecture. As software architecture model for distributed computing it is a variant of the more general client server software architecture model and promotes strictly asynchronous message oriented design for communication and interaction between applications. Its primary use is in Enterprise Application Integration of heterogeneous and complex landscapes. Following are the requirement for an ESB system:

- The solution should support static/deterministic routing, content-based routing, rules-based routing, and policy-based routing, as applicable in various business cases.
- The bidder is expected to propose an Enterprise grade ESB Solution.
- The solution should have capabilities to receive input message in heterogeneous

formats from various different systems, interpret those messages, process and transform those messages to generate output and feed them to various different clients as per formats applicable.

o The solution should have features to communicate across different services, process them and expose as single aggregate service to facilitate business functionality

o ESB should support SOA standards such as XML, XSLT, BPEL, web services standards and messaging standards.

o ESB should support all industry standards interfaces for interoperability between different systems

There are four integration gateways envisaged as part of the solution design. The key requirements with respect to each of these are mentioned below:

SMS Gateway: SMS services are envisaged to be made available as part of the solution design. The service provider may integrate the solution with MSDG, and use the services available through it, or deploy its own SMS Gateway services at no extra charge to DSCL, but it is a mandatory requirement that all the SMS based services (alerts and notifications) should be available as part of the solution. Following are some of the key requirements for the SMS services through the solution:

- Should contain required details/information and targeted to the applicant or designated officers of tax departments and other stakeholders and users as per prevailing TRAI norms
- Facilitate access through access codes for different types of services
- Support automated alerts that allows to set up triggers that will automatically send out reminders
- Provide provision for International SMS
- Provide provision to receive messages directly from users
- Provide provision for personalized priority messages
- Resend the SMS in case of failure of the message
- Provide messaging templates

Email Services: Email services are envisaged to be made available as part of the solution design to send alerts/intimations/automated messages to registered email ids, based on preferences set up/opted by individual users. An authenticated SMTP mail service (also known as a SMTP relay or smart host) is envisaged to be integrated with the solution for sending mail from the solution, and delivered to intended inbox. Support anti-spam features.

Payment Gateway: The solution is envisaged to have integration with payment gateways, to enable authorized Users make financial transactions, as per rights and privileges provided to him/her. The service provider is required to make the provisions for integration with such third party gateways and provide payment services, as per requirement of the DSCL. Some of the key features of payment gateway are mentioned below:

- Should support secure integration with Payment Service Providers
- Should support a unified interface to integrate with all Payment Service Providers

- Should support integration with Payment Service Providers using web services and over HTTP/S protocol
- Should manage messages exchange between UI and payment service providers
- Should support beneficiary's payment transactions tracking against various services
- Should support bank accounts reconciliation
- Should provide logs for all transactions performed through the Payment Gateway for future financial dispute resolution that might arise between entities and either beneficiaries or Payment Service Providers
- Should maintain and keep transactions logs for time period required and specified by the financial regulations followed in country
- Should support redundant Payment Discovery
- Should submit Periodic Reconciliation Report to government entities
- Should support transaction reports to monitor and track payments
- Should support real-time online credit card authorization for merchants
- Should support compliance with emerging trends and multiple payment options such debit card, credit card, cash cards and other payment gateways
- Should provide fraud screening features
- Should support browser based remote administration
- Should support multicurrency processing and settlement directly to merchant account
- Should support processing of one-time or recurring transactions using tokenization
- Should support real time integration with SMS and emails
- IVR Services: IVR services are envisaged as part of Call Centre facility, which will be integrated with the solution, to provide information and services to the people who would contact the Call Centre: Some of the key features of the IVR services are mentioned below:
- Should provide multi-lingual content support
- Should facilitate access through access codes for different types of services
- Should support Web Service Integration
- Should support Dual Tone Multi Frequency (DTMF) using telephone touchpad - in-band and out-of-band
- Should support redirection to human assistance, as per defined rules
- Should be able to generate Data Records – (CDRs) and have exporting capabilities to other systems

There are multiple ways of integration of the solution with other systems is envisaged. These may be through Web Services, Message Queuing, File based or API based. The integration and data sharing mechanism may be either in Batch Mode or Needs basis (synchronous or asynchronous). Some of the key requirements of the interface/integration are mentioned below:

- Interface Definition
- Interface Owner
- Interface Type
- Interface Format
- Frequency
- Source System
- API/Service/Store Procedure
- Entitlement Service
- Consuming System
- Interface Layout (or) Schema

- Should have provision for exceptional scenarios
- Should have syntax details such as data type, length, mandatory/option, default values, range values etc.
- Error code should be defined for every validation or business rule
- Inputs and outputs should be defined
- Should be backward compatible to earlier datasets
- Data exchange should provide transactional assurance
- Response time and performance characteristics should be defined for data exchange
- The failover scenarios should be identified
- Data exchange should be auditable

Note: Bidder is free to proposed their own design to be meet the scope and SLA requirement

7.3 Security

Data exchange should abide by all laws on privacy and data protection Security Architecture. Proposed solution shall adhere to the guidelines & frameworks issued by GoUP/GoI from time-to-time for security for smart city solutions.

