Selection of Master System Integrator (MSI) for Implementation of Command Control and Communication Centre (C4) under Smart City Mission in Ranchi

VOLUME -2: Terms & References (TOR)

Tender Notice No: RSCCL/C4/RFP-58/2017/58

Issue Date: October 12, 2017

E-Procurement Reference: RSCCL/CCCC/2017/01

Ranchi Smart City Corporation Ltd. (RSCCL)
Urban Development and Housing Department
Government of Jharkhand

Selection of Master System Integrator (MSI) for Implementation of Command Control and Communication Centre (C4) under Smart City Mission in Ranchi

Disclaimer

Ranchi Smart City Proposed (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). Ranchi SCP proposes served smart solution in ADB and cross pan-city providing various Smart feature/infrastructure.

To implement Smart City projects in Ranchi, Ranchi Municipal Corporation and Jharkhand Urban Development and Housing Department has formed a SPV called Ranchi Smart City Development Ltd. (RSCCL).

The RSCCL has prepared this Request for Proposals (RFP) for the "Request for Proposals for Selection of Master System Integrator for Implementation of Command Control and Communication Centre for Ranchi City". 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 Control and Communication Centre. RSCCL has taken due care in preparation of information contained herein and believes it to be accurate. However, neither RSCCL 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 RSCCL 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 RSCCL any kind of error, misprint, inaccuracy, or omission.

RSCCL 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.

Selection of Master System Integrator (MSI) for Implementation of Command Control and Communication Centre (C4) under Smart City Mission in Ranchi

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
GIS	Geographical Information Systems
GPS	Global Positioning System
GSM	Global System for Mobile Communication
GST	Goods and Services Tax
CCCC	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
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
RLVD	Red Light Violation Detection
RSCCL	Ranchi Smart City Corporation 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

Table of Contents

1 Introduction

1.1 Project Background

One of the primary objectives of Ranchi under its smart city mission is to enhance the safety and security, improve efficiency of city administration and promote a better quality of life for residents. In order to achieve these objectives, Ranchi desires to foster the development of a robust ICT infrastructure that supports digital applications and ensures seamless steady state operations, traffic management, emergency response mechanisms and real time tracking of services and vital city metrics throughout the city. RSSCL is considering the appointment of a MSI to set up these priority initiatives identified under the Smart City mission which will include Command Control and Communication Centre (CCCC) and Smart Elements; including Intelligent Traffic Management System (ITMS), City Wi-Fi, environment sensors, smart parking etc.

1.2 Project Objectives

The key objective of this project is to establish a collaborative framework where input from different smart solutions implemented by RSCCL, 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. Following are the key outcomes expected to be achieved by the proposed interventions:

a. Improved visualization of ambient situation 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. Integration with all existing and future services as identified by Ranchi Smart City Corporation limited (RSCCL) in the city including but not limited to (with provision for future scalability):
    - Video Surveillance System implemented by Police Department
    - Smart Lighting
    - ICT Enabled Solid Waste Management
    - Intelligent Transportation System
    - E-Challan System
    - Public Bike Sharing
    - Smart Water Supply System
    - Smart Education
    - Smart Health Management System
    - BRTS/MRTS and City Bus Services

1.3 Purpose of this RFP

The purpose of this tender is for the Ranchi Smart City Corporation Limited (RSCCL) to enter into a contract with a qualified firm for the Supply, Installation, Integration, Commissioning, Operations and Maintenance of integrated solutions to support the

command, control and communication centre initiative for smart city initiative of Ranchi. RSCCL is looking to engage a Master Service Integrator -

- Who brings strong implementation experience in smart city integration and operations through integrated, multi-agency coordination platform
- Who can develop Standard Operating Procedures for the various components of the project
- 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 has a quality control plan in place to demonstrate that all equipment is tested and passed prior to shipping
- Who is capable of providing 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 will strongly build capacity of various stakeholders for efficient operations and management of the proposed solutions

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

2 Project Overview and Components

Key foundation components for Ranchi Smart City considered for this RFP are:

#	Component	Geographical Scope
1.	Network Backbone	Pan city including ABD area
2.	Command Control & Communication Centre	Located centrally at one location
3.	Data Centre and DR Site	- Smart and energy efficient Data Centre located centrally with Command Control & Communication Centre - Cloud DR set-up
4.	ITMS	
a.	ATCS system	40 locations
b.	Surveillance system (Fixed and PTZ)	30 locations
c.	ANPR system	50 locations
d.	SVD system	10 locations
e.	RLVD system	30 locations
f.	TAR system	15 locations
5.	Variable Message Sign Board	50 locations
6.	Public Address System	50 locations
7.	Emergency Call Box (ECB) System	50 locations
8.	City Wi-Fi	43 locations spread across city
9.	Smart Parking	Pan city
10.	Environmental Monitoring System	10 locations spread across city
11.	Enterprise GIS	Pan city with multiple layers
12.	Web Portal & Mobile App	City portal and mobile app to disseminate information, infographics and service delivery through integration with stakeholder departments

2.1 Components & Services Scope Overview

The selected MSI shall ensure the successful implementation of the proposed C4 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 RSCCL 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 systems, street infrastructure and 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, gap 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 RSCCL

2. Design, Supply, Installation, Testing and Commissioning of the following primary components:
   a) Command Control & Communication Centre (C4)
   b) Smart Data Centre within C4 Building
   c) Cloud Data Centre for DR (Hosted in data centre of any MEITY empanelled Cloud Service Provider)
   d) Smart Parking Management System
   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
      ▪ 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

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

3. Integration with following listed existing and proposed system ICT systems within Ranchi ICT landscape (but not limited to)
   ▪ Video Surveillance System
   ▪ Smart Lighting
   ▪ ICT Enabled Solid Waste Management
   ▪ Intelligent Transportation System
   ▪ E-Challan System

- Public Bike Sharing
- Smart Water Supply System
- Smart Education
- Smart Health Management System
- BRTS/MRTS and City Bus Services

4. Data Centre: Provisioning of Hardware, Network and Software Infrastructure which includes design, supply, installation and commissioning of ICT Infrastructure at the Command Control and Communication 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) Provisioning of city wide network infrastructure on fibre optic underground/RF etc. on lease to RSSCL
      1. Between field devices (sensors, cameras, Wi-Fi etc.) & Data Centre
      2. Between Data Centre & Command Control Centre (located in the same building)
      3. Between server room & viewing/monitoring centre
   b) Connectivity between DC & proposed DR
   c) Integration with proposed network for Video Surveillance Project and JharNet 2.0 network
   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 impacting overall network performance.

6. Capacity Building for RSCCL and any other department which includes preparation of operational manuals, training documents and capacity building support, including:
   a) Training of city authorities, operators and other stakeholders on operationalization of the system
   b) Support during execution of acceptance testing
   c) Preparation and implementation of the information security policy, including policies on backup and redundancy plan
   d) Preparation of revised KPIs for performance monitoring of various urban utilities monitored through the system envisaged to be implemented
   e) Developing standard operating procedures for operations management and other services to be rendered by CCCC

f) Preparation of system documents, user manuals, performance manuals, Operation manual etc.

7. Operations and Maintenance

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

2.2 Component Architecture

Indicative architecture of the components envisaged under the ""Integrated Command Control and Communication Centre" is as given below. Please note that this component architecture is indicative in nature and is given in the RFP to bring clarity to prospective bidders on the overall scope of project and its intended use. MSI shall carry out the detail requirement analysis and finalize technical architecture in consultation with authority and its consultants. As per the figure below, the architecture of the complete network of smart elements is as follows.
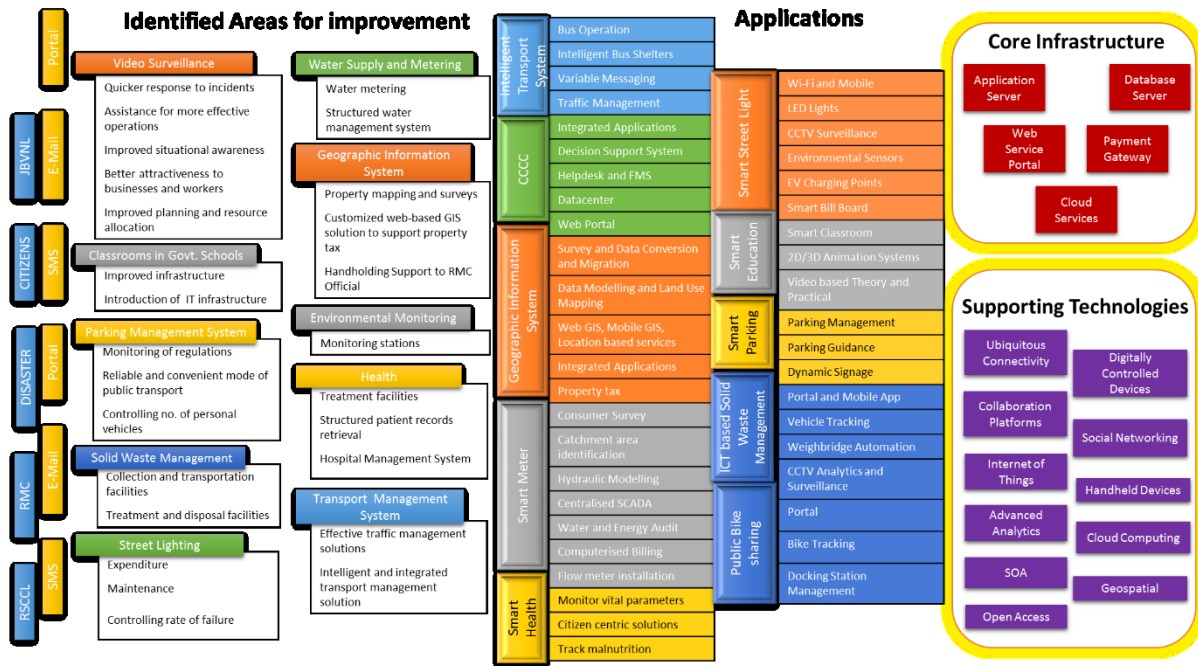
a) Sensor and actuator layer

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. Ranchi 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 Layer (Controllers)

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 CCCC.

c) Network 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. 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) 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 RSCCL. 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 Ranchi , etc.) and non-government agencies.

f) Service delivery and consumption 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.

g) Control Units & Command Centre Layer

The command Centre and control units will enable citizens and administrators alike to get a holistic view of city conditions. Such control units will take shape of either an exhaustive command Centre or control applications which can be viewed over a web browser or available in form of a mobile application. The implementation vendor will have to develop a command Centre at a site location determined by RSCCL and web/ mobile based viewing tools for understanding

the ambient city conditions.

h) Security Layer

As ambient conditions, actuators and display devices are now connected through a network, security of the entire system becomes of paramount significance 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 eGovernance 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

2.3 Assessment and Site Survey for finalization of detailed technical architecture and project plan

After signing of contract, the Systems Integrator needs to deploy local team (based out of Ranchi) proposed for the project and ensure that a Project Inception Report is submitted to RSCCL 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 / learning 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 As-Is study of the existing infrastructure of traffic junctions/intersections (identified for ITMS), Parking, Wi-Fi and City Network backbone etc. 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/ Government of Jharkhand

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

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. Location of Network Provider's Point of Presence (PoP)

8. Design of Cables, Ducts routing, digging and trenching

9. 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:

1. State-of-the-art: Use of the latest & best available standards to avoid locking in obsolescent technologies

2. Saleable: Flexible; standards recognize local conditions with a wide range of ITMS

devices and communication channel capabilities

3. Scalability - Important technical components of the architecture must support scalability to provide continuous growth to meet the growing demand of the Ranchi city. The system should also support vertical and horizontal scalability so that depending on changing requirements from time to time, the system may be scaled upwards. There must not be any system imposed restrictions on the upward scalability in number of field devices. Main technological components requiring scalability are storage, bandwidth, computing performance (IT Infrastructure), and software / application performance

4. 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.

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

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

7. Security - The architecture must adopt an end-to-end security model that protects data and the infrastructure from malicious attacks, theft, natural disasters etc. Cyber-security guidelines issued by MoUD for smart cities (K-15016/61/2016-SC-1) would need to be adhered to by MSI. MSI must make provisions for security of field equipment as well as protection of the software system from hackers and other threats. Using Firewalls and Intrusion detection systems such attacks and theft should be controlled and well supported (and implemented) with the security policy. The virus and worms attacks should be well defended with gateway level Anti-virus system, along with workstation level anti-virus mechanism. Furthermore, all the system logs should be properly stored & archived for future analysis and forensics whenever desired. RSCCL may carry out the Security Audit of the entire system post acceptance / operationalization through a Third Party Auditor (TPA) if required. The following guidelines need to be observed for security:

   a. 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. Ensuring that the security logs are analyzed proactively, and the traffic and data patterns analyzed for proactive threat hunting. Ensure that if a security incident occurs, it is detected, contained and mitigated in a fast and effective manner so as to prevent the spread of the infection.

   b. Access controls must be provided to ensure that the system is not tampered or modified by the system operators. Ensuring that the smart city services are always available to the users/ citizens, and are not impacted by any DDoS attacks.

   c. Implement data security to allow for changes in technology and business needs.

d. 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.

e. 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.

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

g. 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.

h. 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.

i. 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.

j. 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

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

l. 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.

m. 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.

n. All the sensors in the Smart city should connect to a completely separate network.

o. 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.

p. Security Information and Event Management (SIEM) monitoring on all Smart

City networks, devices and sensors to identify malicious traffic.

8. 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

9. Interoperability - The proposed system should adhere to the interoperable standards published by GoI/GoJ from time-to-time.

10. Open Standards –System should be fully complaint with open standards and protocols as published by GoI/GoJ from time-to-time.

11. Convergence - RSCCL 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, RSCCL has envisaged to create a state of the art infrastructure and services for the citizens of Ranchi, 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 RSCCL. The procedure for utilization of the infrastructure will be mutually agreed between the RSCCL 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 RSCCL. 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 RSCCL.

Site Clearance obligations & other relevant permissions –

2.3.1 Commencement of Works

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 RSCCL 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 RSCCL before executing the plan

2.3.2 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 which are proposed and required under the scope of the ITMS. The dismantled infrastructure shall be delivered at the RSCCL designated location without damage at no extra cost.

2.3.3 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 RSCCL guidelines.

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

2.3.4   Electrical works and power supply

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

2.3.5   Lightning-proof measures

MSI shall comply with lightning-protection and anti –interference measures for system structure, equipment type selection, equipment earthing, power, signal cables laying. MSI shall describe the planned lightning-protection and anti –interference measures in the As-Is report. Corresponding lightning arrester shall be erected for the entrance cables of power line, video line, data transmission cables. All crates shall have firm, durable shell. Shell shall have dustproof, antifouling, waterproof function & should be capable to bear certain mechanical external force. Signal separation of low and high frequency; equipment's protective field shall be connected with its own public equal power bodies; small size/equipment signal lightning arrester shall be erected before the 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.

2.3.6   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. RSCCL 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

2.3.7 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 RSCCL 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.

2.3.8 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.

2.4 Design, Supply, Installation & Commissioning of the Field Equipment
The scope includes supply, installation, commissioning and Customization (as required) of various field systems which include Adaptive Traffic Control System (ATCS) at Traffic

Junctions, Traffic Cameras, ANPR Cameras, PA System, ECB System, Variable Message Signs, Red Light Violation Detection system, Speed Violation Detection System, Traffic Violation cameras, Traffic Accident Recording System, Wi-Fi system, devices for Smart parking solution and other IT infrastructure required for successful operation of the application modules.

Based on the approved Survey report, MSI will undertake the system configuration and customization in line with the changed, improved or specific requirements of project including:

1. The implementation methodology and approach must be based on the global best practices in-order to meet the defined Service Levels during the operation.

2. Best efforts have been made to define major functionalities for each sub- system of solution. However, MSI should not limit its offerings to the functionalities proposed in this RFP and is suggested to propose any functionality over and above what has already been given in this tender.

3. MSI shall design the field level equipment architecture to ensure maximum optimization of network equipment, poles, cantilever, and mounting infrastructures, power supply equipment including, electric meters and junction boxes.

4. Finally approved/accepted solution for each component of C4 systems shall be accompanied with "System Configuration" document and the same should be referenced for installation of systems at Junctions that are identified within the scope of this project.

5. MSI shall be required to submit a detailed installation report post installation of all the equipment at approved locations. The report shall be utilized during the acceptance testing period of the project to verify the actual quantity of the equipment supplied and commissioned under the project.

6. MSI shall be responsible for obtaining all permits and approvals necessary to install the ITMS systems components as per the approved design. RSCCL would also extend all the necessary support.

Indicative list of equipment required in the field to operationalize this project are mentioned below -

1. Cameras, traffic lights, pedestrian signals etc. for ITMS
2. Sensors and cameras for smart parking
3. Display boards for cameras
4. Wi-Fi APs
5. Junction boxes, poles etc.
6. Variable message boards
7. Environment sensors
8. Emergency call box
9. Solar panel with batteries (if the bidder proposes alternate power source for field equipment)

2.5 Design, Supply, Installation and Commissioning of Office Interior Spaces, IT Infrastructure at CCCC & Data Centre

2.5.1 Office Interior Spaces and IT Infrastructure

1. It is proposed that MSI shall provide the IT hardware infrastructure at the DC for successful operations of the systems. The CCCC, Office Space and Smart DC has been envisaged to be established in an approximate area of 20000 Square Feet at New Smart City Offices, Ranchi. MSI has to ensure that redundancy is provided for all the key components to ensure that no single point of failure affects the performance of the overall system. It will be MSI's responsibility to:

   a. Supply, Installation and Commissioning of IT Infrastructure including site preparation in CCCC. MSI shall also develop the office interior spaces as per the department requirements.

   b. MSI shall also develop the office interior spaces as per the department requirements and supply TV screens, workstations, IP Phones, network equipment, and required accessories including furniture as needed.

   c. Data Centre Infrastructure and provisioning of DR on cloud

      i. Data Centre developed by MSI should be as per Telecommunications Infrastructure Standard for Data Centre with Tier 2 rating

      ii. MSI shall provide system integration services to customize and integrate the applications procured through the project. The applications proposed by MSI should have open APIs and should be able to integrate and share the data with other third party systems already available or coming up in the near future.

      iii. As part of preparing the final bill of material for the CCCC, data center and Office spaces, the successful MSI will be required to list all passive & active components required in the data center

2. The bill of material proposed by the successful MSI will be approved by RSCCL for its supply and installation. Indicative IT Infrastructure to be commissioned as part of the System at Data Centre are as under:

   a. Servers (inclusive of OS) - Application Servers, Web server, Database Server, Video Recording Server, Video Management Server, Enterprise Backup Server, Domain Controller, Failover Servers for application and Recording Servers etc.

   b. Application & System Software (with necessary customization) – Adaptive Traffic Control System application, Video Management System application, ANPR application, Red Light Violation Detection application, Speed Violation Detection application, Variable message Sign Board application, PA System application, ECB System application, Traffic Violation cameras application, Parking Management system, Environmental sensors, Enterprise GIS, RDBMS (as required), Anti-virus Software, EMS software etc.

   c. Primary Storage Solution, Storage & Tape Management Solution

   d. Network equipment: Switches, Routers etc.

   e. KVM Switches

      f.   Online UPS (60 min backup on full load for IT systems)

  b.   Electrical and Network Cabling and Necessary LED Illumination Devices for approximately 20000 Square feet area

    a.   Cooling, Humidity and Anti Rodent Sensors

    b.   Building Management Systems

    c.   Biometric Security

    d.   All required Passive Components

    e.   Any other Server/ Equipment/Device/ Component/ Application required to the cater to the scope of work mentioned in this

3. The above are only indicative requirements of IT & Non-IT Infrastructure requirements at DC. The exact quantity and requirement shall be proposed as part of the technical proposal of MSI.

4. MSI shall prepare the overall data center hosting & their operational plan for this project. The plan shall comprise of deployment of all the equipment required under the project. The implementation roll-out plan for hosting of the data center shall be approved by RSCCL. The detailed plan shall be also comprise of the scalability, expandability and security that such data center will implement under this project.

5. MSI shall also establish a state of the art CCCC, the key components of the CCCC will be as follows:

    a.   Video Wall system

    b.   Operator workstations

    c.   IP Phones

    d.   Audio & Video conferencing units

    e.   Active Networking Components (Switches, Routers)

    f.   Passive Networking Components

    g.   Office Workstations

    h.   UPS (30 min backup on full load)

    i.   Furniture and fixtures

6. MSI shall be required to submit a detailed installation report post installation of all the equipment at approved locations. The report shall be utilized during the acceptance testing period of the project to verify the actual quantity of the equipment supplied and commissioned under the project.

2.5.2 Non-IT Requirements & Specifications

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.

2.5.2.1 Civil and Architectural Work

#	Description
A.	**False Ceiling**
1	Providing and fixing 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.
2	Providing and fixing 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.
B.	**Furniture and Fixture**
1	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 French 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.
2	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 French polish
3	Cabin table of min. depth 2' made with 1.5mm thick laminate of standard make over 19mm thick commercial board complete with wooden beading including cutting holes & fixing of cable manager etc. complete with French polish.
4	Providing, making & fixing 6" high laminated strip using 1.5mm thick laminate over 10mm thick commercial board on all vertical surface in the entire server & ancillary areas including
5	Low height partition, brick wall, partition wall, cladding etc. complete with French polish in all respect.
6	Providing, making & fixing 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.
C.	**Partitions (wherever required as per approved drawing)**
1	Providing and fixing in position 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 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

#	Description
	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.
2	With glazing including the framework of 4" x 2" powder coated aluminium section complete (in areas like partition between server room & other auxiliary areas).
3	Providing & fixing Fire Rated Wire Glass minimum 6 mm thick for all glazing in the partition wall complete. (External windows not included in this).
4	All doors should be minimum 1200 mm (4 ft.) wide.
D.	**Flooring (wherever required as per approved drawing)**
1	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.
2	MSI shall ensure the following features and parameters are
	considered while designing and commissioning the raised floor: ▪ Point of Load (PoL) shall be considered 20% more than the actual load ▪ Uniform Distribution Load shall be calculated according to the final Point of Load ▪ Noise-proof ▪ Fireproof ▪ Maintenance window for easy access to under the raised floor ▪ Separate electrical and data cable tray under the raised floor ▪ Face of floor tiles shall conform to the aesthetic part of the approved design
3	MSI shall perform load test and noise test of the constructed raised floor.
4	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.
E.	**Air Conditioning and Natural Convection**
1	For Data Center - Precision 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. The task of MSI shall include (but not limited to): ▪ Connecting the indoor unit with the mains electrical point ▪ Connecting indoor and outdoor units mechanically (with insulated copper piping) ▪ Connecting indoor and outdoor unit electrically
2	Comfort Air Conditioning at Command Center and other areas ▪ Cooling Capacity as per the requirements at each of the control rooms ▪ Compressor – Hermetically Sealed Scroll Type

#	Description
	▪ Refrigerant – R 22 Type ▪ Power Supply – Three Phase, 380-415 V, 50 Hz ▪ Air Flow Rate – minimum 19 cu m / min ▪ Noise Level - < 50 dB ▪ Operation – Remote Control
	Air conditioner shall be linked to secondary power supply as well to prevent them from shutting down in case of power outage
F.	**Painting**
1	Providing and applying 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.
2	For all vertical Plain surface.
3	For fire line gyp-board ceiling.
4	Providing and laying POP punning over cement plaster in perfect line and level with thickness of 10 - 12 mm including making good chases, grooves, edge banding, scaffolding pockets etc.
5	Applying approved fire retardant coating on all vertical surfaces, furniture etc. as per manufacturer's specification.

2.5.2.2 PVC conduit

#	Description
1.	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.
2.	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.
3.	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.
4.	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.
5.	Cables shall not be drawn into conduits until the conduit system is erected, firmly fixed and cleaned out. Not more than two right angle bends or the equivalent shall be permitted between draw and junction boxes. Bending radius shall comply with I.E.E regulations for PVC pipes.
6.	Conduit concealed in the ceiling slab shall run parallel to walls and beams and conduit concealed in the walls shall run vertical or horizontal.
7.	The chase in the wall required in the recessed conduit system shall be neatly made and shall be of angle dimensions to permit the conduit to be fixed in the manner desired. Conduit in chase shall be hold by steel hooks of approved design of 60cm

#	Description
	Centre the chases shall be filled up neatly after erection of conduit and brought to the original finish of the wall with cement concrete mixture 1:3:6 using 6mm thick stone aggregate and course sand.

2.5.2.3 Wiring

#	Description
1.	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. They shall be stranded copper conductors with thermoplastic insulation of 650 / 1100 volts grade. Colour code for wiring shall be followed.
2.	Looping system of wring shall be used, wires shall not be jointed. No reduction of strands is permitted at terminations.
3.	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 used for sub main, sub circuit wiring the ferrules shall be provided at both end of each sub main and sub-circuit.
4.	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.
5.	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.
6.	All splicing shall be done by means of terminal blocks or connectors and no twisting connection between conductors shall be allowed.
7.	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.
8.	All power sockets shall be piano type with associate's switch of same capacity. Switch and socket shall be enclosed in a M. S. sheet steel enclosure with the operating knob projecting. Entire assembly shall be suitable for wall mounting with Bakelite be connected on the live wire and neutrals of each circuit shall be continuous everywhere having no fuse or switch installed in the line excepting at the main panels and boards. Each power plug shall be connected to each separate and individual circuit unless specified otherwise. The power wiring shall be kept separate and distinct from lighting and fan wiring. Switch and socket for light and power shall be separate units and not combined one.
9.	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.

2.5.2.4   Cable Work

#	Description
1.	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
2.	All cables will be identified close to their termination point by cable number as per circuit schedule. Cable numbers will be punched on 2mm thick aluminium strips and securely fastened to the. In case of control cables all covers shall be identified by their wire numbers by means of PVC ferrules. 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.
3.	Each section of the rising mains shall be provided with suitable wall straps so that same the can be mounted on the wall.
4.	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.
5.	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.
6.	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.

2.5.2.5   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.

#	Description	Bidder Compliance (Yes/No/)
A.	System Description	
1	The Fire alarm system shall be an automatic 1 ton (e.g. 8) zone single loop addressable fire detection and alarm system, utilizing conventional detection and alarm sounders.	
2	Detection shall be by means of automatic heat and smoke detectors located throughout the Control Room (ceiling, false floor and other appropriate areas where fire can take place) with break glass units on escape routes and exits.	
B.	Control and Indicating Component	

#	Description	Bidder Compliance (Yes/No/)
1	The control panel shall be a microprocessor based single loop addressable unit, designed and manufactured to the requirements of EN54 Part 2 for the control and indicating component and EN54 Part 4 for the internal power supply.	
2	All controls of the system shall be via the control panel only.	
3	The system status shall be made available via panel mounted LEDs and a backlit 8 line x 40-character alphanumeric liquid crystal display.	
4	All system controls and programming will be accessed via an alphanumeric keypad. The control panel will incorporate form fill menu driven fields for data entry and retrieval.	
5	The system will include a detection verification feature. The user shall have the option to action a time response to a fire condition. This time shall be programmable up to 10 minutes to allow for investigation of the fire condition before activating alarm outputs. The operation of a manual call point shall override any verify command.	
C.	**Manual Controls**	
1	Start sounders	
2	Silence sounders	
3	Reset system	
4	Cancel fault buzzer	
5	Display test	
6	Delay sounder operation	
7	Verify fire condition	
8	Disable loop	
D.	**Smoke detectors**	
1	Smoke detectors shall be of the optical or ionisation type. Devices	
2	Heat detectors	
3	Heat detectors shall be of the fixed temperature (58° C) or rate of	
4	Devices shall be compatible with the CIE conforming to the	
5	The detectors shall have a single LED to indicate the device has	
E.	**Addressable detector bases**	
1	All bases shall be compatible with the type of detector heads	
2	The device shall be automatically addressed by the CIE on power	
3	Detector bases shall fit onto an industry standard conduit box.	
F.	**Audible Alarms**	
1	Electronic sounders shall be coloured red with adjustable sound	
G.	**Commissioning**	
1	The fire detection and alarm system will be programmable and	

2.5.2.6   *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.

2.5.2.7   *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.
9.	One user can have different policy / access rights for different access points.

2.6   Command Control & Communication Centre (CCCC / C4)

The vision of the Command Control and Communications Centre (C4) is to have an integrated view of all the smart initiatives undertaken by RSCCL with the focus to serve as a decision support engine for city administrators in day-to-day operations or during exigency situations. C4 involves leveraging on the information provided by various departments and providing a comprehensive response mechanism for the day-to-day challenges across the city. C4 shall be a fully integrated solution that provides seamless traffic management, incident – response management, collaboration and geo-spatial display. C4 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. C4 should be able to integrate with various Utility systems such as Water/SCADA, Power, Gas, ITMS, Parking, BRT, Sewerage/ Drainage system, Disaster Mgmt. System etc.

MSI has to integrate all smart components of the project at Command Control and Communication 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 CCCC components level in the actual deployment.

High Availability / Up Time Targets for CCCC 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
- Maximum Downtime Tolerated per Month: 3 hours 3 minutes
- Maximum Downtime Tolerated per Quarter: 6 hours 9 minutes
- Maximum Downtime Tolerated per Year: 36 hours

2.7 Data Centre and Disaster Recovery Centre

- RSCCL shall provide the location to house the compute and storage infrastructure, at the Data Centre facility being built at the Command Control and Communication Centre.
- The DR for the data centre shall be on cloud. The rate card, for various services offered by the cloud vendor will also be available on request.
- 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.
- 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 2**
        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 (MoUD)

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

2.7.1 Data Centre Topology Overview

Proposed Network Architecture at Data Centre
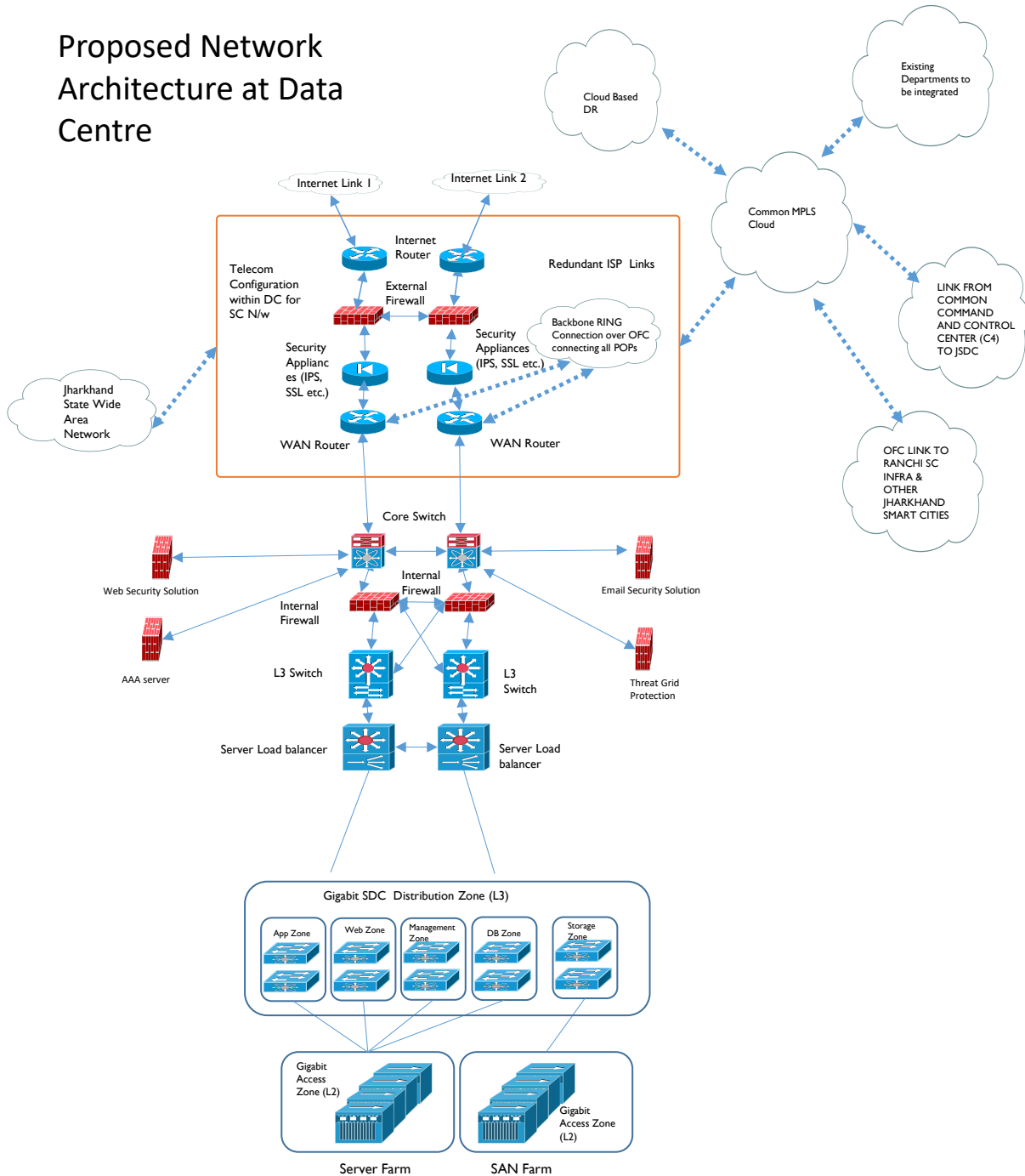
2.7.2 Disaster Recovery and DR Cloud

a) The proposed Cloud Service Provider (CSP) must be an empaneled and audit complaint cloud service provider by MeITY (Ministry of Electronics and Information Technology) for Public cloud, Virtual Private Cloud and Community Government Cloud.

b) 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 RSCCL Data Center and in a different seismic zone.

c) The Cloud Data Centre, where cloud hosting is proposed, must have ISO 27001 certification.

d) 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 RSCCL.

e) Cloud services should be accessible via Internet, Point to Point / MPLS, Leased Lines, OFC WAN etc. MSI must provide private connectivity between RSCCL's network and Cloud Data Centre Facilities.

f) MSI shall be responsible for providing Cloud service for storing all applications at DR [minimum 30% production capacity, RTO – 120 mins, RPO – 15 mins] which will be implemented under Ranchi Smart City project for the project duration. The proposed cloud infrastructure should have not less than 100 cores. Each Compute node should have the latest generation processors containing not less than 128 GB of RAM. The cloud infrastructure should not provide not less than 25 TB for block storage and not less than 100 TB for object. The same can be augmented as per the future requirements. MSI has to design the DR solution as per the requirement of the RFP and factor the same in their technical and financial bid.

g) 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.

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 RSCCL to utilize in case of Change of cloud service provider, migration back to Local Data Centre, burst to a different cloud service provider for a short duration or availing backup services from an alternate Cloud service provider.

j) MSI is required to prepare and submit along with their technical proposal, the details of methodologies and computations for sizing and capacity of storage, compute, backup, network and security resources.

k) RSCCL shall retain ownership of all virtual machines, templates, clones, and scripts/applications created for RSCCL's applications. RSCCL 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 Control and Communication 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 RSCCL.

The below High Level Design (HLD) is just for reference over cloud deployment. MSI can suggest security stack & deployment method according to their recommendations;
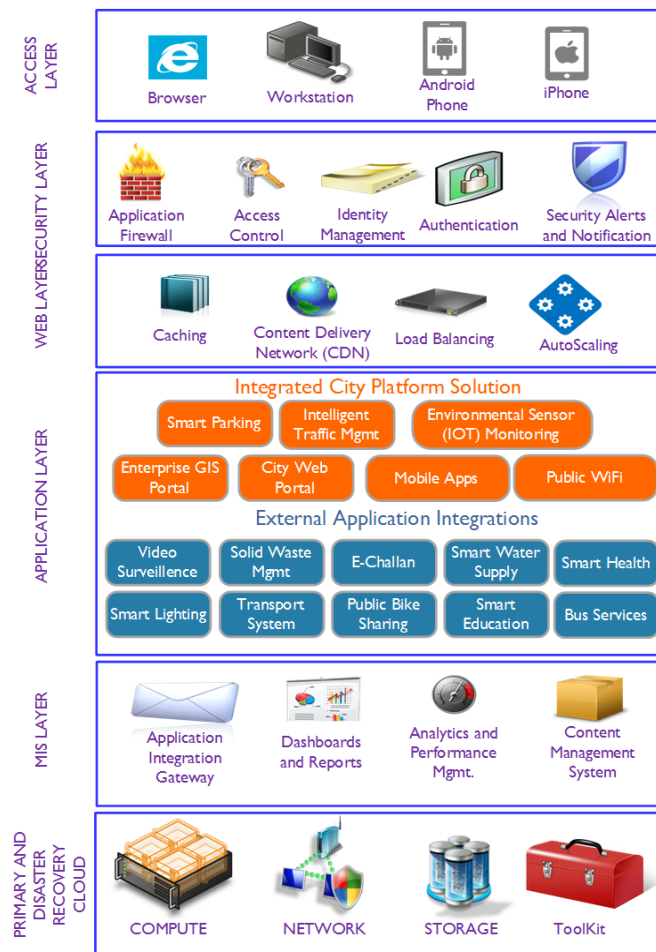
2.7.2.1 *Preparation of Disaster Recovery Operational Plan*

The bidder should provide detailed operating procedures for each application during the following scenarios. These will be mutually agreed upon with RSCCL 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 RSCCL meeting following specifications:

#	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

2.7.2.2 *Periodic Disaster Recovery Plan Update*

The service provider shall be responsible for –
- Devising and documenting the DR policy discussed and approved by RSCCL.
- Providing data storage mechanism with from the Go-Live date till the date of contract expiry for the purpose of compliance and audit

2.8 Intelligent Traffic Management System

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 RSCCL to ensure successful

operations of the system shall essentially be under the scope of MSI and for that no extra charges shall be admissible.

Following key tasks shall be covered under this initiative:

- Provide CCTV cameras including Fixed and PTZ cameras for live video monitoring of key traffic junctions

- Monitor the ongoing activities of the key traffic junctions from the C4.

- Provide pre-recorded and real time announcements in case of emergencies, disasters etc. through Public Address (PA) System at key traffic junctions

- 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 C4.

- Integrate e-challan system with traffic enforcement cameras, sensors, echallan handheld devices for automated issuance of challans

- Provide API integration of Variable Message Sign boards with existing/proposed Smart City Infrastructure such as Smart Parking system, Environmental sensors etc. to provide real time information and services, such as traffic related, pollution levels, parking available, journey planners and accident reporting

- 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.

- Cooperate, 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 C4 -
  - 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 Accident Recording System (TARS)
  - Variable Message Sign boards
  - Public Address (PA)
  - Emergency Call Box (ECB) System

2.8.1 Adaptive Traffic Control System (ATCS)

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

The primary objective of the system is to monitor and control traffic signals, including signaled pedestrian crossings, using a traffic responsive strategy based on real time traffic flow and vehicle presence information. However, the system shall also be capable of operating under fixed time plan.

All junctions under Adaptive Traffic Control System shall be provided vehicle detection system & communication equipment. This shall allow each intersection controller to be monitored from central control for proper functionality. Any corrective action can be initiated either automatically based on status information or by an operator. The real time detection data shall be communicated to the central control station by each controller.