This section recommends the proposed security architecture aligning with the overarching architectural principles. The basic tenets of Smart City security architecture are the design controls that protect confidentiality, integrity and availability of information and services for all the stakeholders.

7.3.1 User Security and Monitoring Authentication & Authorization

A strong authentication mechanism should be considered to protect unauthorized access to the Smart City applications. Consider use of at least two of the following forms of authentication mechanism:

- Something you know, such as a password, PIN etc.
- Something you have, such as a smart card, hardware security token etc.

- Something you are, such as a fingerprint, a retinal scan, or other biometric methods

Levels of Authentication

Based on the security requirements the following levels of authentication should be evaluated.

- For applications handling sensitive data it is recommended that in the least one factor authentication key in the form of a password is essential. Strong password complexity rules should be enforced to ensure confidentiality and integrity of the data

- For applications handling highly sensitive data it is recommended that two factor authentication mechanisms should be considered. The first line of defense is the password conforming to the password complexity rules'. Along with the password next user has to provide a one-time password which varies for each session. One time passwords are valid for each session and it is not vulnerable to dictionary, phishing, interception and lots of other attacks. A counter synchronized One-Time Password (OTP) solution could be used for this purpose.

Authorization

Authorization of system users should be enforced by access controls. It is recommended to develop access control lists. Consider the following approach for developing access control list -

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

7.3.2 Data Security

Traditional Structured Enterprise Data

DSCL should protect Integrated Project information against unauthorized access, denial of service, and both intentional and accidental modification. Data security, audit controls and integrity must be ensured across the data life cycle management from creation, accessed, viewed, updated and when deleted (or inactivated). This provides a proactive way to build defense against possible security vulnerabilities and threats, allowing errors to be corrected and system misuse to be minimized.

The implications for adhering to an effective data security and integrity guideline related to the Project are the following –

- Data security policies and standards to be developed and adopted across Dehradun Smart City applications and stakeholders

- Data security controls to be put in place to restrict access to enterprise data based on roles and access privileges. Data audit logs should be maintained for audit trail purposes. Security controls will be able to be reviewed or audited through some qualitative or quantitative means for traceability and to ensure that risk is being maintained at acceptable levels.

- In order to adequately provide access to secured information, security needs must be identified and developed at the data level, not the application level. Database design must consider and incorporate data integrity requirements.

- Procedures for data sharing need to be established. Data integrity during data synchronization needs to be ensured across the enterprise.

- Audit Capabilities: The system provides for a system-wide audit control mechanism that works in conjunction with the RDBMS.

- Maintaining Date/Time Stamp and User Id: Every transaction, with a date and time and User ID, is captured. The system allows generating various audit reports for verification.

- Access Log: The DSCL Project should have extensive inbuilt security and access control mechanisms. Based on this, the system keeps track of the various functions accessed by any users.

Audit Trail & Audit Log

Audit trails or audit logs should be maintained. Log information is critical in identifying and tracking threats and compromises to the environment.

There are a number of devices and software that should be logged which include hardware & software based firewalls, web servers, authentication servers, central/domain controllers, database servers, mail servers, file servers, routers, DHCP servers etc.

It is essential to decide what activities and events should be logged. The events which ideally should be captured include

- Create, read, update and delete of confidential information;

- User authentication and authorization activities in the system, granting, modification or revoking of user access rights;

- Network or service configuration changes;

- Application process start up, shutdown or restart, abort, failure or abnormal terminations, failure of network services;

- Detection of suspicious activities such as from Intrusion Detection and Prevention system, anti- virus, anti-spyware systems etc.

7.3.3 Application Security

- Project must comply with the Application Security Plan and security guidelines of Government of India as applicable

- Secure coding guidelines should be followed. Secure coding guidelines should include controls against SQL injection, command injection, input validation, cross site scripting, directory traversal, buffer overflows, resource exhaustion attacks etc. OWASP Top 10 standard should be mapped in the secure coding guidelines to cover all major vulnerabilities. MSI has to propose WAF with L4 throughput of 3.5gbps.