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

The broad scope of work to be covered under ATCS sub module will include the following, but is not limited to:

i. Preparation of Solution Architecture as per project blueprint to develop a final BOQ for installation traffic signaling systems.
ii. Installation of vehicle detectors, controllers, Traffic light aspects, poles, cantilevers, Junction Box and other required accessories at specified traffic junctions for successful operation of the ATCS for RSCCL
iii. Integration of ATCS field infrastructures with the proposed ATCS software application
iv. Configuration of traffic signal at each of the junction along with development of signal control plan for individual operations, coordinated signal plan for the junction in sync with the area wide signal plan for different operating conditions. The operating conditions may include different peak and off-peak conditions, special events, contingency plans etc.
v. MSI may design and propose energy saving signaling system by using solar powered signals or other advanced technologies.

2.8.2 Surveillance System

City Safety and Security solution helps protect cities against crime, terrorism, and civil unrest, planning events, monitoring of infrastructure, encroachments etc. It helps law enforcement monitor public areas, analyze patterns, and track incidents and suspects enabling quicker response. Keeping the above perspective, RSSCL for this purpose is intending to implement the high definition IP based surveillance cameras across various locations within Ranchi. The exact location will be finalized after detailed survey by the Concessioner, post award of the contract. The cameras should be housed on the intelligent/street poles. It shall also be possible to adjust the camera focus from a remote location.

Following is an indicative scope of work;
a. Installation and commissioning work includes installation of all required DVRs, cameras, monitors, cables laid in PVC conduit etc., commissioning all the systems at the pre-defined locations in the project area
b. The MSI shall prepare the final camera distribution plan at all the camera locations in discussion with RSSCL

c. Actual location for placement of pole & number of cameras at each location, type of cameras, fixation of height & angle for the cameras would be done carefully to ensure optimum coverage

d. Bidder should use the industry best practices while positioning and mounting the cameras. Some of the check-points which need to be adhered by the Bidder while installing / commissioning cameras are as follows:
   - Ensure Project objectives are met while positioning the cameras, creating the required field of view
   - Ensure appropriate housing is provided to protect camera from the on field challenges
   - Carry out proper adjustments to have the best possible image
   - Ensure that the pole /tower/ mast implementation is vibration resistant
   - During implementation period, in case any camera is damaged by a vehicular accident (or due to any other reason outside the control of Bidder) and needs repair, then the MSI will need to repair / have the new camera within 15 days of the incidence. Damages are to be borne by MSI in such cases through proper insurance.

e. MSI shall undertake detail assessment for integration of the Surveillance System with the Geographical Information System (GIS) so that physical location of cameras are brought out on the GIS map. Bidder is required to carry out the seamless integration to ensure ease of use of GIS in the Surveillance System Applications/ Dashboards in Command Control Centres. GIS Base Map shall be supplied and integrated by the MSI at 1:1000 scale or better with all surveillance cameras located on the map apart from the updated map of all buildings, utilities and roads. Field survey needs to be done by the MSI. Bidder is required to update GIS maps from time to time

f. Bidder shall carry out SMS Gateway Integration with the Surveillance System and develop necessary applications to send mass SMS to groups/individuals, which can be either manual or system generated. Any external/third party SMS gateway can be used, but this needs to be specified in the Technical Bid.

g. MSI will have to identify and obtain necessary legal / statutory clearances for erecting the poles and installing cameras, for provisioning of the required power, etc. the same will be facilitated by RSCCL. It is important to mention that a timely communication and required follow-up will be required by the MSI for the clearances.

h. During implementation period, in case the pole is damaged by a vehicular accident (or due to any other reason outside the control of MSI) and needs repair, then the MSI will need to repair / have the new pole within 15 days of the incident. Damages are to be borne by MSIs in such cases through proper insurance.

i. For the successful commissioning &operation of the edge devices and to provide the video feeds to Command Control Centre, the MSI will be required to provide electricity to the edge devices through the aggregation points. MSI has to plan the power backup based upon the power situation across the city. MSI may propose solar based powering systems however field devices shall be operational 24x7 and power needs to be calculated accordingly.

j. MSI will be responsible for the solution deployment / customization for implementing end-to-end Surveillance System including its integration with other components as required.

k. MSI will ensure that the best practices for software development and customization are used during the software development/customization and implementation exercise.

2.8.3 Automatic Number Plate Recognition (ANPR) System

Mounted at strategic locations, traffic intersections and on identified mid blocks, the solution shall help in identifying the vehicles that violate traffic regulations and helps in enforcement and maintenance of traffic discipline amongst the citizens. There are several violations like Red Light Violation, speed violation, free left turn violation, zebra crossing , wrong direction violation that shall be detected and vehicles can be identified using ANPR System. The e-challan system shall also be integrated with the ANPR System for generating challans to errant vehicle owners.

The broad scope of work to be covered under this sub module will include the following, but is not limited to:

i. MSI shall install the ANPR Cameras at identified junctions/locations (tentative) across the city. This system shall automatically capture the license number plate of the vehicle at these locations.

ii. MSI shall design, supply, and install the ANPR camera system as defined in the RFPs, all camera accessories such as IR Illuminators, camera housing and mounting shall be installed by MSI. MSI shall supply all of the necessary equipment for the camera and local processing system, including but not limited to: computers, local storage, and ancillary camera equipment, camera poles, warning signs and shall make the final connections to the camera.

iii. MSI shall be responsible for providing all the necessary IT infrastructure for detection, analysis, storage & retrieval of the number plate information at CCCC or any other location as specified in the RFP.

2.8.4 Red Light Violation Detection (RLVD) System

The broad scope of work to be covered under this sub module will include the following, but is not limited to:

i. MSI shall install the RLVD Systems at identified traffic junctions (the final no. might vary based on field survey by MSI) across the city. This system shall capture the infractions of Red light, stop line violations, wrong left turn violations, wrong direction violations etc. at these junctions.

ii. MSI shall design, supply, and install the RLVD system as defined in the RFPs, all wiring connections to the traffic signal controllers and to the camera platforms shall be installed by MSI. MSI shall supply all of the necessary equipment for the camera and detection system, including but not limited to: computers, ancillary camera equipment, camera housings, camera poles, warning signs and shall make the final connections to the camera.

iii. The solution proposed by MSI shall seamlessly integrate with the E-Challan system proposed under the scope of this project. RSCCL shall facilitate to get access to the Vaahan and Sarathi database. MSI shall be required to access the same through use of appropriate APIs.

iv.   MSI shall be responsible for providing all the necessary IT infrastructure for analysis, storage & retrieval of the infraction information at CCCC or any other location as specified in the RFP.

2.8.5   Speed Violation Detection (SVD) System

The broad scope of work to be covered under this sub module will include the following, but is not limited to:

i.   MSI shall install the Speed Violation Detection Systems at identified locations (the final no. might vary based on field survey by MSI) across the city. This system shall capture the infractions of speed violations at these locations.

ii.   MSI shall design, supply, and install the speed violation detection system as defined in the RFPs, all wiring connections for the system shall be installed by MSI. MSI shall supply all of the necessary equipment for the camera and detection system, including but not limited to: sensors, computers, ancillary camera equipment, camera housings, camera poles, warning signs and shall make the final connections to the camera.

iii.   The solution proposed by MSI shall seamlessly integrate with the E-Challan system proposed under the scope of this project.

iv.   MSI shall be responsible for providing all the necessary IT infrastructure for analysis, storage & retrieval of the infraction information at CCCC or any other location as specified in the RFP.

2.8.6   Traffic Accident Recording System (TARS)

Traffic Accident Recording System (TARS) shall provide the accident investigator with advanced techniques in accident data storage and analysis with tools to identify 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. The bidder shall provide field units (tablets or similar) for collecting the accident data (First Information Reports), the data from which shall be transferred to CCCC platform. The data shall be integrated with other city-wide information on the platform. It shall consist of:
- Accident reporting system
- Accident recording system
- Analysis of accidents

2.8.7   Variable Message Sign Board

i.   Central Control Software shall allow controlling multiple VMSB from one console.

ii.   Capable of programming to display all types of Message/ advertisement having alphanumeric character in English and Hindi and combination of text with pictograms signs. The system should have feature to manage video / still content for VMSB display.

iii.   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.

iv.   The system shall also provide airtime management and billing system for

paid content management

v. Capable of controlling and displaying messages on VMSB boards as individual/ group.

vi. Capable of controlling and displaying multiple font types with flexible size and picture sizes suitable as per the size of the VMSB.

vii. Capable of controlling brightness & contrast through software.

viii. 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.

ix. Real time log facility – log file documenting the actual sequence of display to be available at central control system.

x. Multilevel event log with time & date stamp.

xi. Access to system only after the authentication and acceptance of authentication based on hardware dongle with its log.

xii. Location of each VMSB will be plotted on GIS Map with their functioning status which can be automatically updated.

xiii. 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.

xiv. Configurable scheduler on date/day of week basis for transmitting pre-programmed message to any VMSB unit.

xv. 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.

xvi. Apart from role based access, the system shall also be able to define access based on location.

xvii. Rights to different modules / Sub-Modules / Functionalities shall be role based and proper log report should be maintained by the system for such access

xviii. 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.

xix. 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 endeavor to make use of the SSL/VPN technologies to have secured communication between Applications and its end users. Furthermore, all the system logs shall be properly stored & archived for future analysis and forensics whenever desired.

xx. 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.

xxi.   System shall use open standards and protocols to the extent possible
xxii. Facility to export reports to excel and PDF formats.
xxiii. Remote Monitoring
   a. 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.
   b. Remote Diagnostics to allow identifying reason of failure up to 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:

i.   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.

ii. VMSB shall enable RSCCL/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.

iii. These displays can also be used for advertisement purposes. Approximately 20% to 30% of the total running time will be utilized by RSSCL in day-to-day scenario (i.e. normal, non-emergency situations) for its own discretion whereas the remaining time can be used for advertisement purpose. However during emergency or disaster situations, VMBS would be required to play messages issued by C4 all the time till normal situation is restored.

2.8.8   Public Address System

i.   The Public Address System (PA) shall be capable of addressing citizens at specific locations from the C4.

ii.   The proposed system shall contain an IP-based announcing control connected to the C4.

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

iv.   The system shall contain an IP based amplifier and uses PoE power which shall drive the speakers. The system shall also contain the control software which shall be used to control/ monitor all the components of the system which include Controller, Calling Station & keypad, Amplifier (Mixing & Booster).

v.   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.

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

vii. The system shall contain an IP-based amplifier and uses PoE power that could

drive the speakers. The system shall also contain the control software that could be used to control/monitor all the components of the system that includes Controller, Calling Station & keypad, Amplifier (Mixing & Booster).

viii. PA system's master controller shall have function keys for selecting the single location, group of locations or all locations, simple operation on broadcasting to any terminal or separated zones.

ix. PA system's master controller should facilitate multiple MIC inputs and audio inputs.

The broad scope of work to be covered under this sub module will include the following, but is not limited to:

1. MSI shall install IP based Public Address System as part of the information dissemination system at 50 locations (tentative) in the city. These systems shall be deployed at identified junction to make public interest announcements. The system deployed shall be IP based and have the capability to be managed and controlled from the CCCC

3. MSI, in consultation with RSCCL can propose alternate locations apart from the locations mentioned in this RFP for installing the PA system where their effectiveness in communicating information about traffic conditions in Ranchi will be maximized.

4. RSCCL shall review and approve the proposed locations. MSI shall install the PA system on the approved locations.

Refer subsequent section for minimum functional and technical requirement specifications.

2.8.9 Emergency Call Box (ECB) System

A high quality digital transceiver, to be placed at strategic locations determined by the RSCCL. Key is to make it easily accessible by public. The unit shall preferably have a Double button which when pressed, shall connect to the CCCC over the existing network infrastructure setup for ITMS project. These are to be placed only at a select locations such as CCTV field of view to avoid misuse and vandalism of the call box.

The broad scope of work to be covered under this sub module will include the following, but is not limited to:

i. MSI shall also install Emergency Call Box/Panic buttons at 50 locations (the final no. might vary based on field survey by MSI) in the city. These systems shall be deployed at identified junction for ease of access by citizens of Ranchi city.

ii. MSI, in consultation with RSCCL can propose alternate locations apart from the locations mentioned in this RFP for installing ECB system where their effectiveness in communicating information about traffic conditions in Ranchi will be maximized.

iii. RSCCL shall review and approve the proposed locations. MSI shall install ECB system on the approved locations.

Refer subsequent section for minimum functional and technical requirement specifications.

2.9 Pan City Network Backbone (WAN) and Internet Connectivity

2.9.1.1 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 Ranchi. Ranchi 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. RSCCL intends to provide connectivity under at locations like; municipal offices, BRT 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 (CCCC).

RSCCL intends to procure Leased Circuits & Internet Bandwidth for the city wide network under the Ranchi 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.

2.9.1.2   Scope of work

The detailed scope of work for MSI for providing of pan city network backbone is given below:

2.9.1.2.1 As Is Study and Gap Analysis Report

- MSI would be required to carry out an extensive As – Is study as part of site survey and submit a comprehensive Site Survey Report to the RSCCL. The As-Is study and Gap Analysis report would comprise of the outcome of the site survey, As-Is Study, Gap Analysis and site-wise action plan to effectively fill the Gaps in the existing setup and the improvement that would be made in a particular site. The Gap Analysis would primarily capture the WAN and Local connectivity requirements. The report should target to cover the detailed requirements of IT and Non IT infrastructure at each location. The Site-wise Action Plan report should detail out the actionable and its associated timelines and dependencies. The report of each location should be in the same format
- MSI shall prepare the site wise design based on (a) all data contained in the RFP, Climatic and physical conditions and (b) all criteria of design contained in the RFP
- These As-IS and Gap Assessment reports should be submitted to RSSCL for sign off. RSCCL will analyse the reports and will review the suggestions submitted by the Bidder. RSCCL may undertake the procurement, if necessary on Rate Contract quoted by the Bidder. Bidder's consultation shall be required to consult and coordinate with other vendors to ensure procurement of right equipment
- The bidder shall require to undertake the changes suggested as per the Gap assessment Report

2.9.1.2.2 Network Architecture

Leased circuit connectivity architecture should be as per below:
- Leased Circuit connectivity to be provided at offices and remote locations as shared by the RSCCL.
- Further all the Leased Circuit coming to its respective office should be terminated as a single Ethernet drop/port and should not be configured with separate Ethernet connectivity from each remote location, at zonal side of connectivity, for each respective ward or remote location.
- Leased circuit connectivity should be configured to achieve Multiple Hub & Spoke topology

2.9.1.2.3 Network Design:

- Bidder shall be responsible for preparing a network design comprising WAN (Modem, Media Converters, CPE Router devices, etc.) components to meet the intended objectives & SLAs and scope of the project.
- The network design should at least detail out the network connectivity strategy, network scalability, traffic flow management, bandwidth optimization strategy, security strategy, site-wise bill of material, WAN drawings, Leased Circuit network

configuration plan for seamless integration with other infrastructure, etc. Any additional network design aspects, to meet overall scope of work also need to be documented by the bidder.

- The network design shall be submitted to RSSCL and this shall be reviewed and approved by the RSCCL for its implementation.
- The network solution as designed by MSI shall be based on Leased Circuit platform to manage the traffic flow including but not limited to various applications & services such as Voice, Video & Data.
- Further it should provide capability of doing traffic classification and prioritization of applications as per the best practices and requirement of RSCCL efficiently.
- The bidder shall be required to map each location of the RSCCL's offices vis-à-vis the network design and provide technological solution for implementing the network solution.
- The bidder shall be required to propose solution based on the network architecture that is scalable and has adequate redundancy. However, the RSCCL reserves right to optimize the architecture to meet the specific needs at a later date before implementation.
- The bidder shall be required to integrate the existing LAN (starting from the LAN/Field switch being connected) at each of its locations with the proposed WAN based on Leased Circuits.
- The IP schema need to be validated by RSCCL.
- Solution designed should have provisions to offer different classes of service in order to prioritize traffic as desired by RSCCL without any additional investment. Such service level prioritization will include- packet prioritization, bandwidth prioritization at the application/ source IP/ target IP level.
- MSI shall ensure that the network deployed should be IPV4 as well as IPv6 compliant.
- It is the responsibility of MSI to provide all the last mile terminating devices including MUX, Modem, VPN Concentrators, Media Convertors, Routers, Power Backup for device, etc. If any racks, wall bracket support and any other equipment as may be required shall be MSI's responsibility.
- Any active or passive component inadvertently missed out, but required to meet the SLA, shall be provided by the bidder at no extra cost.

2.9.1.2.4 Leased Circuit WAN (Internet & Intranet, Last Mile Connectivity):

- MSI shall study the existing setup and design the new WAN architecture under this project to meet the intended objectives and scope of pan city network backbone. MSI shall provide End to End connectivity to all field locations including the Special Sites and Data Centre sites over Leased Circuits.
- In addition to the provisioning of connectivity, MSI shall also provide all the WAN equipment (Routers, MUX, VPN Concentrators, Modems, etc.) required under this engagement for the successful commissioning of the network.
- The solution should be capable of supporting the communication requirement of the project during the currency of the contract. The bidder is not only required to provide Leased Circuit connectivity at all these locations, but also maintain and upgrade the WAN connectivity as and when required.

- Additionally, MSI shall also be responsible for providing connectivity for the sites which the RSCCL intends to cover over the contract period, as and when the RSCCL feels the needs.
- MSI shall be required to provide maintenance services for the WAN connectivity at all the sites covered under this engagement.
- As part of the preventive maintenance services MSI shall be required to maintain the upkeep of the medium of connectivity, reinstating the medium, any other maintenance job required to meet the redundancy and SLAs as stipulated in the RFP.

2.9.1.2.5 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 RSCCL, at no additional cost to the RSCCL. The network & bandwidth should meet following requirements:
- RSCCL 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.

2.9.1.2.6 Internet Bandwidth at C4, Data Center and all field locations

- RSCCL 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.

2.9.1.2.7 Redundancy

- As a measure of redundancy remote locations, CCCC, 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.

2.9.1.2.8 Network Security

- Security being one of the most important aspects for the RSCCL, it would be governed by stringent standards. Security incidents could consist of any of the following:
    o Denial of Service Attack: - This shall include non-availability of service (Internet bandwidth, messaging service and other web services due attacks that consumes related network resources)
    o Data Theft: - Compromise of any kind of the network.
    o Intrusion: - Successful Unauthorized access to the Purchaser information system, resulting in loss of confidentiality/Integrity/availability of data.
    o Malicious Traffic: - The bidder shall be responsible for isolation of the node/network in which malicious traffic is generated which may be due to virus, malware etc. on detection.
- All active components shall have adequate security provisions, to protect itself from any security attack including but not limited to DoS, password break,

malicious software, unauthorized access and recording of all access information in the active components.

- Link Security: Bidder has to ensure that the link provided is a secure VPN from end to end including CPE, last mile and LAN.
- MSI shall be required to bind the MAC address of the computer with IP as and when required by the RSCCL.
- All the network solution offered by the bidder shall have the security provisions to prevent any unauthorized access to anybody including bidder or its partners. The RSCCL may reserve the right to get testing of components/ equipment supplied under this contract by any designated Third Party Agency.
- During the currency of the project bidder shall adhere and conform to the Network Security Policy of the RSCCL and guidelines issued by Government of India/Government of Jharkhand from time to time.

2.9.1.2.9 Operation, Monitoring, Maintenance and Management of Network services at DC, CCC and other field locations

a. Configuration, Operation, Monitoring, Maintenance and Management of CPE Routers and MUX, Modem installed for the project
b. Rectifying problems / faults of all Router cores and Switches reporting the status to the RSCCL.
c. Orderly Start-up and Shutdown of all network infrastructure for city network backbone as per the laid down procedures mutually finalized by the RSCCL and MSI
d. Incident wise reporting, Link Availability, Loss of Link Availability, Historical trends for availability must be reported to the RSCCL
e. Daily monitoring of WAN, manual testing, Rectifying and reporting the status to the RSCCL.
f. Maintaining an updated inventory / asset list of complete IT Network Infrastructure
g. Protocol migration to any protocol as and when required
h. Configuration / re-configuration / maintenance / monitoring management of Dynamic
i. Host Configuration Protocol (DHCP) servers installed on core routers, routing tables.
j. Maintaining and updating IP address list and optimum management of IP addresses through DHCP/Static entry
k. Maintain and update IP address list and optimum management of IP address
l. Maintain and update LAN and WAN diagrams with relevant details
m. Replacement of supplied equipment in case if the hardware is faulty or any parts is non-functioning
n. Installation, Uninstallation, re-installation of IOS of Routers and Switches due to reasons of bugs, etc.
o. De-commissioning of the existing network & Establishment of the new Leased Circuits across AMC network in phase manner without disturbing the regular operations & working of the existing software applications
p. Network Management & Monitoring Services across City –

1. Daily monitoring of WAN and Internet
2. Manual testing, troubleshooting of WAN.
3. Discovery of existing and all new networking equipment in Network Management software.
4. Updated inventory/asset list of complete IT network infrastructure for the project
5. Updated document for WAN network diagrams with relevant details
6. Services for link / devices augmentation / deletion, relocation / connection /disconnection etc.

q. Bandwidth and Communication Management
   1. The committed bandwidth that has to be provided at all locations. MSI shall have to calculate the requirement of bandwidth at each office. This calculated bandwidth should be allocated to the RSCCL on 24X7 basis.
   2. Bandwidth should be managed using tools that ensure availability of bandwidth on a remote basis. The services should ensure that the bandwidth is available to the department as per the requirements
   3. MSI is required to make provision in the terminal equipment for providing scalability in terms of WAN bandwidth. The RSCCL may order an increase in bandwidth, which would be released from the Pool of Bandwidth. MSI should complete the task of increase or decrease of bandwidth as per below requirements:
      i. For planned activities the bandwidth should be augmented before 15 days of prescribed date, and for unplanned activities selected bidder should augment the bandwidth within 4 hours
      ii. Network should also be capable of providing Bandwidth on Demand.
   4. Communication Management (NMS proposed under this project to be used for this)
      i. Monitoring of quality of various communication links on LAN, WAN, leased circuit/ISDN and Liaison with ISPs
      ii. Link Availability
      iii. Alerts for loss of Availability
      iv. Historical trends for Availability
      v. Incident-wise Reporting
      vi. All incidents leading to downtimes on a particular link should be available at least end-of-day online
      vii. Historical trending for today/yesterday/last 7 days/last week/last month should be available
   5. Internet, Intranet and Gateway Access
      i. Daily monitoring of Internet Leased circuits and All Intranet services.
      ii. Bandwidth Utilization monitoring and reporting the status to AMC in case if the utilization on the constant basis is exceeding 80%.
      iii. DNS Server and Domain Resolution.
      iv. Lookup for Internet hosts.
      v. Proxy Server Configuration, URL filtering and URL Access log.
      vi. If any intranet services are not available the status should be immediately reported to AMC/SCADL IT Cell

     vii.   Disk Utilization monitoring

r.   Helpdesk Support Services [Internal for stakeholders]

As part of overall project scope, MSI is also tasked with operation of an help desk for complaint registration related to network availability/uptime across locations covered as part of the SoW. The detailed activities to be carried out by MSI are listed below:

1. The Helpdesk services should be in accordance to ITIL standards and should be running 24x7x365. MSI has to propose a setup hunting telephone lines for lodging telephonic service request, as well as an email ID, which is monitored 24x7x365.
2. Call Logging for queries / services / complaints (Trouble Ticketing)
3. Call logging will be through telephone / mobile, e-mail or service desk software or through personal messenger.
4. Proactive monitoring has to be done by service provider to reduce the resolution time in case of any link failure. Proactive monitoring should have mechanism of auto generation of link down request for faster resolution. Ticket raise information should be inform to RSCCL and to central helpdesk for ticket resolution monitoring.
5. Recording redressal of complaints in the Service Desk Software, Call closure
6. Call Routing to respective vendors.
7. Call Escalation for all the IT assets supplied under the purview of this contract to senior authority of MSI to be listed in the system, if call is not redressed by respective field representative of MSI.
8. Call monitoring which includes recording status of complaint redressal and reasons for not redressing complaint if any.
9. Incident Management
10. Call analysis and generation of reports using a computerized tool for uptimes and SLA's.
11. Help Desk shall follow up all the calls and perform audio recording calls so that SLA is not violated.
12. MSI shall keep CCCC team informed about the progress at regular intervals. Problems shall be classified into various levels of priority mentioned in the SLA. The assigned priority for each problem shall be dependent upon:
    i.   The extent of the problem's impact on the usability of the system
    ii.   The percentage of project users affected by the system
13. The initial assignment of priorities is the responsibility of the Help / Service Desk's Problem Manager. However, RSCCL can challenge the priority assigned to a particular problem and procedures that exist for escalating a problem to progressively higher management levels, until agreement is secured. The precise definition of problem priorities should be documented in MSI's problem management procedures.
14. Primary telephonic support (complaint / issue resolution) at Helpdesk where resources are deployed and field level support on a need basis.

15. Any other help / service desk related services not listed above but required for smooth functioning of help / service desk services as directed by the RSCLL.

s. Network Management (NMS proposed for the project to be used for this service)

1. Network Performance Monitor
   i. Simplifies detection, diagnosis, & resolution of network issues before outages occur
   ii. Tracks response time, availability, & uptime of routers, switches, & other SNMP-enabled devices
   iii. Shows performance statistics in real time via dynamic, drillable network maps
   iv. Includes dashboards, alerts, reports, & expert guidance on what to monitor & how
   v. Automatically discovers SNMP-enabled network devices & typically deploys in less than an hour
   vi. Provides network views in an intuitive graphical format
   vii. Discovers network devices and provides a map to illustrate the structure of the network
   viii. Provides the status of devices and segments
   ix. Help network administrators prevent problems by identifying potential trouble spots before a failure occurs
   x. Automatically discovers, maps and monitors switches, ports, and network devices
   xi. Quickly finds devices and retrieves user name, port details, connection history and more
   xii. Enables searching on IP address, user name, Hostname or MAC address to track endpoints
   xiii. Allows white listing and watch lists with automatic alerts and click-of-a button port shutdown
   xiv. Provides detailed switch port usage data, capacity analysis, and built-in reporting

2. Network Configuration Manager
   i. Enables bulk change deployment to thousands of devices
   ii. Performs automatic, scheduled network configuration backups
   iii. Protects against unauthorized & erroneous network changes
   iv. Detects & reports on network compliance policy violations
   v. Provides real-time network inventory & asset service management

3. Net-Flow Traffic Analyzer
   i. Monitors network bandwidth & traffic patterns down to the interface level
   ii. Identifies which users, applications, & protocols are consuming the most bandwidth
   iii. Highlights the IP addresses of top talkers
   iv. Monitoring tools include Real-Time Interface Monitor, SNMP real time graph

     v. Diagnostic tools include Ping Sweep, DNS Analyzer, and Trace Route

     vi. Network discovery tools include Port Scanner, Switch Port Mapper, Advanced Subnet Calculator

     vii. Management tools include Real-time NetFlow Analyzer, Config Downloader

4. IP Address Management Software

     i. Centralizes IP infrastructure management, monitoring, alerting and reporting

     ii. Automatically scans IP address space at customizable, scheduled intervals

     iii. Consolidates multi-vendor DHCP/DNS management via a single, integrated interface

     iv. Delivers real-time, at-a-glance dashboard visibility along with historical tracking

     v. Provides active IP address conflict detection and preventative alerts

5. VOiP Network Quality Manager

     i. Monitors VoIP metrics including jitter, latency, packet loss, and MOS

     ii. Correlates call issues with WAN performance for advanced troubleshooting

     iii. Searches & filters call detail records

     iv. Monitors site-to-site WAN performance

t. Reports

1. Bidder should submit the reports on a regular basis in a mutually decided format.

2. Softcopy of these reports shall be delivered automatically via email at specific frequency and to the pre-decided list of recipients

3. The detailed list of reports as well as templates will be decided once the bidder is on-boarded

4. Bidder should also submit certain information as part of periodic review as and when required by the RSCCL

5. Daily Reports

     i. Summary of issues / complaints logged at the Help Desk

     ii. Summary of NMS, other performance monitoring tools

     iii. Network Bandwidth utilization.

     iv. Summary of resolved, unresolved and escalated issues / complaints

6. Weekly Reports

     i. Issues / Complaints Analysis report for calls, call trend, call history, etc.

     ii. Summary of network equipment rebooted.

     iii. Summary of issues / complaints logged with the OEMs.

     iv. Summary of changes undertaken in the WAN Network including major changes like configuration changes, patch upgrades etc.

7. Monthly Reports

     i. Component wise physical as well as Network infrastructure availability and resource utilization.

     ii. Consolidated SLA / (non)-conformance report

      iii. Log of preventive / scheduled maintenance undertaken
      iv. Log of break-fix maintenance undertaken
      v. Network Traffic Analysis, pattern identification and suggestions for improvement across network backbone
      vi. Network Utilization
      vii. Network Device Status
      viii. Network Uptime Statistics & Threshold violation
      ix. Bandwidth utilization as measured at aggregation point as well as on individual links

8. Quarterly Reports
   i. Uptime, Downtime and performance report
   ii. SLA compliance Report for the Quarter
   iii. Hardware pool Report

9. Half yearly Reports
   i. Network infrastructure Upgrade / Obsolescence Report

10. Incident Reporting
    i. Detection of security vulnerability with the available solutions / workarounds for fixing
    ii. Hacker attacks, Virus attacks, unauthorized access, security threats, etc. with root cause analysis and plan to fix the problems

2.9.1.2.10 Rate Contract

- RSCCL is procuring leased circuits to be delivered at various locations spread across the Ranchi 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, RSCCL 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 RSSCL, 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.

2.9.1.2.11 Supply, Installation and Commissioning of Network Infrastructure for pan city network backbone

- MSI shall procure, supply, install, upgrade and commission, all the required WAN, LAN and other IT & Non-IT equipment including, but not limited to, routers, modems, core switches, structural cabling, PVC/ HDPE / conduit Piping etc.
- MSI has to perform site inspection to verify the appropriateness of the sites before installation /commissioning of the Leased Circuit network.
- MSI has to ensure the support of the equipment is for contract period and in case of equipment becoming the End of Life on or before contract period, then it should

be supported with the similar or higher version of equipment for O&M requirements.

- MSI shall also ensure that none of the equipment has reached End of Sale, at the time of PAT of last site before Go – Live and if there is any such equipment then all such equipment installed in the project should be changed before offering for Go – Live.

- MSI shall also ensure that the equipment have not reached End of Support during the currency of the contract, and at the time of transfer of assets. Any equipment which has reached "End of Support" shall need to be replaced at no extra cost to the Purchaser. The equipment shall be replaced with equivalent of higher model.

- The supply and installation of all connecting cables between routers, modems, switches and other equipment shall also be the bidder's responsibility. The bidder to also ensure proper structured cabling (of CAT 6A standards) at each office location/ wherever required. It shall be the responsibility of the bidder to bring all the tools required for the installation, upgrading and commissioning of the equipment/ network.

- The bidder is responsible for last mile connectivity at all field location & DC. The connecting cables between routers, modems, switches and other equipment shall also be the bidder's responsibility.

- All cabling up to CPE should be done with proper clamping. The cabling should be neat and structured with PVC pipe casing.

- It shall be the responsibility of MSI for providing required "Electrical ground" at all points, as required, if necessary. MSI will not take any responsibility of equipment going bad due to non-availability of proper earthling and unstable power.

- The system shall be subjected to inspection at various stages. Local regulation/ codes shall be followed at all times. MSI shall follow all safety regulations and practices. At all times clean work area should be maintained which is free of debris and waste materials etc.

- MSI shall not cause any damage to the RSCCL's (or any other) premises and property and shall perform restoration if any damage occurs. Trenches, path-cutting etc. shall be back-filled and restored to the original condition immediately after laying of the conduit/cable. The bidder shall plug conduits and entrance holes where the cabling has been installed with suitable sealing material to restore it to its original/best state. Wherever needed, the bidder shall have to retrofit existing facilities in order to install the new system.

- MSI must ensure that all statutory and regulatory approvals are obtained within the building (building in-charge, owners of the building etc.) and from various other authorities such as municipal bodies, central government, electricity utility companies etc. MSI shall also be responsible to get required documentation completed for obtaining such approvals from time to time. This should not affect the timelines.

2.9.1.2.12 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. RSCCL 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.
- RSCCL 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. RSCCL will not pay or reimburse any last mile of extra work cost.

2.10 Smart Parking Management & Information System

Lack of sufficient parking space has been a real phenomenon which citizens of Ranchi has been facing for long. As of now, there is no multilevel parking available in the city. There are total ~42 designated open parking area in the city and 72 proposed parking areas. The proposed parking lots shall have ~12000 Sq Meter area which can accommodate ~500 cars considering 25 Sq meter per vehicle. Out of these available parking spaces, there has been a need to find real-time information on availability of parking spaces in the city and disseminate this information to commuters. With Smart Parking solution, it is envisaged to have a system that alerts residents where the open parking space is available, provide parking rates and guides them to the parking area.

As part of this RFP, RSCCL has decided to going for Smart Parking solution over conventional parking due to the following parameters:
- High Parking Search Time
- Traffic Congestion on Road
- Poor Usage of Parking Space

- Poor Occupancy in Parking Lot
- Less effective parking operations
- High Parking violations
- Accidental Hazards
- Stress to user & dissatisfaction
- Pollution – High Emission of gas
- No real time tracking, data/report for analysis for future need/expansion

Smart Parking Solution

With Smart Parking Management System, residents shall come to know the open parking space available around the city, parking charges, map based guidance and probability of finding a space in the parking based on predictive algorithm. MSI shall assess the existing and proposed street parking places and recommend the parking solutions for the same.

Intelligent parking operators shall have following features;
1. Mobile App to help in finding parking space quickly & easily
2. Finding parking space with clear & simple directions reducing traffic Congestion.
3. Improved Parking Occupancy increase collection
4. Improved user satisfaction by saving time, effort & cost
5. Less parking search time reduces emission of gases & control pollution
6. Correct detections of violations & suspicious parking/over duration parking
7. Availability of data & Analysis for growing need for expansion or more parking slots; subsequently required measures to handle problem

Smart Parking Key Components

1. Parking Sensors

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

2. Wireless Sensor Networks Module

   a. Collect sensor data

   b. Check parking slot state in real-time

   c. Send parking slot information to webserver

3. Web Portal and Mobile App for Public

   a. Connect to central web-server

   b. Receive parking slot information from central web-server

   c. Display the real-time monitoring of parking slots state in the nearest parking zone

4. Control and command center

   a. Integration with C4 system

   b. Data management, analytics and Business Intelligence on real time basis

   c. Monitoring of real time transactions, parking availability

d. Management of Equipment status and alarms on real time basis

e. Dash boards and reports

5. Central Web-Server

    a. Receive parking slot information from wireless sensor networks

    b. Display the parking slots state of parking zone in real-time

    c. Send information to mobile phone application

    d. Save information in SQL database

    e. Reporting & analytics

6. Digital Display Unit

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

2.11 City Wi-Fi Hotspots

Hot Spot Wi-Fi serves as the foundation for creating a connected city to access the wireless internet service with ease and convenience. For this purpose RSCCL has identified locations where these services has to be provided to citizens. As a part of this initiative free Wi-Fi need to be provided; Wi-Fi shall be free for the first 30 Minutes per Mobile subscriber per day with aggregate limit of 5 GB per month whichever is achieved first beyond that it is chargeable. Beyond the above specified limit services would be chargeable by RSSCL. For implementing the same the Bidder will carry out survey at these 43 locations (tentative) and will deploy the access points as required for providing the Wi-Fi services. As a part of Wi-Fi solution the MSI needs to provide Wi-Fi controller, DNS, Internet bandwidth from Internet Service Provider (ISP). ISSID for E governance (for Client) shall be reserved. For installation of Access Points, if there is any requirement of additional poles, the same will be provided by Bidder at its own cost with prior approval from RSCCL

City Wi-Fi Hot Spot helps cities provide citizens with Internet connectivity and access to a broad range of citywide service which has following benefits:
- Internet availability at lower costs
- E-government services delivered to citizens, faster, and at a lower operating expense
- Local economic development
- Improved productivity and service
- Access to city services and Internet connectivity
- Increased access to online services
- Revenue generation

The objective is to implement wireless networking technology that uses radio waves to provide wireless high-speed Internet and network connections. All wireless networking equipment must be based on the IEEE standards of 802.11a, 802.11b, 802.11g, 802.11n, 802.11ac compatible.

Scope of Work – Wi-Fi

MSI shall be responsible for establishment of Wi-Fi network at the selected location in the Ranchi, these locations are normally tourist spots, public places or any other identified place by RSCCL. MSI shall provide Operation & Maintenance throughout the concession period from the date of commissioning. The broad scope of work for MSI during the entire project period would be as under;

- MSI Shall undertake a Site-survey of all the specified sites and submit a site wise survey report to RSCCL mentioning the location &number of Access Points (APs) required to be installed at each site.
- MSI proposal must provide all the necessary electronic components needed to provide wireless access to the public. This includes but is not limited to Wireless controllers, Access points, Power over Ethernet devices, L2 and L3 managed switches, Routers, UPS, passive components i.e. UTP, OFC, Electric wires, racks etc.
- MSI shall install the Access Points at approved locations (on directions by RSCCL after approval of Site-Survey report). The power points, connectivity and LAN points will be the responsibility of Bidder. RSCCL will facilitate the requirement/clearances as and when required.
- MSI shall properly Wall Mount/ Pole Mount the Access Points at approved locations with external mounting kit as per OEM standard practice.
- MSI shall install the AP Controller, NMS, NAS and required software at Command & Control Centre
- The Patch Cords, Power adapter, Power cables, connectors, mounting kit and other required accessories for successful commissioning of the Wi-Fi network shall be provided by the MSI and shall be properly cased and tied such that it doesn't get broken.
- All intended coverage areas must be covered with wireless AP/array for high rate data applications. For density concerns, there must be multiple radios per classroom/area. Each wireless AP/array must be 802.11 a/b/g/n/ac 3x3:3 MIMO WAVE2 capable and be able to scale without adding additional controllers or user licenses. At each site Bidder must consider at least one primary controller and secondary controller to avoid a single point of failure.
- Controller should be configured with 1 + 1 in Active-Active Load Balancing mode.
- Each controller should be ready for supporting 300 AP's and 20000 devices from day one to run in Active-Standby / Active-Active Load Balancing Mode, with scalability for 1000 AP support in future.
- Each wireless device (not system) must support per SSID traffic shaping and limiting at line- rate at the Access Point (not controller). This is to prevent additional data on the network
- Each wireless device (AP) must employ a future-proof modular architecture for upgradability to future standards
- Bidder must include PoE-injectors in the pricing and clearly define where PoE injectors are needed
- System must include a centralized management system that provides a platform for central management of all devices across the network
- PVC case wiring should be done for the entire required passive cabling i.e. UTP and electrical wiring

- MSI will ensure a secure Wi-Fi connectivity and internet access through user Login ID and password to all the subscribers with central authentication mechanism
- MSI shall ensure that unique user ID and Password do not have provisions for simultaneous multiple logins
- Policy on validity of the user ID and Password for internet access should be configurable as per the requirement.
- Wi-Fi access points (APs) must be configured to use cryptographic keys or other methods to ensure that only authenticated users can use the Wi-Fi services
- Internal / External AAA server should be deployed ensuring DOT guidelines for providing public Wi-Fi access. The log trails for any specific user shall be made available online for at least last 3 months and the backup shall be kept for one year.
- The system should be capable of managing automatically upgrade or degrade of end-user's account after threshold usage (download/time limit) is reached
- Wi-Fi network should be secure and conform to the industry standard security requirement. Bidder shall suggest and help RSCCL team to deploy policies at various levels (i.e. on firewall, IDS, antivirus etc.) to prevent any attack/intrusion in the Wi-Fi network
- MSI shall be responsible for integrating the Wi-Fi Network with the existing LAN/SWAN network
- MSI shall be responsible for integrating the available payment gateway(s) at RSCCL for making online payments (if any) according to respective plans for internet usage
- MSI shall be responsible for integrating SMS gateway (HTTP) at RSCCL for automatically sending the required details/ information through SMS to the users as per the requirement e.g. during user registration, forgot password, password reset etc.