- Validation checks should be incorporated into the application to detect any corruption of information through processing errors or deliberate acts.

- Data output from an application should be validated to ensure that the processing of stored information is correct and appropriate to the circumstances

- Should implement secure error handling practices in the application

- Project should have Role based access, encryption of user credentials. Application level security should be provided through leading practices and standards including the following:

o Prevent SQL Injection Vulnerabilities for attack on database

o Prevent XSS Vulnerabilities to extract user name password (Escape All Untrusted Data in HTML Contexts and Use Positive Input Validation)

o Secure Authentication and Session Management control functionality shall be provided through a Centralize Authentication and Session Management Controls and Protect Session IDs from XSS

o Prevent Security Misconfiguration Vulnerabilities (Automated scanners shall be used for detecting missing patches, misconfigurations, use of default accounts, unnecessary services, etc. maintain Audits for updates

o Prevent Insecure Cryptographic Storage Vulnerabilities (by encrypt off-site backups, ensure proper key storage and management to protect keys and passwords, using a strong algorithm)

o Prevent Failure to Restrict URL Access Vulnerabilities (By providing authentication and authorization for each sensitive page, use role-based authentication and authorization and make authentication and authorization policies configurable

o Prevent Insufficient Transport Layer Protection Vulnerabilities (enable SSL for all sensitive pages, set the secure flag on all sensitive cookies and secure backend connections

o Prevent Id Redirects and Forwards Vulnerabilities

o For effective prevention of SQL injection vulnerabilities, MSI should have monitoring feature of database activity on the network and should have reporting mechanism to restrict or allow the traffic based on defined policies.

7.3.4 Infrastructure Security

The following focused initiatives to discover and remedy security vulnerabilities of the IT systems of Dehradun Smart City should be considered to proactively prevent percolation of any threat vectors -

- Deploy anti-virus software to all workstations and servers to reduce the likelihood of security threats;
- Deploy perimeter security technologies e.g. enterprise firewalls to reduce the likelihood of any security threat;
- Deploy web content filtering solutions to prevent threats from compromised websites to help identify and block potentially risky web pages;
- Install enterprise-level e-mail anti-security software to reduce vulnerability to phishing and other e-mail security spams. This would check both incoming and outgoing messages to ensure that spam messages are not being transmitted if a system becomes compromised.
- Perform periodic scanning of the network to identify system level vulnerabilities
- Establish processes for viewing logs and alerts which are critical to identify and track threats and compromises to the environment. The granularity and level of logging must be configured to meet the security management requirements.
- Deploy technology to actively monitor and manage perimeter and internal information security.

- Deploy network Intrusion Detection System (IDS) on the perimeter and key points of the network and host IDS to critical systems. Establish process to tune, update, and monitor IDS information.
- In case of cloud deployment, cloud services can be disrupted by DDoS attacks or misconfiguration errors which have the potential to cascade across the cloud and disrupt the network, systems and storage hosting the cloud application.
- Deploy security automation techniques like automatic provisioning of firewall policies, privileged accounts, DNS, application identity etc.
- MSI should deploy DLP solution with Auto data classification and Auto policy generation without manual intervention.

Network Security for Smart Devices

The core principles of security for any smart device network rest on the three most important data security concerns of confidentiality, integrity and authentication. Hence the security for smart device networks should primarily focus on the protection of the data itself and network connections between the nodes. From a network perspective, following are to be considered for designing the smart devices network -

- Protection of fair access to communication channels (i.e. media access control)
- Concealing of physical location of the nodes
- Defence against malicious resource consumption, denial of service, node capturing and node injection
- Provision for secure routing to guard the network from the effects of bad nodes
- Protection of the mobile code

Smart devices have a triple role in most networks - data collectors, processors and traffic forwarders for other devices in the network. The typical attacks for which countermeasures are to be defined and implemented are: Radio Jamming, Nodes Reporting Wrong Data, Data Aggregation Attacks and Battery Attacks.

The following guidelines need to be considered for security enhancement of smart devices and their networks:

- Use of IP-based network for smart devices
- Use of Link Layer Security for password-based access control and encryption
- Protection of smart devices nodes behind a firewall for carrying out SSL-based application data transfer and mechanism to avoid distributed DoS attacks
- Public-key-based authentication of individual devices to the network and provisioning them for secure communications
- Conformance of the security solution to the standards of IETF, IEC and IEEE to ensure maximum security and interoperability, with support for the following commonly used protocols at a minimum - IPSec/IKE, SSH and SSL/TLS

7.4 Software Development Lifecycle Continuous Build

The DSCL Project should be highly modular and parallel development should be carried out for faster execution using industry's best Software Development Lifecycle practices. All

application modules within the same technology platform should follow a standardized build and deployment process.