Operation & Maintenance

Following are the indicative activities MSI shall perform during O&M period;
- MSI need to ensure that adequate spares are retained at all times to meet onsite warranty/support and SLA requirements
- The maintenance services involves comprehensive maintenance of all component covered under the contract, including repairing, replacement of parts, modules, sub-modules, assemblies, sub-assemblies, spares part, updating, security alerts and patch uploading etc. to make the system operational
- MSI shall insure all the APs to ensure theft protection of all APs throughout the project period

Refer subsequent section for minimum functional and technical requirement specifications.

2.12 Environmental Monitoring Sensors

Environmental parameters, specifically air and noise pollution, are a major concern for the citizens and administrators of any city. RSCCL believes it is important that citizens know of the air that they breathe. Citizens & visitors to the city can enjoy unique experiences that keep them feeling good by knowing city's environment condition at different locations. The business requirements of environmental

monitoring is given below:

- Integrated ambient air and noise pollution monitoring stations comprising of various environmental sensors shall be implemented in Ranchi for monitoring and trending of various ambient air and noise parameters.

- Environment monitoring shall be done for tracking that the pollution and noise levels are within the acceptable limits.

- Display of parameters to citizens to create awareness and support 'open data' initiatives.

- Establish frameworks for regulating these parameters in terms of any supporting initiatives for maintaining acceptable levels.

- Central monitoring at C4, city application, website and variable message screen in an integrated manner.

The Environmental monitoring system installations shall be provided variable messaging board installed at strategic locations across the City to display environmental parameters to the public.

The Air quality should be monitored by a network comprising:

- fixed monitoring stations

- Data processing

- Data transmission to a central system

- A central processing system

Refer subsequent section for minimum functional and technical requirement specifications.

2.13 Enterprise GIS

Availability of timely and relevant information about cityscape, the physical growth trend taking place in different parts of the city is a very important input to the Smart City Development process. Geographical Information System (GIS) is for management, analysing and displaying data of all areas within Ranchi Smart city which are spatially referenced to earth for efficient and effective decision making, spatial planning, management of crisis/disasters and for monitoring of normal circumstances, thus providing an important tool to respond faster to incidents or even avert certain incidents. GIS platform is intended to provide common GIS capability to all other systems being deployed as part of Ranchi Smart City initiative. The objective of architecting a common GIS layer is to keep a single repository of all GIS data (pan city data) for easy maintenance, avoid duplication and easy dissemination of information to all the dependent systems. The dependent systems include Smart Parking, City Wi-Fi, Pan City Network Backbone, Intelligent Transport Management and Utility Management Systems. More systems may be added in the future and therefore the GIS application should be able to integrate with such applications through standards based interfaces. GIS platform would be importing a lot of existing data from various sources into most industry standard formats. GIS platform would also need to exchange data with a number of external applications and

therefore should be capable of exporting data in most industry standard formats Following services shall be configured through Web GIS software (but not limited to):

- Location Based Services
- Traffic Management System, Vehicle Tracking and Management System (VTMS)
- Mobile GIS Services
- "What if" analysis
- Mapping Gallery for Inter-Departmental use of Maps/ data Integration of Applications and disparate databases

Refer subsequent section for minimum functional and technical requirement specifications.

2.14 City Web Portal & Mobile App

At the core of the stakeholder's service experience will be citizen portal of RSCCL 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, status check on service request, lodge an incident/complaint and provide suggestions. Portal shall exhibit enriched infographics 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 RSCCL'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 RSCCL'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 RSCCL 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 RSCCL, 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.

2.15 Handholding and Training

In order to strengthen the staff, structured capacity building programmes shall be undertaken for identified resources of RSCCL, Corporation, UD&HD and stakeholder departments. It is important to understand the training needs to be provided to each and every staff personnel of CCCC. 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 RSCL 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 RSCL 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 C4 system.
g) MSI shall prepare the solution specific training manuals and submit the same to RSCCL 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 RSCCL 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 RSCCL 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 RSCCl feels that on-field sessions are required, the same shall be conducted by the MSI.

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

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

s) RSCCL 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 RSCCL/authorized entity to review and track the progress, In case, after feedback, more than 40% of the respondents suggest that the training provided to them was unsatisfactory or less than satisfactory then the SI shall re-conduct the same training at no extra cost.

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

I. Functional Training
- ✓ Basic IT skills
- ✓ Web portal, Mobile App, Enterprise GIS, ITMS, Smart Parking, Wi-Fi, environmental sensors, Data Analytics, ANPR, smart solutions etc.
- ✓ Software Applications (Command Control and Communication 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

2.16 Project Implementation Schedule, Deliverables and Payment Terms

2.16.1 Project Implementation Schedule and Deliverables Payment Schedule

T = 14 Days from Issue of LOI or LOA

#	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 Control and Communication Centre (C4) including Data Centre • City IT Network Infrastructure • Smart Parking Management System (SPMS) • Intelligent Traffic Management System (ITMS) • Environmental Monitoring System • City Web Portal & Mobile App • Enterprise GIS	Architecture and design for C4, City IT Network and Data Centre including Data Centre Architecture, Network Architecture, Security architecture etc. Submission of FRS, SRS including Solution Architecture, Application Design Documents (HLD & LLD) of the proposed system	T + 3 months

#	Milestones	Deliverables	Timelines (in months)
	• City Wi-Fi • Integration of CCCC platform with existing & under-development external Systems/ Applications as per scope	Integration report for external applications	
1.3	**Phase I: Go-Live** a. Design, supply, installation, commissioning including interior civil work, hardware, system software, network equipment, bandwidth & operationalization of Command Control & Communication Centre along with DC and DR b. 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 c. GIS – Supply, installation, data migration, training & operationalization of enterprise GIS system for the city d. City web-portal – Design, development, content writing, training & deployment of city web portal e. ITMS – Supply, installation, commissioning, training and operationalization of ITSM components (ANPR, RLVD, SVDS, ATCS, PA, ECB) at 30% of total identified locations f. Wi-Fi - Supply, installation, commissioning, training & operationalization of City Wi-Fi at 50% of total identified locations g. Environmental Sensors - Supply, installation, commissioning, training & operationalization of Environmental sensors at sensors	1. Site Completion/readiness Report 2. Delivery Acceptance Reports from RSCCL/authorized entity 3. Installation & Commissioning Reports 4. Software Licenses details 5. UAT/FAT and Go Live Certificate from RSCCL/authorized entity 6. Training Content & Completion Certificate 7. Security Audit Certificate from Cert-In/STQC for Data Centre and Applications	T + 7 months

#	Milestones	Deliverables	Timelines (in months)
	h. Variable Messaging Board - Supply, installation, commissioning, training & operationalization of Variable Messaging Boards at 50% of total identified locations		
1.4	**Phase II: Go-Live** a. ITMS – Supply, installation, commissioning, training and operationalization of ITSM components (ANPR, RLVD, SVDS, ATCS, PA, ECB) at remaining 70% of total identified locations b. Wi-Fi - Supply, installation, commissioning, training & operationalization of City Wi-Fi at 50% of total identified locations c. Smart Parking Solution – Supply, installation, commissioning, training & operationalization of smart parking solution at identified location d. Variable Messaging Board - Supply, installation, commissioning, training & operationalization of Variable Messaging Boards at remaining 50% of total identified locations e. Mobile App – Design, development, delivery, training & installation of mobile app in android & iOS for identified services & integration with existing services of RSCCL	1. Site Completion/readiness Report 2. Delivery Acceptance Reports from RSCCL/authorized entity 3. Installation & Commissioning Reports 4. Software Licenses details 5. UAT/FAT and Go Live Certificate from RSCCL/authorized entity 6. Availability of Mobile App on Play Store & Apple App Store 7. Training Content & Completion Certificate	T + 9 months
1.5	**Phase III: Integration & Project Final Go-Live** Integration with external applications (existing & proposed)- ▪ City Surveillance System ▪ Smart Lighting ▪ ICT Enabled Solid Waste Management	1. UAT/FAT and Go Live Certificate from RSCCL/authorized entity 2. Training Content & Completion Certificate 3. Security Audit Certificate from Cert-In/STQC	**T + 10 months = T1**

#	Milestones	Deliverables	Timelines (in months)
	- Intelligent Transportation System - E-Challan System - Public Bike Sharing - Smart Water Supply System - Smart Education - Smart Health Management System - BRTS/MRTS and City Bus Services	4. Source code of portal, Mobile App & customized applications	
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. RSCCL 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 RSCCL.

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 RSCCL 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 RSCCL'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.

2.16.2 Payment Schedule

#	Milestones	Timelines	Payment
1.	Requirement study	T + 3 Months	2% of capex value
2.	Hardware Delivery & commissioning for C4 & DC in Phase I	T + 5 Months	5% of capex value
3.	Phase I : Go Live	T + 7 Months	23% of capex value
4.	Phase II : Go Live	T + 9 Months	10% of capex value
5.	Phase III : Integration & Project Final Go-Live	T1 = T + 10 months	30% of capex value
6.	One year of successful completion of Project Final Go-Live	T1 + 12 Months	Remaining 30% of capex value shall be paid in two (2) equal half yearly instalments
7.	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 110% of the requested amount
   c. Mobilization advance shall be interest bearing and PLR rate of interest shall be payable to RSCCL 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 RSCCL
   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

3 Detailed Scope of Work and Considerations

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 RSCCL 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 RSCCL. 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. 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 RSCCL, 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 RSCCL 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 RSCCL 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 RSCCL.

f. For all the discussion with RSCCL team, MSI shall be required to be present at RSCCL 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 IX, 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 RSCCL. The dismantled infrastructure shall be delivered at the RSCCL 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 RSCCL 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. RSCCL shall facilitate the same. The recurring electricity charges will be borne by RSCCL as per actual consumption.

3.3 Design Phase

MSI shall build the solution as per the Design Considerations detailed in Annexure – IV. 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.

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

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 RSCCL regularly :

    o Functional Requirement Specification (FRS)

    o High level design of whole system

    o Low Level design for whole system / Module design level

    o System Requirements Specifications (SyRS)

    o Any other explanatory notes about system

    o Traceability matrix

    o Technical and product related manuals

    o Installation guides

    o User manuals

    o System administrator manuals

    o Toolkit guides and troubleshooting guides

    o Other documents as prescribed by RSCCL

    o Quality assurance procedures

    o Change management histories

    o Version control data

    o SOPs, procedures, policies, processes, etc. developed for RSCCL

      o 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 RSCCL.)

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 Ranchi 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.

#	Solution to be integrated	Integration requirements
1	Video Surveillance System	Should allow user to visualize the video feeds accessing from Ranchi Police Command Control Center
2	ICT based Solid Waste Management	C4 will be required to integrate with the Solid Waste Vehicle tracking project (Pan City Initiative) to receive feeds on the location of the solid waste vehicles. C4 will also get other information like fuel utilization of Vehicles. All the information received will also be required to be mapped on the GIS map. All the information received from the command centre will also go into the Analytical layer which will help city in better planning and running of operations. C4 should also be able to trigger the commands / alerts (if required) to the respective department.
3	Smart Lightning	C4 will be required to integrate with smart lighting sensors. C4 will be required to get information on the

#	Solution to be integrated	Integration requirements
		status of working of the installed LED lights, All the information received will also be required to be mapped on the GIS map. C4 should also be able to trigger the commands / alerts (if required) to the respective lightning team.
4	Intelligent Transport System	C4 will be required to integrate Intelligent Transport System to get all kinds of feeds from Transport System. These feeds will be sensor based feeds on location of public transport vehicles, bus station information operations, etc. All the information received from the command centre will also go into the Analytical layer which will help city in better planning and running of operations. C4 should also be able to trigger the commands / alerts (if required) to the respective department.
3.	Public Bike Sharing	C4 will be required to integrate Public Bike sharing system to get all kinds of feeds from PBS system. These feeds will be sensor based feeds on location of public bikes, docking station information operations, receive feeds on the status of utilization of public bike sharing docks across the city etc. All the information received will also be required to be mapped on the GIS map, and shall also go into the Analytical layer which will help city in better planning and running of operations. C4 should also be able to trigger the commands / alerts (if required) to the respective department.
6.	Smart Water Supply	C4 will be required to integrate Water Management System (SCADA) get all kinds of sensor and edge devices feeds. C4 shall be able to map this information on the GIS layer and help RSCCL to monitor the water management of the city. C4 shall also be able to trigger the commands / alerts (if required) to the respective department. All the information received from the application will also go into the Analytical layer which will help city in

#	Solution to be integrated	Integration requirements
		better planning and running of operations.

3.6 Pilot Deployment

- MSI shall conduct Pilot deployment and testing for meeting RSCCL's business requirements before rolling out the complete system. The pilot will be run for four weeks to study any issues arising out of the implementation. MSI shall also review health, usage and performance of the system till it is stabilized during pilot deployment. Based on RSCCL's feedback for incorporating changes as required and appropriate, MSI shall train staff involved in the Pilot implementation.

- Pilot shall be demonstrated to the RSCCL's representatives. If for any reason the pilot is found to be incomplete, these will be communicated to the MSI in writing on the lapses that need to be made good. A one-time extension will be provided to the MSI for making good on the lapses pointed out before offering the system to Client for review. Failure to successfully demonstrate the Pilot may lead to termination of the contract with no liability to Client.

3.7 Go-Live Preparedness and Go-Live

- MSI shall prepare and agree with RSCCL, the detailed plan for Go-Live (in-line with RSCCL's implementation plan as mentioned in RFP).

- MSI shall define and agree with RSCCL, 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 RSCCL team on the same.

- Go-live of the application shall be done as per the finalized and agreed upon Go-Live plan.

3.8 Operations and Maintenance

MSI will operate and maintain all the components of the C4 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 NRDA. 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 C4 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 C4 System be ported outside the geographical limits of the country. Some broad

details of O&M activities are mentioned below:

3.8.1 Applications Support and Maintenance

Application support includes, but not limited to, production monitoring, troubleshooting and addressing the functionality, availability and performance issues, implementing the system change requests etc. The MSI shall keep the application software in good working order; perform changes and upgrades to applications as requested by the RSCCL 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 RSCCL.

b. Annual Technology Support

MSI shall be responsible for arranging for annual technology support for the OEM products to RSSCCL 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 RSCCL'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 NRDA 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 RSCCL's approval. A detailed process in this regard will be finalized by MSI in consultation with RSCCL.

   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 RSCCL.

   vi. MSI, at least on a monthly basis, will inform RSCCL 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 RSCCL 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 RSCCL personnel whenever there is any change in the functionality. Training plan has to be mutually decided with RSCCL.

h. Maintain System documentation

MSI shall maintain at least the following minimum documents with respect to the C4 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 updation of documentation of software system ensuring that:

i.   Source code is documented

ii.   Functional specifications are documented

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

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

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

vi.   changes/enhancements

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

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 RSCCL 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. RSCCL 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.

3.8.2 ICT Infrastructure Support and Maintenance

ICT infrastructure includes servers, storages, back up, networking, load balancers, security equipment, operating systems, database, enterprise management system, help desk system and other related ICT 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.

3.8.3 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 RSCCL 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 RSCCL, 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 RSCCL.

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 RSCCL team as well.

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

i. The MSI shall ensure that the warranty complies with the agreed technical

standards, security requirements, operating procedures, and recovery procedures.

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

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

iii. The MSI shall introduce a comprehensive Assets Management process & appropriate tool to manage the entire lifecycle of every component of C4 system.

3.8.4 Maintenance of ICT Infrastructure at the DC and CCCC

a. Management of DC and CCCC

MSI need to deploy requisite mix of L1, L2 and L3 resources (on 24X7 basis) for management of entire C4 System including ICT infrastructure deployed at DC and CCCC. 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 RSCCL. It is expected that resources have proven track record and reliability. Considering the criticality of the project, RSCCL 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 RSCCL and keep the same updated. A detailed process in this regard will be finalised between RSCCL 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 RSCCL on monthly basis. RSCCL 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 RSCL. MSI shall comply with this.

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

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

ii. 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. Updation 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 RSCL.

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 RSCCL 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 NRDA on need basis.

vii. MSI shall implement a password change mechanism in accordance with the security policy formulated in discussion with NRDA 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 RSCCL.

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 RSCCL at all times.

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

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

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

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

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

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

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

Agreement.

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

d. Storage Administration

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

ii. MSI shall be responsible for storage management, including but not limited to management of space, SAN/NAS volumes, RAID configuration, LUN, zone, security, business continuity volumes, performance, etc.

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

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

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

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

vii. To facilitate scalability of solution wherever required.

viii. The administrators will also be required to have experience in technologies such as virtualisation 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 NRDA 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 RSCCL. The MSI is responsible for getting acquainted with the storage policies of RSCCL before installation and configuration. It should be noted that the activities performed by the MSI may be reviewed by RSCCL.

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 RSCCL 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 RSCCL.

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/CCCC etc.

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

h. Security Management

i. Regular hardening and patch management of components of the C4 System as agreed with RSCCL

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

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 RSCCL 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 RSCCL

    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 RSCCL 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 RSCCL
>
> xxix. Implementing and maintaining security rules
>
> xxx. Performing any other day-to-day administration and support activities

i. Other Activities

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

3.8.5 Compliance to SLA

> i. MSI shall ensure compliance to uptime and performance requirements of project solution as indicated in the SLA table of RFP and any upgrades/major changes to the C4 System shall be accordingly planned by MSI for ensuring the

SLA requirements.

ii. MSI shall be responsible for measurement of the SLAs at the C4 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 RSCCL officials as per the project requirements.

3.9 Manpower Deployment

MSI shall deploy Manpower during implementation and O&M phases. The deployed resource shall report to RSCL 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:

#	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 RSCCL in operationalization of the project. Total number of operators required for the project is 30 in three shifts. RSCCL 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 RSCCL 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. RSCCL 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 RSCCL officers on right approaches for monitoring the feeds & providing feedback to RSCCL, 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 RSCCL, as per requirements.

3.10 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.

3.10.1 Cooperation and Provision of Information

During the exit management period:

a. MSI will allow the RSCCL 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 RSCCL to assess the existing services being delivered;

b. Promptly on reasonable request by the RSCCL, 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 RSCCL 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 RSCCL 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.

3.10.2 Confidential Information, Security and Data

a. MSI will promptly on the commencement of the exit management period supply to the RSCCL 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 RSCCL or its nominated agencies transitioning the services to its Replacement MSI in a readily available format nominated by the RSCCL, its nominated agency;

- all other information (including but not limited to documents, records and agreements) relating to the services reasonably necessary to enable RSCCL or its nominated agencies, or its Replacement MSI to carry out due diligence in order to transition the provision of the Services to RSCCL 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 RSCCL 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.

3.10.3 Transfer of Certain Agreements

On request by the RSCCL or its nominated agency MSI shall effect such assignments, transfers, licenses and sub-licenses RSCCL, 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 RSCCL or its nominated agency or its Replacement MSI.

3.10.4 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 RSCCL 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.

3.10.5 Exit Management Plan

a. MSI shall provide the RSCCL 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 RSCCL'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 RSCCL and identification of specific security tasks necessary at termination;

 ▪ Plans for provision of contingent support to RSCCL, 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 RSCCL 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 RSCCL or its nominated agencies within 90 days from the Effective Date of this Agreement.

3.11 Compliance to Standards & Certifications

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

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

#	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

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. Quality Audits

- RSCCL, 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.

3.12 Project Management and Governance

3.12.1 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 RSCCL 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.   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.

3.12.2 Helpdesk and Facilities Management Services

MSI shall be required to establish the helpdesk and provide facilities management services to support the RSCCL 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 RSCCL'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:

#	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.

3.12.3 Steering Committee

- The Steering Committee will consist of senior stakeholders from RSCCL, 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, RSCCL may call for a Steering Committee meeting with prior notice to MSI.

3.12.4 Project Monitoring and Reporting

- MSI shall circulate written progress reports at agreed intervals to RSCCL 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. RSCCL reserves the right to ask the bidder for the project review reports other than the standard weekly review reports.

3.12.5 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 RSCCL based on the risk appetite and shall prepare and share the RSCCL 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 RSCCL.

- MSI shall monitor, report, and update the project risk profile. The risks should be discussed with RSCCL 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.

3.12.6 Governance procedures

MSI shall document the agreed structures in a procedures manual.

3.12.7 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 RSCCL 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 RSCCL 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 RSCCL

3.12.8 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 CCCC, and DC. This may be carried out through the use of standard license metering tools.

3.13 Change Management & Control

3.13.1 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.

3.13.2 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.

3.14 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 RSCCL will review. Once RSCCL provides its approval, the Acceptance criteria can be finalized. In case required, parameters might be revised by RSCCL 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. RSCCL 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. RSCCL doesn't intend to own these tools
Integration Testing	✓ MSI	▪ MSI to perform Integration testing ▪ MSI to prepare and share with RSCCL 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 ✓ RSCCL / 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 RSCCL ▪ 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. RSCCL doesn't intend to own these tools ▪ RSCCL if required, could involve third party auditors to monitor/validate the performance testing. Cost for such audits to be paid by RSCCL
Security Testing (including Penetration	✓ MSI ✓ RSCCL / Third Party Auditor (to	▪ 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

Type of Testing	Responsibility	Scope of Work
and Vulnerability testing)	monitor the security testing)	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 RSCCL ▪ 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. ▪ RSCCL 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 RSCCL
User Acceptance Testing of Project	✓ RSCCL or RSCCL appointed third party auditor	▪ RSCCL / RSCCL 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 RSCCL /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. RSCCL 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 RSCCL directly. All tools/environment required for testing shall be provided by MSI.

e. STQC/Other agencies appointed by RSCCL 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.

3.15 Factory Testing

Success MSI shall have to submit Factory Test Certificate for the below mentioned materials before the actual supply of the items.

1. Cable
2. Traffic Pole
3. Signal Aspects

Authorized representative from RSCCL will visit the manufacturing plant of the product subject to present in India. Authorized representative will check the testing process.

3.16 Final Acceptance Testing

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

Prerequisite for Carrying out FAT activity:

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

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

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 Ranchi 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 RSCCL.

   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 RSCCL 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 RSCCL may mutually agree to redefine the Network so MSI can complete installation and conduct the Final Acceptance Test within the specified time.

4 Requirement Specifications (Functional & Technical)

4.1 Field Equipment: UPS and Others

4.1.1 Industrial Grade Outdoor PoE switches

#	Parameter	Minimum Specifications	Bidder Compliance (Y/N)	Product and Documentation Reference
1.	Make		<to be provided by the bidder>	
2.	Model		<to be provided by the bidder>	
3.	Type	Managed Outdoor switch		
4.	Ports	▪ Minimum 4 10/100 TX PoE ▪ May require higher port density at some locations, depending upon site conditions ▪ May require fibre ports at some locations, depending upon site conditions/distances		
5.	PoE Standard	IEEE 802.3af or better		
6.	Protocols	▪ Support 802.1Q VLAN ▪ DHCP support ▪ SNMP Management		
7.	Access Control	▪ Support port security ▪ Support 802.1x (Port based network access control). ▪ Support for MAC filtering.		
8.	PoE Power per port	Sufficient to operate the CCTV cameras connected		
9.	Others	All switches shall have a Mean Time Between Failure (MTBF) of at least 175,000 hours.		
10.	Rating	IP 30 or equivalent Industrial Grade Rating (This is not essential if the switch is placed in equivalent or better junction box / enclosure)		

#	Parameter	Minimum Specifications	Bidder Compliance (Y/N)	Product and Documentation Reference
11.	Operating Temperature	0 – 50 degrees C or better		

4.1.2   Online UPS – I/2 KVA

#	Parameter	Minimum Specifications	Bidder Compliance (Yes/No)	Product Documentation Reference
1.	Make		<to be provided by the bidder>	
2.	Model		<to be provided by the bidder>	
3.	Capacity	Adequate capacity to cover all above IT Components at Dc for at-least 60 min		
4.	Output Wave Form	Pure Sine wave		
5.	Input Power Factor at Full Load	>0.90		
6.	Input	Three Phase 3 Wire for over 5 KVA		
7.	Input Voltage Range	305-475VAC at Full Load		
8.	Input Frequency	50Hz +/- 3 Hz		
9.	Output Voltage	400V AC, Three Phase for over 5 KVA UPS		
10.	Output Frequency	50Hz+/- 0.5% (Free running); +/- 3% (Sync. Mode)		
11.	Inverter efficiency	>90%		
12.	Over All AC-AC Efficiency	>85%		
13.	UPS shutdown	UPS should shutdown with an alarm and indication on following conditions 1)Output over voltage 2)Output under voltage 3)Battery low 4)Inverter overload 5)Over temperature 6)Output short		
14.	Battery Backup	60 minutes in full load		

#	Parameter	Minimum Specifications	Bidder Compliance (Yes/No)	Product Documentation Reference
15.	Battery	VRLA (Valve Regulated Lead Acid) SMF (Sealed Maintenance Free) Battery		
16.	Indicators & Metering	Indicators for AC Mains, Load on Battery, Fault, Load Level, Battery Low Warning, Inverter On, UPS on Bypass, Overload, etc. Metering for Input Voltage, Output Voltage and frequency, battery voltage, output current etc.		
17.	Audio Alarm	Battery low, Mains Failure, Over temperature, Inverter overload, Fault etc.		
18.	Cabinet	Rack / Tower type		
19.	Operating Temp	0 to 50 degrees centigrade		
20.	Management Protocol	SNMP Support through TCP/IP		

4.1.3 Field Junction Box

#	Parameter	Minimum Specifications	Bidder Compliance (Y/N)	Product and Documentation Reference
1.	Make		<to be provided by the bidder>	
2.	Model		<to be provided by the bidder>	
3.	Size	Suitable size as per site requirements to house the field equipment		
4.	Cabinet Material	Powder coated CRCA sheet/ Stainless steel		
5.	Material Thickness	Min 1.2mm		
6.	Number of Locks	Two		
7.	Protection	IP66 / NEMA 4X		
8.	Mounting	On Camera Pole / Ground mounted on concrete base		
9.	Form Factor	Rack Mount/DIN Rail		

#	Parameter	Minimum Specifications	Bidder Compliance (Y/N)	Product and Documentation Reference
10.	Other Features	Rain Canopy, Cable entry with glands and Fans/any other accessories as required for operation of equipment's within junction box.		

4.1.4 Camera Poles

#	Parameter	Minimum Specifications	Bidder Compliance (Y/N)	Product and Documentation Reference
1.	Make		<to be provided by the bidder>	
2.	Model		<to be provided by the bidder>	
3.	Pole type	Hot Dip Galvanized after Fabrication with Silver coating of 86 micron as per IS:2629; Fabrication in accordance with IS-2713 (1980)		
4.	Height	5-10 Meters, as-per-requirements for different types of cameras & Site conditions		
5.	Pole Diameter	Min. 10 cm diameter pole (bidder to choose larger diameter for higher height)		
6.	Cantilevers	Based on the location requirement suitable size cantilevers to be considered with the pole		
7.	Bottom base plate	Minimum base plate of size 30x30x15 cm		
8.	Mounting facilities	To mount CCTV cameras, Switch, etc.		
9.	Pipes, Tubes	All wiring must be hidden, through tubes/pipes. No wires shall be visible from outside.		
10.	Foundation	Casting of Civil Foundation with foundation bolts, to ensure vibration free erection (basic aim is to ensure that video feed		

#	Parameter	Minimum Specifications	Bidder Compliance (Y/N)	Product and Documentation Reference
		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.		
11.	Protection	Lightning arrester at select sites as per the requirements		
12.	Sign-Board	A sign board describing words such as "This area under surveillance" (in English and Hindi)		

4.1.5 Standardized Signs for CCTV Camera Locations

#	Parameter	Minimum Specifications	Bidder Compliance (Y/N)	Product and Documentation Reference
1.	Make		<to be provided by the bidder>	
2.	Model		<to be provided by the bidder>	
3.	Size	Board Width = 8" / 12" (For type A and B) Board Width = 12" / 18" / 24" (For type C and D)		
4.	Plate Material	Corrosion resistant Aluminium Alloy as per IRC 67:2001 (Code of Practice for Road signs)		
5.	Plate Thickness	Minimum 1.5 mm		
6.	Retro-Reflective sheeting for sign-plate	Weather-resistant, having colour fastness		
7.	Other Specifications	As per IRC 67:2001 (Code of Practice for Road signs)		
8.	Mounting	Can be mounted on wall or pole (appropriate mounting brackets to be provided)		
9.	Design	Aesthetically designed as per industry standard		

4.1.6   Junction Boxes

The junction box shall be fitted in secure locations (not easily accessible to the general public) and shall be fitted with a standard cabinet lock. Roadside cabinets shall be secured with anti-tamper fixings in addition to the standard cabinet lock.

- Each Junction box shall be fitted with sufficient screw type terminals to terminate all pairs used and unused. The terminal blocks shall be certified for use with the box.
- Each box shall be equipped with certified cable glands/plug and with earthing bar.
- Cable continuity shall be through junction box dedicated terminals.
- Junction box shall be weather proof to IP 65 as minimum.

4.2   Command Control & Communication Centre (CCCC / C4)

4.2.1   Command Control and Communication Centre Application

#	Functions	Minimum Specifications	Bidder Compliance (Y/N)	Product Documentation Reference
1.	Make		<to be provided by the bidder>	
2.	Model		<to be provided by the bidder>	
3.	Solution & Platform	The Command & Control solution should adhere to the principles & guidelines of open standards published by GoI.		
4.		Must have built-in fault tolerance, load balancing and high availability & must be certified by the OEM.		
5.		Software (Application, Database and any other) must not be restricted by the license terms of the OEM from scaling out on unlimited number of cores and servers during future expansion.		
6.		The CCA should have the capability to integrate with GIS.		
7.		It shall provide complete view of facilities, sensors, and alarms in an easy-to-use and intuitive GIS-enabled graphical interface with a powerful workflow and business logic engine.		
8.		The system shall integrate with GIS and map information and be able		

#	Functions	Minimum Specifications	Bidder Compliance (Y/N)	Product Documentation Reference
		to dynamically update information on the GIS maps to show status of resources.		
9.		The system shall provide CCA operators and managers with a management dashboard that provides a regular 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.		
10.		System must provide a comprehensive API (Application Programming Interface) or SDK (Software Development Kit) to allow interfacing and integration with existing systems.		
11.		The solution should be network and protocol agonistic and provide option to connect legacy system through API's with either read, write or both options. It should connect diverse on premise and/or cloud platform's and make it easy to exchange data and services between them.		
12.		The system shall allow seamless integration with all of the existing and future initiatives of RSCCL and related departments/agencies like Police etc.		
13.		The platform should be able to integrate with any type of sensor platform being used for the urban services irrespective of the underlying technology used.		
14.		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		

#	Functions	Minimum Specifications	Bidder Compliance (Y/N)	Product Documentation Reference
		water/energy meters from different OEMs etc.) and provide secure access to that data using data API(s) to application developers		
15.	Application Graphical User Interface (GUI)	▪ Solution should present information on standard Windows based workstations and terminals. ▪ Application GUI should have the following capabilities as standard: ✓ GUI shall be able to present management data such as dashboards, alarm and alerts, resource management information, incident information in colour coded, clear, simple and unambiguous, logical format. ✓ The colour coding on the CCA GUI shall represent the different status of a task or incident / alert. ✓ The GUI layout and arrangement of windows shall be user customizable. ✓ Be able to present information and distinguish between an "early warning or anticipation" type set of data and "emergency or crisis" operating mode. ✓ Solution should be capable of presenting information in a browser based format such that it is accessible from any terminal with a web-browser. The supported browser should include, but not limited to, Internet Explorer, Chrome, Firefox and Safari		

#	Functions	Minimum Specifications	Bidder Compliance (Y/N)	Product Documentation Reference
		✓ Solution should be capable of showing still as well as video imagery. ✓ Solution shall also be able to present information on mobile devices such as tablets, smartphones and tablet type devices while maintaining the basic UI features such as user friendliness, colour coding etc.		
16.		The solution should be capable of providing the following features for still imagery: ▪ system shall have a thumbnail gallery to display all imported images ▪ system shall be able to import pictures from still imagery cameras ▪ system shall be able to import pictures from local hard drives ▪ system shall be able to share the imported images with other users ▪ system shall time and date stamp any imported images ▪ system shall have the ability to view each still image full screen ▪ system shall have the ability to zoom in an out of a still image when viewed full screen ▪ system shall allow the image to be imported to the planning whiteboard module ▪ system shall enable users to add tags to images for easy search and retrieval later ▪ system shall enable users to group and title images together for easy retrieval		
17.		Solution should be capable of providing the following features for video imagery:		

#	Functions	Minimum Specifications	Bidder Compliance (Y/N)	Product Documentation Reference
		▪ system shall be able to display video imagery ▪ system shall have a thumbnail gallery to display all video images ▪ system shall allow the video streams to be grouped and titled as per defined requirements ▪ presentation server shall have the capability of only refreshing those elements of the GUI that have changed state		
18.	General System Display	▪ Shall have the facility to view and handle multiple alarms at one time ▪ Shall have the facility to view multiple video windows at one time. Operators shall be able to resize and move video windows. ▪ Shall have the facility to view windows in a single monitor or across multiple monitors ▪ Shall have the facility to access, display and manage incidents/alarms and related sensors data and information from subsystem based on priority and authority level. ▪ Shall view and manage detailed response procedures and tasks ▪ Shall enable a single operator or multiple operators to monitor and control commands from connected subsystems, including all operational capabilities for detection, assessment, notification, entry control, and communications ▪ Shall provide the rapid annunciation and display of alarms to facilitate evaluation and assessment		

#	Functions	Minimum Specifications	Bidder Compliance (Y/N)	Product Documentation Reference
19.	GIS Display	▪ Shall view the environment through geospatial or fixed composite computer-generated(JPEG, BMP, AutoCAD, etc.) map ▪ Should allow user to view sensor and related name from the displayed map ▪ Should allow all resources, objects, sensors and elements on the map to be geo-referenced such that they have a real world coordinate. ▪ Should visually display a camera sensor with related camera orientation, camera range and camera field of view angle. ▪ Should visually display an alarming sensor on map ▪ Should visually differentiate sensor alarm severities on map through different color and icon identifiers ▪ Should immediately view alarm details (including description, video, etc.) and investigate the alarm from the map ▪ Should allow user to choose camera and other sensors from map to view live video and the data ▪ Should allow user to choose camera and take live video image snapshot and save to file from any camera ▪ Should allow user to choose camera from map to move PTZ cameras ▪ Should allow user to choose camera to play, pause, stop, fast-forward, rewind, and play recorded video from preset time		

#	Functions	Minimum Specifications	Bidder Compliance (Y/N)	Product Documentation Reference
		- Should allow user to choose camera and take recorded video image snapshot and save to file or print from any live or recorded video - Should allow user to jump from one map to the next with a single click of a mouse with map links - Should allow map information "layers" to be displayed/hidden on items such as – - Sensor names - Sensors - Sensor range (e.g. camera – orientation, range, field of view angle) - Locations and zones - Perimeter ranges - Resource tracks - Allow user to zoom in/out on different regions of map graphic		
20.	Convergence of Multiple feeds / services	System need to have provision that integrates various services and be able to monitor them and operate them. The solution should provide option to integrate existing deployed solution by City and also need to provide scalability option to implement new use cases. System should have capability to source data from various systems implemented in Ranchi (being implemented as part of this project or other projects) to create actionable intelligence.		
21.	Industry Standards for the Command and Communications Center	The solution should adhere to the industry standards for interoperability, data representation & exchange, aggregation, virtualization and flexibility		

#	Functions	Minimum Specifications	Bidder Compliance (Y/N)	Product Documentation Reference
22.		IT Infrastructure Library (ITIL) standards for Standard Operations Plan & Resource Management		
23.		Geo Spatial Standards like GML & KML etc.		
24.		Business Process Model and Notation (BPMN) or equivalent for KPI Monitoring.		
25.	Analytics Engine	Analytics Engine module should have below intelligence capabilities; a) Advanced Predictive Analytics should be part of the solution. b) The solution should be able to predict insights consuming data from city infrastructure viz., Traffic, Parking, Lighting etc. c) The solution should be able to predict and integrate with Smart City solutions helping in driving operational policies creation. d) The solution should be robust, secure and scalable. e) The solution should have a visualization platform to view historic analytics, predictive analytics such as to enable department to implement the corrective actions and remedial measures		
26.		The application should enable the users to discover, compare, and correlate data across heterogeneous data sources to unravel the patterns that are previously hidden. At a broader level, when you work with the		

#	Functions	Minimum Specifications	Bidder Compliance (Y/N)	Product Documentation Reference
		application, system do the following tasks: a) Connect to a variety of data sources b) Analyze the result set c) Visualize the results d) Predict outcomes		
27.	Supported Data sources and types	Analytics Engine should support multiple and diverse Data Sources and types.		
28.		▪ Analytics Engine should provide analysis of data from a selected data source(s). ▪ Analytics engine should provide capability to check analysis with multiple predictive algorithms		
29.	Analytics Engine Visualizations	▪ Analytics Engine should provide visualizations dashboard. ▪ In the visualization workspace it should allow to change visual attributes of a graph. ▪ User should not be allowed to alter the graph/visualization definition. ▪ In the visualizations workspace, user should able to do the following operations: a) Change the graph/visualization type b) Print the graph c) Export the graph d) Narrow down on the value ranges e) Toggle the axis labels f) Integrate with other 3rd		

#	Functions	Minimum Specifications	Bidder Compliance (Y/N)	Product Documentation Reference
		party applications seamlessly		
30.	Components	Web server to manage client requests. Client should provide web-based, one-stop portals to event information, overall status, and details. The user interface (UI) to present customized information in various preconfigured views in common formats. All information to be displayed through easy-to-use dashboards.		
31.		▪ System Platform – The platform should provide a common data integration layer which can collect and contextualize information from disparate data sources regardless of protocol. ▪ Workflow and Incidents Lifecycle engine – This function should allow users to define and modify new workflows. The workflow could cut across multiple system via the interfacing modules. Workflow for operational alerts and escalation should be triggered automatically without human intervention. ▪ Workflow approvals should have facility to approve from any device with e-signature. ▪ This function should provide facility to trigger a corrective action workflow and define the stakeholders for the same. Should manage the life cycle of incidents and related entities via pre-define workflows. The workflow could cut across multiple systems via the interfacing modules. Workflow for operational alerts and		

#	Functions	Minimum Specifications	Bidder Compliance (Y/N)	Product Documentation Reference
		escalations should be triggered automatically without human intervention. ▪ Incidents Planning – should manage the planning preparations of an incident including resource allocation, tasks management etc. ▪ Analytics and MIS – should provide users with business analytics reporting and tools to organize, evaluate and efficiently perform day to day operations ▪ Security & Roles – should manage roles definition for internal as well as external access ▪ Centralized data archiving for operational data: Should provide facility for centralized storage of operational data (time-series or transactional) with high granularity and data compression capability ▪ Mobility: should enable app-based access to monitor alerts, KPI, KOPs, SOPs and reports to mobile users. Should support popularly user's smartphone /tablets. App content should be presented in context to the user role.		
32.		Application server to provide a set of services for accessing and visualizing data. Should be able to import data from disparate external sources, such as databases and files. It should provide the contacts and instant messaging service to enable effective, real-time communication. It should provide business monitoring service to monitor incoming data records to generate key		

#	Functions	Minimum Specifications	Bidder Compliance (Y/N)	Product Documentation Reference
		performance indicators. It should also provide the users to view key performance indicators, standard operating procedures, notifications, and reports, spatial-temporal data on a geospatial map, or view specific details that represent a city road, building or an area either on a location map, or in a list view. The application server should provide security services that ensure only authorized users and groups can access data. Analytics functionality can be part of application server or separate server		
33.	Video Display	▪ Shall view live or recorded video from resizable and movable windows ▪ Should have an ability to perform video controls for video systems from workstation ▪ Shall play, fast-forward, rewind, pause, and specify time to play recorded video ▪ Shall take a video still image (snapshot) from live or recorded video ▪ Shall export video for user specified time and duration ▪ Shall have the capability to move PTZ cameras ▪ Shall view Video in Video Matrix ▪ Shall display in 1x1, 2x2, 3x3 and 4x4 window formats ▪ Shall enable operator to specify video windows to be displayed in matrix ▪ Shall enable matrix settings to be saved per user ▪ Shall view either live or recorded video can be		

#	Functions	Minimum Specifications	Bidder Compliance (Y/N)	Product Documentation Reference
		displayed in the video matrix window ▪ Shall enable video snapshot to be taken and saved from any window pane in the matrix view ▪ Shall rotate video in "virtual" video guard tour ▪ Shall rotate through multiple video views based on predefined video camera sequence and duration. ▪ Shall enable the user to pause the rotation of video and resume the video rotation again ▪ Shall enable times between new video to be adjusted ▪ Shall enable both live video and recorded video to be played through the video guard tour. ▪ Shall enable alarms to be generated from any video pane ▪ Shall enable user to only view and control video for which they have been assigned permissions by the administrator ▪ Shall manually create an alarm from the live or recorded video with specified severity and description		
34.	Incident Management Requirements	The system must provide Incident Management Services to facilitate the management of response and recovery operations:		
35.		Should support comprehensive reporting on event status in real time manually or automatically by a sensor/CCTV video feeds.		
36.		Should support for sudden critical events and linkage to standard operating procedures automatically without human intervention.		