A dedicated 'development / customization' environment should be proposed and setup. MSI must provision separate development and testing environment for application development and testing. Any change, modifications in any module must follow industry standard processes like change management, version control and release management in large and complex application development environment.

Application source code could be maintained in source control and could be broken up into a number of projects. Source control projects are created to abstract related set of modules or feature that can be independently included in another application.

It is a mandatory to create, update and maintain all relevant documentation throughout the contract duration. Also it should be ensured that a bug tracking toll is maintained for proper tracking of all bugs fixes as per various tests conducted on the application.

7.5 Quality Assurance

A thorough quality check is proposed for the DSCL Project and its modules, as per standard Software Development Life Cycle (SDLC). MSI is expected to lay down a robust Quality Assurance program for testing of the developed application for its functionality, performance and security before putting in production environment. The program must include an overall plan for testing and acceptance of system, in which specific methods and steps should be clearly indicated and approved by DSCL. MSI is required to incorporate all suggestions / feedback provided after the elaborate testing of the system, within a pre-defined, mutually agreed timeline. MSI must undertake the following:

- Outline the methodology that will be used for testing the system.
- Define the various levels or types of testing that will be performed for system.
- Provide necessary checklist/documentation that will be required for testing the system.
- Describe any technique that will be used for testing the system.
- Describe how the testing methodology will conform to the requirements of each of the functionalities and expected outcome.
- Indicate / demonstrate to DSCL that all applications installed in the system have been tested.

7.6 Performance and Load Testing

MSI is expected to implement performance and load testing with following features:

- Testing workload profiles and test scenarios based on the various functional requirements should be defined. Application as well as system resource utilization parameters that need to be monitored and captured for each run also needs to be defined.
- Should support application testing and API testing including HTTP(s), web services, mobile applications and different web 2.0 frameworks such as Ajax/Flex/HTML5.
- MSI should perform the load testing of DSCL Project for multiple workload profiles, multiple scenarios, and user loads to handle the envisaged users of the system.
- Different activities before load testing i.e. identification of work load profiles, scenarios,

information capturing report formats, creation of testing scripts, infrastructure detailing and workload profile should be prepared before the start of actual load testing exercise.

- Solution parameters needs to be tuned based on the analysis of the load testing reports. The tuning process could be iterative until the issues are closed. Multiple load runs needs to be executed for users to simulate different scenarios, such as peak load (year end, quarter end, etc.), load generation within the LAN, Load generation across WAN or mobile network simulator while introducing configurable latency/jitter/packet loss etc.
- Should eliminate manual data manipulation and enable ease of creating data-driven tests.
- Should provide capability to emulate true concurrent transactions.
- Should identify root cause of performance issues at application or code level. Include code performance analysis to quickly pinpoint component-level bottlenecks: Slowest classes and methods, most frequently called methods, most costly (aggregate time spent for each method), response time variance etc.
- Should allow selection of different network bandwidth such as analog modems, ISDN, DSL, or custom bandwidth.
- Should be able to monitor various system components e.g. Server (OS, Web, Application & Database) Monitoring, Network (between Client & Server) Delay Monitoring, Network Devices (Firewall, Switch & Router) Monitoring during the load test without having to install any data capturing agents on the monitored servers/components
- Should correlate response times and system performance metrics to provide quick insights in to root cause of performance issues.
- Reports on following parameters (but not limited to) such as transaction response time, transaction per second (Passed), user interface rendering time, transaction per second (Failed), web transaction breakdown graphs, hits per second, throughput, HTTP responses per Second, pages downloaded per second, system infrastructure performance metrics etc.
- Should provide End-to-End system performance analysis based on defined SLAs. Should monitor resource utilization including memory leakage, CPU overload and network overload. Should have the ability to split end-to-end response time for Network & Server(s) and provide drill-down capability to identify and isolate bottlenecks.

7.7 Annexure III- Common guidelines regarding compliance of systems/equipment

1. The specifications mentioned for various IT / Non-IT components are indicative requirements and should be treated for benchmarking purpose only. MSIs are required to undertake their own requirement analysis and may propose higher specifications that are better suited to the requirements.