#	Functions	Minimum Specifications	Bidder Compliance (Y/N)	Product Documentation Reference
37.		Should support for multiple incidents with both segregated and/or overlapping management and response teams.		
38.		Should support Geospatial rendering of event and incident information.		
39.		Should support plotting of area of impact using polynomial lines to divide the area into multiple zones on the GIS maps.		
40.		Should support incorporation of resource database for mobilizing the resources for response.		
41.		Should provide facility to capture critical information such as location, name, status, time of the incident and be modifiable in real time by multiple authors with role associated permissions (read, write). Incidents should be captured in standard formats to facilitate incident correlation and reporting.		
42.		The system must identify and track status of critical infrastructure / resources and provide a status overview of facilities and systems		
43.		Should provide detailed reports and summary views to multiple users based on their roles.		
44.		A Reference Section in the tool must be provided for posting, updating and disseminating plans, procedures, checklists and other related information.		
45.		Provide User-defined forms as well as Standard Incident Command Forms for incident management.		
46.	Integrated User Specific & Customizable Dashboard	Should provide integrated dashboard with an easy to navigate user interface for managing profiles, groups, message templates, communications, tracking receipts and compliance		

#	Functions	Minimum Specifications	Bidder Compliance (Y/N)	Product Documentation Reference
47.		▪ Collects major information from other integrated City sensors/platforms. ▪ Should allow different inputs beyond cameras, such as, PC screen, web page, and other external devices for rich screen layout ▪ Multi-displays configurations ▪ Use of, GIS tool which allows easy map editing for wide area monitoring (Google map, Bing map, ESRI Arc GIS map, etc.).		
48.		Should provide tools to assemble personalized dashboard views of information pertinent to incidents, emergencies & operations of command Centre		
49.		Should provide historical reports, event data & activity log. The reports can be exported to pdf or html formats		
50.		Should provide dashboard filtering capabilities that enable end-users to dynamically filter the data in their dashboard based upon criteria, such as region, dates, product, brands, etc. and capability to drill down to the details		
51.	Integration with Social Media & Open Source Intelligence	Should provide integration of the Incident Management application with the social media. Should Provide analytics based on the social media feed collected from the open source intelligence and collate with the surveillance inputs to alert the responders for immediate action on the ground		
52.		Should extract messages and display it in an operational dashboard		
53.		Should be able to correlate the extracted message from the social media with existing other events		

#	Functions	Minimum Specifications	Bidder Compliance (Y/N)	Product Documentation Reference
		and then should be able to initiate an SOP		
54.		Should be able to identify the critical information and should be able to link it to an existing SOP or a new SOP should be started		
55.		Should provide notifications to multiple agencies and departments (on mobile) that a new intelligence has been gathered through open source		
56.	Device Status, Obstruction Detection and Availability Notification	Should provide icon based user interface on the GIS map to report non-functional device.		
57.		Should also provide a single tabular view to list all devices along with their availability status in real time.		
58.		Should provide User Interface to publish messages to multiple devices at the same time.		
59.	Event Correlation	Solution should be able to correlate two or more events coming from different subsystems (incoming sensors) based on time, place, custom attribute and provide correlation notifications to the operators based on predefined business and operational rules in the configurable and customizable rule engine.		
60.	Standard Operations Procedures (SOP)	Command & Control Centre should provide for authoring and invoking un-limited number of configurable and customizable standard operating procedures through graphical, easy to use tooling interface.		
61.		Standard Operating Procedures should be established, approved sets of actions considered to be the best practices for responding to a situation or carrying out an operation.		

#	Functions	Minimum Specifications	Bidder Compliance (Y/N)	Product Documentation Reference
62.		The users should be able to edit the SOP, including adding, editing, or deleting the activities.		
63.		The users should be able to also add comments to or stop the SOP (prior to completion).		
64.		There should be provision for automatically logging the actions, changes, and commentary for the SOP and its activities, so that an electronic record is available for after-action review.		
65.		The SOP Tool should have capability to define the following activity types:		
66.		Manual Activity - An activity that is done manually by the owner and provide details in the description field.		
67.		Automation Activity - An activity that initiates and tracks a particular work order and select a predefined work order from the list.		
68.		If-Then-Else Activity - A conditional activity that allows branching based on specific criteria. Either enter or select values for Then and Else.		
69.		Notification Activity - An activity that displays a notification window that contains an email template for the activity owner to complete, and then sends an email notification.		
70.		SOP Activity – An activity that launches another standard operating procedure.		
71.	Key Performance Indicator	Solution should be able to facilitate measurement or criteria to assay the condition or performance of departmental processes & policies.		
72.	Reporting Requirements	Solution should provide easy to use user interfaces for operators such as Click to Action, Charting, Hover and Pop Ups, KPIs, Event Filtering,		

#	Functions	Minimum Specifications	Bidder Compliance (Y/N)	Product Documentation Reference
		Drill down capability, Event Capture and User Specific Setup		
73.		Solution should generate Customized reports based on the area, sensor type or periodic or any other customer reports as per choice of the administrators		
74.	Collaboration Tools	Should provide tools for users to collaborate & communicate in real-time using instant messaging features.		
75.	Communication Requirements	Provide the ability to search/locate resources based on name, department, role, geography, skill etc. for rapidly assembling a team, across department, divisions and agency boundaries, during emergency		
76.		Provide the capability to invite using information provided during the location of those individuals or roles, invite them to collaborate and to share valuable information.		
77.		Provide a single web based dashboard to send notifications to target audiences using multiple communication methods including voice-based notification on PSTN/Cellular, SMS, Voice mail, E-mail and Social Media		
78.		Provide dispatch Console integrates with various communication channels. It should provide rich media support for incidents, giving dispatchers the power to consolidate information relating to an incident and instantly share that information among responder teams. It should assess the common operating picture, identify & dispatch mobile resources available nearby the incident location. Augment resources from multiple agencies for coordinated response.		

#	Functions	Minimum Specifications	Bidder Compliance (Y/N)	Product Documentation Reference
79.	Authentication	Use authentication information to authenticate individuals and/or assign roles.		
80.	Instant messaging	Provide ability to converse virtually through the exchange of text, audio, and/or video based information in real time with one or more individuals within the emergency management community.		
81.	Events and Directives control	Should provide the capability for the events that are produced from a sub- system and are forwarded to the Command Control and Communication Center. Events could be a single system occurrence or complex events that are correlated from multiple systems. Events could be ad hoc, real-time, or predicted and could range in severity from informational to critical. At the center, the event should be displayed on an operations dashboard and analysed to determine a proper directive.		
82.		Directives issued by the Command & Control Centre should depend on the severity of the monitored event. Directives will be designed and modified based on standard operating procedures, as well as state legislation. A directive could be issued automatically via rules, or it could be created by the operations team manually.		
83.	What-if Analysis Tool	The solution should provide the capability to manage the emergencies and in-turn reducing risks, salvaging resources to minimize damages and recovering the assets that can speed up recovery.		
84.		To take proactive decisions that help minimize risks and damages,		

#	Functions	Minimum Specifications	Bidder Compliance (Y/N)	Product Documentation Reference
		the solution should provide Analytical and Simulation systems as part of the Decision Support System. The solution should help simulate what if scenarios. It should help visualize assets/resources at risk due to the pending/ongoing incident, should render impacted region on a GIS/3D map. The solution should help build the list of assets, their properties, location and their interdependence through an easy to use Graphical User Interface. When in What if Analysis mode the solution should highlight not only the primary asset impacted but also highlight the linked assets which will be impacted. The user should be able to run the What-if Analysis mode for multiple types of emergency events such as Bomb Blast, Weather events, Accidents etc.		
85.	Alert & Mass Notification Requirements	The system should provide the software component for the message broadcast and notification solution that allows authorized personal and/or business processes to send large number of messages to target audience (select-call or global or activation of pre-programmed list) using multiple communication methods including SMS, Voice, Email.		
86.		Provide function for creating the alert content and disseminating to end users. Provision of alerting external broadcasting organizations like Radio, TV, Cellular, etc., as web-service.		
87.	Security & Access Control	Provide Role based security model with Single-Sign-On to allow only authorized users to access and		

#	Functions	Minimum Specifications	Bidder Compliance (Y/N)	Product Documentation Reference
		administer the alert and notification system.		
88.	Internet Security	Provide comprehensive protection of web content and applications on back-end application servers, by performing authentication, credential creation and authorization.		
89.	API & Interface Security	Solution should provide an open standards based Integration Bus with API Management, providing full API lifecycle management with governance and security.		
90.	Authorization	System should offer comprehensive policy-based security administration to provide all users specific access based on user's responsibilities.		
91.	User group	Should provide support to enable assignment of permissions to groups, and administration of access control across multiple applications and resources. Secure, web-based administration tools to manage users, groups, permissions and policies remotely		
92.	Provide multi-dimensional access control	Provide policies using separate dimensions of authorization criteria like Traditional static Access Control Lists that describe the principals (users and groups) access to resource and the permissions each of these principals possess.		
93.	Flexible single sign-on (SSO)	SSO to Web-based applications that can span multiple sites or domains with a range of SSO options.		
94.	Authentication	Support LDAP authentication mechanism		
95.	Rule Engine & Optimization	Should have ability to respond to real-time data with intelligent & automated decisions		
96.		Should provide an environment for designing, developing, and		

#	Functions	Minimum Specifications	Bidder Compliance (Y/N)	Product Documentation Reference
		deploying business rule applications and event applications.		
97.		The ability to deal with change in operational systems is directly related to the decisions that operators are able to make		
98.		Should have at-least two complementary decision management strategies: business rules and event rules.		
99.		Should provide an integrated development environment to develop the Object Model (OM) which defines the elements and relationships		
100.	Task Management	The system should be able to create, assign, track and report on the lifecycle of tasks during a particular incident		
101.	Alarm Display	▪ Should have an ability to display alarm condition through visual display and audible tone. ▪ Should have an ability to simultaneously handle multiple alarms from multiple workstations ▪ Should have an ability to automatically prioritize and display multiple alarms and status conditions according to pre-defined parameters such as alarm type, location, sensor, severity, etc. ▪ Should display the highest priority alarm and associated data / video in the queue as default, regardless of the arrival sequence		
102.	Alarm Reporting	Should have an ability to generate a full incident report of the alarm being generated.		

#	Functions	Minimum Specifications	Bidder Compliance (Y/N)	Product Documentation Reference
103.	Integration capability	▪ Solution should aggregate various data feeds from sensors and systems and further process information out of these data feeds to provide interface /dashboards for generating alert and notifications in real time. ▪ Single Dashboard for City Infrastructure Management & Smart City Services for Smart Lighting, Utility/Surveillance System, GIS Services and Other Services of RSCCL work visualized real time on 2D/3D map of City. This dashboard can be accessed via web application as well as mobile app. The various information that may be accessed from the system but not limited to are as below: o Visual alerts generated by any endpoint that is part of the city infrastructure e.g. cameras, Wi-Fi points, sensors etc. that manages various city management use cases o Information about waste management resources through integration with existing and proposed solution o City environmental data o Take action based on events generated by any city infrastructure device ▪ Solution should provide reporting & audit trail functionalities to track all the information and monitor operator interactions with the system and to impart necessary training to the users		

4.2.2 Contact Centre

#	Minimum Requirements	Bidder Compliance (Yes/No)	Product Documentation Reference
1.	Make	<to be provided by the bidder>	
2.	Model	<to be provided by the bidder>	
3.	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.		
4.	Solution should be designed for upto 30 agents		
5.	IVRS should be modular and scalable in nature for easy expansion without requiring any change in the software.		
6.	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.		
7.	The callers should be able to access the various services through state-of-art centralized integrated Interactive Voice Response System (IVRS).		
8.	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.		
9.	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.		
10.	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 VoiceXML for ASR, TTS, and DTMF call flows e. be able to Read data from HTTP and XML Pages be able to run outbound campaigns		

11.	Automatic call distribution (ACD) solution should - a. be able to route the call to any remote call center agent using IP phones b. have an ability to queue or hold the call for an agent if none is immediately available c. have an ability to keep the callers informed as to the status of the call and providing information to callers while they wait in queue d. be able to perform prioritized call routing e. be highly available with hot standby and seamless failover in case of main server failure f. support skill based routing and it should be possible to put all the agents in to a single skill group and different skill groups g. support routing of incoming calls based upon caller input to menus, real-time queue statistics, time of day, day of week, ANI, dialed number etc. h. support call routing based on longest available agent, circular agent selection algorithms i. maintain log of all services offered which can be used for audit and analysis purpose. j. support the playing of customizable queuing announcements based upon the skill group that the call is being queued to, including announcements related to position in queue and expected delay k. allow agents to chat with other Agents or supervisor from the Agent desktop software l. allow supervisor to see the real-time status of agents, supervisors should be able to make agent ready or logout from the supervisor desktop m. support Queuing of calls and playing different prompts depending on the type of call and time in the queue		
12.	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.		
13.	Solution should have automatic identification of incoming number based on landline and mobile number mapping		

14.	Solution should support call recording mapped to incident tickets		
15.	Solution should offer customizable agent and supervisor desktop layout		
16.	Solution should offer Inbound and outbound capability		
17.	Solution should provide facilities for outbound calling list management, and software based predictive or preview dialing		
18.	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.		
19.	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.		
20.	Should intelligently and automatically responds to email inquiries or routes inquires with skills based routing discipline to agents		
21.	Live data reporting gadgets		
22.	Multiline support		
23.	Speed dial in IP phones		
24.	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
		  o a caller whose call is being attended by the agent
		  o Call routing facilities such as business rule based routing, skills-based routing etc.		

25.		Supervisor Module
		▪ The call centre should provide a graphical console application program for the supervisor's workstation. This position shall facilitate the following features:-
		  o Any supervisor shall be able to monitor or control any group in the call Centre
		  o 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.
		  o Supervisor console shall also graphically display live status of the call session summary, number of call waiting in the queue, call traffic etc.
		  o Live status of the group shall be shown, including waiting calls and calls being answered currently.
		  o Access to the supervisor console shall be restricted.
		  o It shall be possible for a supervisor to attend calls whenever necessary.		

26.		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. ▪ 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.		

27.	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 reports:
	  o List of users, user privileges and status
	  o User sign-off and sign-on
	  o User violation – unsuccessful logon attempts
	  o User additions, amendments and deletions with before & after image		

4.2.3 IP Push to Talk (interpretability Communication Channel)

#	Minimum Requirements	Bidder Compliance(Yes/No)	Product Documentation Reference
1	Make	<to be provided by the bidder>	
2	Model	<to be provided by the bidder>	
3	IP Push to Talk Radio: Instant communication to critical first responders via push to talk over IP. This will enable All communication across various business sites.		
4	The radio over IP solution must integrate any analog or digital radio system, any to any Push To Talk (PTTT) communications.		
5	The system shall create virtual talk groups (VTGs) to facilitate Push-to-Talk (PTT) communications between users of multiple types and technologies of Land Mobile Radios with users of PCs, landline phones, cellular and android phones, and IP phones.		
6	The system shall provide a High Availability option of adding a secondary hot standby server to provide high availability with no single point of failure. If a primary server fails, the secondary server automatically takes over service without communication interruption		
7	The solution must send encrypted data for PTT communications.		
8	The system shall provide a web service API to integrate System with third party applications, such as Command and Control		
9	The system shall support role-based management to provide compartmentalized functions for personnel who need to perform different roles.		
10	System shall provide an easy-to-use Web interface. Authorized personnel shall be able to access the System Server from any location by using a supported browser and a network connection		

#	Minimum Requirements	Bidder Compliance(Yes/No)	Product Documentation Reference
11	Integrate with IP phones to talk to radio walkie talkies / Any other compatible Phone		
12	The system shall provide Loop Prevention: As multiple dispatchers patch channels together, there is always the possibility of creating a channel loop that causes audio feedback into the communication path. The system should automatically identify potential audio loops and resolve them before they become an issue		
13	The System Server shall provide an audit trail for analysis, critique, and operations management. Detailed activity logging shall allow administrators to determine which user actions were performed and when they were performed		

4.2.4 Video Display Wall (VDM)

#	Minimum Specifications	Bidder Compliance (Yes/No)	Product Documentation Reference
1.	Make	<to be provided by the bidder>	
2.	Model	<to be provided by the bidder>	
3.	VDW shall be made up of DLP™ rear-projection cubes.		
4.	Seamless Video wall of DLP Cubes. Each cube size to be 70" (70 Inches diagonally) or more with complete configuration of (5 cubes x 3 cubes) with covered base. All cubes have to be of the exactly same size, configuration and model wise mandatorily. The wall to be installed in curved fashion with all required support system like Controller / stand for DLP Cubes / Interfaces / Connecting cables.		
5.	The native resolution of each Visual Display Unit / Rear Projection Module should be 1920 X 1080 pixels (Full HD) and should have LED as its light source with ultra-thin configuration.		
6.	Cubes shall have an aspect ratio of 16:9.		
7.	Dynamic contrast should be 1,200,000:1 or better		
8.	The Rear Projection Module shall have LED or laser as its light source.		
9.	The Cube shall have redundancy in power supply, LED light source.		
10.	The brightness uniformity of the VDM shall be >95%.		
11.	The light source lifetime of the LED shall be at least 90,000 hours. This should be certified by the OEM.		
12.	The inter screen gap (bezel gap) should be <0.4 mm.		
13.	Each cube of the VDW shall have its own IP address and on-board web server to provide standard information like status and health.		
14.	Other requirements - ▪ RS232 control (with loop-through) ▪ On Screen Display (OSD) ▪ IR remote control ▪ flicker free image on the Large Screen		
15.	VDW should be able to show the images of the monitor, which is connected on the LAN with		

#	Minimum Specifications	Bidder Compliance (Yes/No)	Product Documentation Reference
	various OS and the windows should be freely resizable, scalable and repositionable on any part of the large video screen. VDW shall provide image uniformity across the whole display area		
16.	VDW should provide real-time clear luminous view to share information between operators and decision makers. The operators whose systems are on the same Ethernet should be able to work on the large screen sitting at their own position with their own workstation.		
17.	VDW shall include video walls mounted close to each other to give a seamless viewing experience.		
18.	VDW shall be the primary visual information point to see CCTV videos, incident alarms, IoT screens, network health conditions, GIS maps, and any application running on city systems.		
19.	VDW shall provide a collaborative visual for operators and management to work and coordinate on various tasks in different situations.		
20.	The dashboard shall be capable of simultaneously displaying one (1) to one hundred (100) independent sets of information on the video display wall. Specific outputs to be displayed shall be chosen by operators.		
21.	VDW shall have system availability with limited maintenance and low disruption of the operations room operations.		
22.	VDW shall be capable of displaying high definition (HD) and standard definition (SD) content.		
23.	VDW shall provide minimum viewing angles of: ▪ Horizontal - ½ gain: ±35 degrees, 1/10 gain: ±57degrees ▪ Vertical - ½ gain ±10 degrees, 1/10 gain: ±28 degrees		
24.	Auto colour and brightness management mechanism to be provided.		
25.	Screen should have an anti-reflective glass backing to prevent bulging.		
26.	All video display cubes shall have a consistent image quality and uniform brightness across the display wall.		