2. In case of addition/update in number of license for the products, MSI is required to meet of technical specifications contained in the RFP and for the upward revisions and/or additions of licenses is required be made as part of change order and cost would be commensurate to the itemized rate approved at the LOI issuance.

3. Any manufacturer and product name mentioned in the Tender should not be treated as a recommendation of the manufacturer / product.

4. None of the IT / Non-IT equipment's proposed by MSI should be End of Life product. It is essential that the technical proposal is accompanied by the OEM certificate in the format given in Volume I of this Tender, where-in the OEM will certify that the product is not end of life product & shall support for at least 6 years from the date of Bid Submission.

5. All IT Components should support IPv4 and IPv6.

6. Technical Bid should be accompanied by OEM's product brochure / datasheet. MSIs should provide complete make, model, part numbers and sub-part numbers for all equipment/software quoted, in the Technical Bid.

7. MSIs should ensure complete warranty and support for all equipment from OEMs. All the back-to-back service agreements should be submitted along with the Technical Bid.

8. All equipment, parts should be original and new.

9. The user interface of the system should be a user friendly Graphical User Interface (GUI).

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

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

12. The Successful MSI should also propose the specifications of any additional servers / other hardware, if required for the system.

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

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

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

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

17. All the hardware and software supplied should be from the reputed Original Equipment Manufacturers (OEMs). DSCL reserves the right to ask replacement of any hardware / software if it is not from a reputed brand and conforms to all the requirements specified in the tender documents.

7.8 Annexure IV- Tentative List of Locations

A. ATCS – Junction Details.

S. No	Junction Name	No. of approaches
1	Clock Tower	3
2	Prince Chowk	4
3	Kwality Chowk	3
4	Kanak Chowk	4
5	Bhel Chowk	3
6	Nanys Bakery	4
7	DBS Chowk	3
8	Survey Chowk	5
9	Araghar Chowk	4
10	Railway Station Chowk	4
11	Tehsil Chowk	4
12	Ballupur Chowk	4
13	Yamuna Colony Chowk	3
14	Kishan Nagar Chowk	3
15	Dilaram Chowk	3
16	Balliwala Chowk	4
17	Lencidon Chowk	4
18	Buddha Park	4
19	Laal Pul Chowk	3
20	Niranjanpur Sabji Mandi Chowk	3
21	Shimla Bypass Chowk	3
22	ISBT Chowk	3
23	Gandhi Chowk	4
24	Saharanpur Chowk	4
25	City Heart Centre Chowk	3
26	Bindal Chowk	3
27	Aggarwal Filling Station	4
28	Dwarika Chowk	4
29	DAV Chowk	3
30	Near DBS(PG) college	4
31	Sri durga sweet shop	3
32	Near CMI hospital	3
33	Race course chowk	4
34	Masjid Huda	3
35	District & sessions court	4
36	St Francis church	3
37	Doon Hospital	5
38	Nehru Colony Junction	3
39	Rispana Junction	3

40	Saint Jude Chowk	4
41	Kargi Chowk	4
42	Dharampur Chowk	4
43	Sahasdhara Crossing	3
44	Kaulagarh Crossing	3
45	Saint Jude Chowk	3
46	Darshan Lal Chowk	4
47	FRI Gate	4
48	Vasant Vihar	3
49	ONGC Chowk	4

B. ITMS Locations:

S. No	Locations	Number Of Devices			
		System Type	Sensor Traffic/Speed	ANPR	RLVD (Context Camera)
1.	Ballupur chowk	RLVD	0	8	4
2.	Survey chowk	RLVD	0	9	5
3.	Budha park	RLVD	0	7	4
4.	Aaraghar (E.C Road)	RLVD	0	8	4
5.	Doon Hospital	RLVD	0	9	5
6.	Dwarika chowk	RLVD	0	8	4
7.	Kwality chowk	RLVD	0	6	3
8.	Chaudhari charan singh chowk	RLVD	0	8	4
9.	Yamuna colony	RLVD	0	6	3
10.	Tehsil chowk	RLVD	0	10	6
11.	Lalpul chowk	RLVD	0	8	4
12.	Sabji mandi chowk	RLVD	0	6	3
13.	Simla bypass chowk	RLVD	0	6	3
14.	CMI Hospital	RLVD	0	6	3
15.	Bindal tiraha	RLVD	0	6	3
16.	Mahamaya Maa Basundhara(Chakarata Road) Latitude & Longitude(30.34875, 77.865704)	Speed Detection System	2	4	0
17.	Dehradun Saharanpur Road near sahasakhand Commercial Check Post (30.262938, 77.9813992)	Speed Detection System	2	4	0

18.	Mussourie Road Just After Diversion (30.372885, 78.077526)	Speed Detection System	2	4	0
19.	Ring Road Near Commercial Tax Office (30.3013801, 78.0726966)	Speed Detection System	2	4	0
16.	Clock Tower	ANPR	6	12	0
17.	Nany's bakery chowk	ANPR	8	16	0
18.	Railway station chowk	ANPR	7	14	0
19.	Dilaram chowk	ANPR	6	12	0
20.	ISBT chowk	ANPR	6	12	0
21.	Saharanpur chowk	ANPR	6	12	0
22.	City heart center chowk	ANPR	6	12	0
23.	Race course chowk	ANPR	8	16	0

C. SMART CORRIDOR

S.N	Name Of The Road	Stretch Km	Start Point	End Point	Category	No. systems
1.	Chakrata Road	10	IMA	NIVH	Smart traffic sensors	20
					Average Speed	8
2.	E.C Road	5	Bhel chowk	Vidhan sabha	Smart traffic sensors	10
					Average Speed	3
3.	Ring Road	4	Beliver's Church	Maa Vaisano Devi Mandir	Smart traffic sensors	6
					Average Speed	3
4	Centralize Traffic Suit & Management centre					1

D. Wi-Fi location in city:

S. No.	City Wifi Locations
1	ISBT
2	Railway Station
3	Paltan Bazaar
4	Rajpur Road
5	EC Road
6	Chakrata Road
7	Clock Tower Area
8	Lansdowne Chowk
9	Doon Chowk
10	Tehsil Chowk
11	Gandhi Park
12	Arhat Bazaar
13	Gautam Buddha Park
14	Saharanpur Chowk
15	Ashley Hall
16	Survey Chowk
17	SP Traffic Office
18	Silver City
19	Dilaram Chowk
20	Dav College Area
21	Ballu Pur Chowk
22	Krishan Nagar Chowk
23	Balli wala Chowk
24	Majra mandi
25	Prince Chowk
26	Rispana Bridge
27	Vidhan Sabha
28	Dispensary Road
29	Outside All Major Mall (5 Nos)
30	In 30 Anganwadi Centers

E. CCTV Camera Locations:

S. No.	CCTV Camera Locations	Box	Dome	PTZ
1	Outside All Major Malls (5 nos)	5	5	1
2	Blind Turns Accident Prone Areas (5 Nos)	5		1
3	Paltan Bazaar	10		3
4	Kanwali road	4		1
5	Dav College Area	4		1

6	Near MDDA Complex	4		1
7	SP Traffic Office	4		1
8	Tilak Road	4		1
9	Curzon Road	4		1
10	Govind Garh	4		1
11	Kishan Nagar Chowk	4		1
12	Ballupur Chowk	4		1
13	Balliwala Chowk	4		1
14	Kamla Palace	4		1
15	Mazra Mandi	5		1
16	Railway Station	4		1
17	30 Anganwadi Centres	30	30	1
18	ISBT	4	4	1
19	Gandhi Park	4	4	1
20	Darshan Lal Chowk	4		1
21	RTO Office	4		1
22	Pacific Mall	2		1
23	Sai Baba Temple	4		1
24	GRD + Kothal Gate	5		1
25	DIT	5		1
26	EC Road	10		1
27	Rajpur Road	20		1
28	Chakrata Road	10		1

F. City Exit Points:

S. No.	City Entry/Exit Point	Box Camera
1	Daat Kali Mandir	1
2	Kothal Gate	1
3	Kilmadi Road	1
4	Maharana Pratap (Sports college Stadium)	1
5	Raipur	1
6	Chuna Bhatti	1
7	Salequi Chowk	1

8	Tea State	1
9	ITDA (IT-Park)	1
10	Gargi Chowk	1
11	Sapera Basti	1
12	Doiwala	1
13	Jogiwala	1
14	Laxman Sidh Mandir Check Post	1

G. Public Address System

S. No.	Public Address System
1	Dilaram Chowk
2	Clock Tower Area
3	Rispna Bridge
4	ISBT
5	Asharodi
6	Ballupur Chowk
7	Shimla Bypass Chowk
8	Kulhal
9	Niranjanpur Mandi

7.9 Annexure V- Bill of Material (BOM)

Bill of Material

The Bidder shall quote the prices of CAPEX and OPEX in the price bid BOQ as per the items given below

S.No	Line Item	Unit of Measurement	Indicative Quantity	Complied/Not Complied
Data Center				
1	Integrated Command and Control software and solution	Set	1	
2	Enterprise Service Bus with API Integration	Set	1	
3	Internet Router	Nos.	2	
4	Data Center Next Generation Firewall	Nos.	2	
5	Internet Firewall	Nos.	2	
6	Core Router	Nos.	2	
7	Core Switch	Nos.	2	
8	TOR/Distribution Switch	Nos.	4	
9	Anti-APT	Nos.	2	
10	End Point Detection and Response	Set	1	
11	SIEM	Set	1	
12	Server Load balancer	Nos.	2	
13	Link Load Balancer	Nos.	2	
14	DDoS	Nos.	2	
15	WAF	Nos.	2	
16	Key Management	Set	1	
17	Data Security	Set	1	
18	Secure Email Gateway	Set	1	
19	Secure Web Gateway	Set	1	
20	WebSite and File Monitoring Solution	Set	1	
21	Secure Communication	Set	1	
22	EMS	Set	1	
23	Endpoint Security	Set	1	
24	HCI infrastructure	Set	As per requirement	
25	Non-HCI infrastructure	Set	As per requirement	

26	Video Wall, Controller and Management Software	Set	1	
27	Video Conferencing solution	Set	1	
28	IP Telephony with Citizen Centric Services	Set	1	
29	Analytics VMS and Video Analytics	Set	1	
30	Network Video Recorder	Set	1	
31	Integrated Data Center Infrastructure	Set	1	
32	10 KVA UPS	Nos.	2	
33	Site Preparation Cost	Lumpsum	1	
Field Equipment				
34	DCPS	Nos.	As per requirement	
35	Field Junction Box	Nos.	As per requirement	
36	Camera Poles	Nos.	As per requirement	
Other Items				
37	Workstation	Nos.	30	
38	Desktop for Help Desk	Nos.	5	
39	PAS	Nos.	5	
40	Multifunctional Device	Nos.	2	
Disaster Recovery				
41	DR as a service with 50 % Capacity of DC	Lumpsum	1	
42	DR Management Software	Set	1	
42 a	DC - DR bandwidth	Set	1	
ATCS				
43	ATCS Software and Solution	Set	1	
44	ATCS Traffic signal controller	Nos.	49	
45	4D Radar traffic Detector	Nos.	174	
46	Countdown timer	Nos.	180	
47	Traffic Light Aspects – Red	Nos.	515	
48	Traffic Light Aspects – Green	Nos.	1030	
49	Traffic Light Aspects – Amber	Nos.	515	

50	Pedestrian countdown timer with red and green lamp	Nos.	360	
51	Disabled Friendly Audio Tactile Device	Nos.	360	
52	Cantilever pole with mounting structure and junction box along foundation (Min Qty. MSI has to do Survey)	Nos.	115	
53	Straight pole with Mounting Structure with poles, junction boxes along with foundation (Min Qty MSI has to do Survey)	Nos.	160	
54	Network Switch Ruggedized, and civil work	Nos.	49	
ITMS				
55	ITMS - ANPR Software and Solution	Set	1	
56	ITMS - RLVD Software and solution	Set	1	
57	ITMS - SVD (Instant and Average Speed) software and solution	Set	1	
58	ITMS – TARS & E Challan solution	Set	1	
59	ITMS - PA Software and solution	Set	1	
60	ITMS - ECB management software and solution	Set	1	
61	ITMS - Variable Message Software and solution	Set	1	
62	ITMS – Traffic Monitoring & Management System	Set	1	
63	Smart Traffic Sensor A	Nos	28	
64	ANPR Systems for critical sites in the city	Nos	30	
65	Traffic Sensors B for Smart road and mobility	Nos	40	
RLVD				
66	Red Light Violation Detection (RLVD) sensors	Per leg	58	
67	Camera with ANPR capability	No.	209	

68	Local processing unit	No.	35	
69	Mounting structure with pole, junction boxes etc.	Set	As per requirement	
70	Network Switch Ruggedized	No.	As per requirement	
	SVD			
71	Speed Detection System for covering 2 lanes in one direction with complete subcomponents including ANPR camera, sensors, wide angle evidence camera, IR illuminator, non-intrusive speed	Instant Speed No of Lanes	60	
72	SVD	Average Speed No of lanes	20	
73	SVD for dangerous junction	Lumpsump	20	
74	Sensor, with cabling & mounting	Lumpsump	As per requirement	
75	infrastructure as required	Lumpsump	As per requirement	
Surveillance System				
76	Outdoor Fixed Box Camera + IR Illuminator	No.	204	
77	Bullet Cameras + IR Illuminator	No.	150	
78	Outdoor PTZ Camera + IR Illuminator	No.	35	
79	Dome Cameras + IR Illuminator	No.	40	
80	ANPR Camera for Borders	No.	28	
81	Hand held units for E challan & TARS	Nos	150	
PA System				
82	Public Address System – IP based PA with speakers	No.	24	
83	UPS (required capacity)	No.	As per requirement	
84	Mounting structures with pole etc.	No.	As per requirement	

	Variable Message Sign			
85	VMS board including VMS controller size 3000mm*1500mm*200 mm (minimum) with complete hardware and accessories as required + Mounting structure for VMS including UPS facility as per specifications	No.	50	
86	UPS (required capacity)	No.	As per requirement	
87	Mounting structures with pole etc.	No.	As per requirement	
ECB				
88	ECB system	No.	35	
89	UPS (required capacity)	No.	As per requirement	
90	Mounting structure with pole etc.	No.	As per requirement	
91	Junction boxes for ITMS solution	No.	As per requirement	
92	Power cables	Meter	As per requirement	
Environmental Sensors				
93	Environment sensors	No.	50	
Last Mile Connectivity and Bandwidth				
94	24 Core Optical Cable based last mile connectivity	As required to cover pan city	As required to cover pan city	
95	Aggregate bandwidth at DC	As required to cover pan city	As required to cover pan city	
96	Leased Circuit Bandwidth	As required to cover pan city	As required to cover pan city	
97	Helpdesk			
98	Head Set	No.	5	
99	Voice Logger	No.	1	
100	Soft telephone	No.	5	

101	Desktops	No.	5	
102	Officer Furniture and Revolving Chair	Lot	5	
City Wi-Fi				
103	Access Point	No's	300	
104	Wi-fi Management/Controller	No's	As per requirement	
105	Network Switch Ruggedized	No.	As per requirement	
106	Junction Box	No.	As per requirement	
107	Online UPS – 1 KVA (in case bidder proposes solar power, required items should be mentioned in the technical proposal)	No.	As per requirement	
City Portal				
108	City Portal	Set	1	
109	Mobile Application	Set	1	
110	Enterprise GIS	Unit	1	
Other Software				
111	Enterprise database	Set	1	
112	ERP	Set	1	
113	Backup Software	Set	1	
114	Work-Flow and DMS solution	Set	1	
115	Directory Services	set	As per requirement	
Power Backup				
116	Diesel Genset 250 KV	Unit	1	
Manpower				
117	Manpower as per the RFP	No.	1	
Solid Waste Management				
118	RFID Reader (With Controller)	No	30	
119	RFID Tags	No	25000	
120	Application Server Supply &Installation for data centre hosting	Set	1	
121	Database Server Supply & Installation for data centre hosting	Set	1	

122	RDBMS Supply & Installation for data centre hosting	Set	1	
123	Bin Level Sensors	No	500	
124	Solution Cost including License cost if any	Set	1	
125	VTMS (Vehicle Tracking and Monitoring system) solution cost including License cost if any	Lot	1	
126	GPS Devices (for new Vehicles)	Nos.	30	
127	Citizens' App Development & integration Cost	Set	1	
128	Biometric Face Recognition Device	No	4	
Transit Management System (VTS)				
129	GPS/OBU for Buses	Nos	1	
130	GPS for E-Rickshaws	Nos	1	
131	4G (or above) enabled SIM Cards	Nos	1	
132	Any other Hardware or Software required to meet the requirements (Bidder to list individual items and provide costing).	Nos	1	
133	Transit Management System Software	Set	1	
Smart Bus Shelter/ Depots				
134	19" size of PIS display at Bus Shelters/stops + UPS	Nos	72	
135	55" size of PIS display at Bus Depots + UPS	Nos	2	
136	Fixed Box Camera	Nos	72	
137	ECB/ Panic Button	Nos	72	
138	VMD board (at Bus Shelters including VMS controller) size 960mm*960mm*200 mm (minimum) with complete hardware and accessories as required including UPS facility as per specifications	Nos	72	
139	4G (or above) enabled SIM Cards	Nos	72	

140	Any other equipment/solution if required for completion of the scope of work	Lumpsum	1	

Note: The O&M for the Data Centre shall be taken care by the ITDA Department from the first day after the successful establishment of Data Centre by the MSI. The MSI has to quote the prices of OPEX in the price bid BOQ exclusive of the O&M prices for the data centre.