#	Minimum Specifications	Bidder Compliance (Yes/No)	Product Documentation Reference
27.	Input - Analog D-sub/Ethernet/Digital DVI/Digital HDMI (as per solution)		
28.	Each display cube shall not exceed a thermal dissipation of eight hundred (800) BTU per hour under normal operating conditions.		
29.	The VDW units shall be new and current to the manufacturer's product line. The units shall not be discontinued products.		
30.	A pedestal shall be provided to support the VDW. Pedestal shall be physically secured to the concrete floor of the building. Support structure shall be with a laminate finish. Support structure shall incorporate sound proofing to prevent noise penetration from the equipment into the command centre.		
31.	Each VDW projection engine shall be modular to allow sub-components to be replaced without disruption to other components.		
32.	The VDW shall have an operational temperature between ten degrees Celsius (10°C) to thirty degrees Celsius (40°C).		
33.	The AC input power shall be 110-240 VAC +/- 10% at 50/60 Hz +/- 1Hz. Power consumption of each cube shall be less than 350W.		
34.	The VDW shall have a relative humidity of 20 to 80%, non-condensing or better.		
35.	The VDW shall be of sufficient design, manufacturing and operational quality to provide 24x7 mission critical functionality.		
36.	Warranty: 5 Years		

4.2.5 Video Wall Controller

#	Parameters	Minimum Requirements	Bidder Compliance (Yes/No)	Product Documentation Reference
1	Make		<to be provided by the bidder>	
2	Model		<to be provided by the bidder>	
3	Controller	Controller to control Video wall in a matrix as per requirement along with software		
4	Chassis	19" Rack mount		

Selection of Master System Integrator (MSI) for Implementation of Command Control and Communication Centre (C4) under Smart City Mission in Ranchi

#	Parameters	Minimum Requirements	Bidder Compliance (Yes/No)	Product Documentation Reference
5	Processor	Latest Generation 64 bit x86 Quad Core processor (3.4 Ghz) or better		
6	Operating System	Pre-loaded 64-bit Operating System Windows / Linux / Equivalent, with recovery disc		
7	RAM	16 GB DDR3 or higher ECC RAM		
8	HDD	2x500 GB 7200 RPM HDD (Configured in RAID 0) or SAS drives with equivalent storage capacity		
9	Networking	Dual-port Gigabit Ethernet Controller with RJ-45 ports		
11	RAID	Should support all RAID levels		
12	Power Supply	(1+1) Redundant hot swappable		
13	Input/ Output support	VI/HDMI/USB/ LAN/ VGA/SATA port		
14	Accessories	104 key Keyboard and Optical USB mouse		
15	USB Ports	Minimum 4 USB Ports		
16	Redundancy support	Power Supply, HDD, LAN port & Controller		
17	Scalability	Display multiple source windows in any size, anywhere on the wall		
18	Control functions	Brightness/ Contrast/ Saturation/ Hue/ Filtering/ Crop/ Rotate		
19	Inputs	To connect to minimum 2 sources through HDMI		
20	Output	To connect to minimum 16 Displays through HDMI		
21	Operating Temperature	10°C to 35°C, upto 80 % Humidity		
22	Cable & Connections	Successful bidder should provide all the necessary cables and connectors, so as to connect Controller with LED Display units		

4.2.6 Video Wall Management Software

#	Parameter	Minimum Specifications	Bidder Compliance (Yes/No)	Product Documentation Reference
1.	Make		<to be provided by the bidder>	
2.	Model		<to be provided by the bidder>	
3.	Display & Scaling	Display multiple sources anywhere on display up to any size		
4.	Input Management	All input sources can be displayed on the video wall in freely resizable and movable windows		
5.		Should be able to display visual content on any network attached display device		
6.		Solution should enable various operators to access the display wall from the local keyboard and mouse of their workstation connected with the DCMS and Video Wall on the Ethernet.		
7.		Should be able to input, manage, and distribute visual content, including digital CCTV video, web pages, CATV, workstation applications, and active screens from any networked workstation.		
8.	Scenarios management	Save and Load desktop layouts from Local or remote machines		
9.	Layout Management	Support all Layout from Input Sources, Internet Explorer, Desktop and Remote Desktop application		
10.	Multi View Option	Multiple view of portions or regions of Desktop, Multiple Application Can view from single desktop		
11.		Solution should be able display multiple sources anywhere on video wall in any size.		
12.		Solution should be able to stretch, re-position, and resize any video source on any display device.		
13.		Solution should treat the VDW as a single display. It shall act as a		

#		Minimum Specifications	Bidder Compliance	Product Documentation Reference
		single canvas with no pixel separation.		
14.	Other features	SMTP support		
15.		Remote Control over LAN		
16.		Solution should include an administrator role that shall be able to manage system configuration, sources, user groups, and user authentication.		
17.		Alarm management		
18.		Remote management		
19.		Multiple		
20.		concurrent client		
21.		shall allow 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		
22.		KVM support		
23.	Cube Management	Cube Health Monitoring		
24.		Pop-Up Alert Service		
25.	nt	Graphical User Interface		

4.2.7 Monitoring Workstations

#	Parameter	Minimum Specifications	Bidder Compliance (Yes/No)	Product Documentation Reference
1.	Make		<to be provided by the bidder>	
2.	Model		<to be provided by the bidder>	
3.	Processor	Latest generation 64bit x86 Quad core processor(3Ghz) or better		
4.	Chipset	Latest series 64bit Chipset		
5.	Motherboard	OEM Motherboard		
6.	RAM	32GB (2x16GB) 2133MHz DDR4 Non-ECC scalable up to 64GB		

#	Parameter	Minimum Specifications	Bidder Compliance (Yes/No)	Product Documentation Reference
7.	Graphics card	NVIDIA Quardro 4 GB DDR5 Graphics card with OpenGL or higher		
8.	HDD	2 TB SATA-3 Hard Drive @7200 rpm or higher. Provision for installing 4 more drives.		
9.	Media Drive	NO CD / DVD Drive		
10.	Network interface	10/100/1000 Mbps autosensing on board integrated RJ-45 Ethernet port.		
11.	Audio	Line/Mic IN, Line- out/Spr Out (3.5 mm)		
12.	Ports	Minimum 6 USB (3.0/2.0) ports (out of that at least 2 in the front)		
13.	Keyboard	minimum 104 keys keyboard of similar make of OEM		
14.	Mouse	2 button optical scroll mouse (USB) of similar make of OEM		
15.	PTZ joystick controller (with 10 of the workstations in CCCC)	▪ 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		
16.	Monitor (OEM monitors of same make to be provided)	▪ Two monitors of 24" TFT LED monitor ▪ Minimum 1920 x1080 resolution, 5 ms or better response time ▪ Thin bezel not exceeding ½ inch ▪ Minimum input of 1xDP, 1x HDMI, 1xDVI ▪ Energy Saving ▪ Allow tilt and swivel motion ▪ Black colour		

#	Parameter	Minimum Specifications	Bidder Compliance (Yes/No)	Product Documentation Reference
		▪ TCO 05 (or higher) certified ▪ Monitor shall have high refresh rate to eliminate screen flicker causing eyestrain and headache ▪ Monitor shall have adjustment controls (e.g. brightness/contrast) easily accessible, easy to locate and easy to use		
17.	Certification	Energy star 5.0/BEE star certified		
18.	Operating System	64 bit pre-loaded Windows® 10 Professional OS with recovery media		
19.	Security	BIOS controlled electro-mechanical internal chassis lock for the system.		
20.	Antivirus feature	Advanced antivirus, antispyware, desktop firewall, intrusion prevention (comprising of a single, deployable agent) which can be managed by a central server. (Support, updates, patches and errata for the entire contract/ project period)		
21.	Power supply	SMPS; Minimum 350- watt Continuous Power Supply with Full ranging input and APFC. Power supply should be 90% or better efficient with EPEAT Gold certification for the system.		

4.2.8 Desktops for Helpdesk

#	Parameter	Minimum Specifications	Bidder Compliance (Yes/No)	Product Documentation Reference
1.	Make	<to be provided by the bidder>		
2.	Model	<to be provided by the bidder>		

#	Parameter	Minimum Specifications	Bidder Compliance (Yes/No)	Product Documentation Reference
3.	Processor	Intel Core i5-latest generation (3.0 Ghz) or higher		
4.	Memory	8 (8x1) GB DDR4 RAM @ 2133 MHz. One DIMM Slot must be free for future upgrade		
5.	Motherboard	OEM Motherboard		
6.	Hard Disk Drive	Minimum 500 GB SATA III Hard Disk @7200 RPM or higher		
7.	Audio	Line/Mic In, Line-out/Speaker Out (3.5 mm)		
8.	Network port	10/100/1000 Mbps auto-sensing on-board integrated RJ-45 Ethernet Port		
9.	Wireless Connectivity	Wireless LAN - 802.11b/g/n/		
10.	USB Ports	Minimum 6 USB (2.0/3.0) ports (at-least 2 in front)		
11.	Display Port	Minimum 1 HDMI/VGA port		
12.	Keyboard	104 keys Heavy Duty Mechanical Switch Keyboard (USB Interface) with 50 million keystrokes life per switch. Rupee Symbol to be engraved.		
13.	Mouse	Optical scroll with USB interface (same make as desktop)		
14.	Monitor	Minimum 18.5" diagonal LED Monitor with 1366x768 or higher resolution. (Same make as desktop). Must be TCO-05 certified.		
15.	Operation System and Support	Pre-loaded Windows 10 (or latest) Professional 64 bit, licensed copy with certificate of authenticity (or equivalent authenticity information) and all necessary and latest patches and updates. All Utilities and driver software, bundled in CD/DVD/Pen-drive media.		

#	Parameter	Minimum Specifications	Bidder Compliance (Yes/No)	Product Documentation Reference
16.	Certification for Desktop	Energy Star 5.0 or above / BEE star certified | RoHS complaint		

4.2.9   LED Display

#	Parameter	Minimum Specifications	Bidder Compliance (Yes/No)	Product Documentation Reference
1.	Make	<to be provided by the bidder>		
2.	Model	<to be provided by the bidder>		
3.	Technology	HD IPS LED Display, Direct LED Backlight		
4.	Screen Size	55 inch diagonal or better		
5.	Resolution	Full high definition (Min 1920 x 1080) 16:9 Widescreen		
6.	Contrast ratio	5000:1		
7.	Brightness	350 nit		
8.	Viewing angle	178 degree/178 degree (H/V) or better		
9.	Response time	8ms		
10.	Control	RS232 control On Screen Display (OSD) IR remote control		
11.	Operations	24x7		

4.2.10 Ceiling Speakers

#		Minimum Specifications	Bidder Compliance (Yes/No)	Product Documentation Reference
1.	Make	<to be provided by the bidder>		
2.	Model	<to be provided by the bidder>		
3.	The ceiling speakers shall have high power and high sensitivity with extended frequency responses.			
4.	The ceiling speakers shall have wide, controlled constant directivity dispersions for optimum coverage.			

#	Minimum Specifications	Bidder Compliance (Yes/No)	Product Documentation Reference
5.	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.		
6.	The ceiling speakers shall have a conical coverage pattern of at least 105 degrees (1kHz – 6 kHz).		
7.	The ceiling speakers shall be in a colour to match the ceiling and surrounding interior design.		
8.	The ceiling speaker shall have a diameter not greater than 8.5".		
9.	MSI shall quantify and space speakers to provide full audio coverage within the command centre room and conference room.		
10.	The ceiling speakers shall follow the manufacturer recommendation for connectivity.		
11.	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.		
12.	The ceiling speakers shall be operational in temperature between ten degrees Celsius (10°C) to forty degrees Celsius (40°C).		

4.2.11 IP Phones

#	Parameter	Minimum Specifications	Bidder Compliance (Yes/No)	Product Documentation Reference
1.	Make		<to be provided by the bidder>	
2.	Model		<to be provided by the bidder>	

#	Parameter	Minimum Specifications	Bidder Compliance (Yes/No)	Product Documentation Reference
3.	Display	2 line or more, Monochrome display for viewing features like messages, directory		
4.	Integral switch	10/100 mbps for a direct connection to a 10/100BASE-T Ethernet network through an RJ-45 interface		
5.	Speaker Phone	Yes		
6.	Headset	Wired, Cushion Padded Dual Ear- Speaker, Noise Cancelling headset		
7.		with mouthpiece microphone, port compatibility with IP Phone		
8.	VoIP Protocol	SIP V2		
9.	POE	IEEE 802.3af or better and AC Power Adpater (Option)		
10.	Supported Protocols	SNMP, DHCP, DNS		
11.	Codecs	G.711, G.722, G.729 including handset and speakerphone		
12.	Speaker Phone	Full duplex speaker phone with echo cancellation Speaker on/off button, microphone mute		
13.	Volume control	Easy decibel level adjustment for speaker phone, handset and ringer		
14.	Phonebook/ Address book	Minimum 100 contacts		
15.	Call Logs	Access to missed, received, and placed calls. (Minimum 20 overall)		
16.	Clock	Time and Date on display		
17.	Ringer	Selectable Ringer tone		
18.	Directory Access	LDAP standard directory		
19.	QoS	QoS mechanism through 802.1p/q		

4.2.12 IP PBX (Call Control System)

#	Minimum Specifications	Bidder Compliance (Yes/No)	Product Documentation Reference
1.	Make	<to be provided by the bidder>	
2.	Model	<to be provided by the bidder>	
3.	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		
4.	The single IP PBX system should be scalable to support up to 500 stations (any mix/percentage of Analog/IP) to achieve the future capacity		
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, Voice Gateway) should be from a single OEM		
	Support for call-processing and call-control		
10.	Should support signaling standards/Protocols – SIP, MGCP, H.323, Q. Sig		
11.	Voice Codec support - G.711, G.729, G.729ab, g.722, ILBC		
12.	The System should have GUI support web based management console Security		
13.	The protection of signaling connections over IP by means of authentication, Integrity and encryption should be carried out using TLS		
14.	System should support MLPP feature		
15.	Proposed system should support SRTP for media encryption and signaling encryption by TLS		

#	Minimum Specifications	Bidder Compliance (Yes/No)	Product Documentation Reference
16.	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		
17.	The administrator logging on to the call control server needs to authenticate by suitable mechanism such as User Login Information and Passwords/ Radius Server		
18.	Voice gateway to be provided with 1 PRI card scalable to 3 PRI in future for PSTN (PRI) line termination.		

4.2.13 Video Conferencing Unit

#	Minimum Requirements	Bidder Compliance (Yes/No)	Product Documentation Reference
1.	Make	<to be provided by the bidder>	
2.	Model	<to be provided by the bidder>	
3.	Video conferencing systems should be based on ITU's standards and guidelines.		
4.	Video Standards: H.263, H.264		
5.	Should support 30 fps & 60fps (frames per second) with 1080p resolution from day one		
6.	Video Features: Ability to send and receive two live simultaneous video sources in a single call, so that the image from the main camera and PC or document camera can be seen simultaneously		
7.	Should support H.239 and BFCP protocols with 1080p resolution		
8.	Video Output: Should have at least 2 HDMI / DVI (High Definition Multimedia Interface) output to connect Full High Definition display devices such as LCD / LED and projectors for both Video and Content. (Dual Monitor Support)		
9.	It should be possible to display the main video on one HD screen and the presentation / dual video on the other HD screen.		

#	Minimum Requirements	Bidder Compliance (Yes/No)	Product Documentation Reference
10.	Video Input: Should have at least one HD video Input to connect HD camera with full functionalities as mentioned in the camera specifications.		
11.	Should have DVI (Digital Video Interface) input to connect PC / Laptop directly to the Video conferencing system and display resolutions WXGA / HD720p along with PC Audio.		
12.	Audio standards: G.711, G.722, G.722.1, 64 kbps MPEG-4 AAC-LD or equivalent standards must be supported.		
13.	Audio Inputs: Should support minimum 2 Microphone inputs. 1 needs to be supplied from day one.		
14.	1 LAN / Ethernet - 10/100/1000 Mbps		
15.	IP - at least 6 Mbps bandwidth support		
16.	Security: Password protected system menu		
17.	Camera: Minimum of 12X Optical zoom. Camera shall be mountable on flat panel display or on a shelf in the cart		
18.	1920 x 1080 pixels progressive @ 30fps		
19.	The camera module and microphones should have omni-directional coverage of 360 degrees.		
20.	Controls of the video conference system shall be accessed via the room control system to maintain a single source for control.		
21.	System shall have the capability to zoom in and follow the person speaking.		
22.	Participants shall be able to have the following feature controls using Remote Control or GUI of video system through the multipoint control unit: ▪ Mute My Line / Unmute My Line ▪ Increase Broadcast Volume / Decrease Broadcast Volume ▪ Mute All Except Me / Cancel Mute All Except Me ▪ Change Password ▪ Mute Incoming Participants / Unmute Incoming Participants ▪ Play Help Menu ▪ Enable Roll Call / Disable Roll Call		

#	Minimum Requirements	Bidder Compliance (Yes/No)	Product Documentation Reference
	▪ Roll Call Review Names / Roll Call Stop Review Names ▪ Terminate Conference ▪ Start Personal Layout ▪ Change To Chairperson ▪ Increase Listening Volume / Decrease Listening Volume ▪ Override Mute All ▪ Start Recording / Stop Recording / Pause Recording ▪ Secure Conference / Unsecured Conference; and ▪ Show Number of Participants		
23.	The Camera and codec should be from the same manufacturer		

4.2.14 Multiparty Conference Unit (Video and Audio Conferencing Bridge with Secure VC over Internet)

#	Minimum Requirements	Bidder Compliance (Yes/No)	Product Documentation Reference
1.	Make	<to be provided by the bidder>	
2.	Model	<to be provided by the bidder>	
3.	The Bridging should be running on the standard Intel servers on standard Virtualized platforms. The hardware, software and virtualization software should be supplied and supported by a single bidder.		
4.	From day one the bridge must provide 6 full HD video ports @1080p 30 fps and 30 audio conference ports.		
5.	All necessary hardware to support the above capacity needs to be supplied from day one. Bridge must have a redundant power supply.		
6.	All the ports must be able to connect different sites at different bandwidths and protocols.		
7.	H.264 AVC standard must be supported at the minimum to connect all the sites.		
8.	The bridge should support room based video end points, users joining from browsers' supporting WebRTC and		

#	Minimum Requirements	Bidder Compliance (Yes/No)	Product Documentation Reference
	HTML5 and its own clients. In case additional components are required for this functionality, all additional components required to have this functionality has to be included in the solution.		
9.	The bridge should have the capability to host meetings with internal and external participants in a secure way such that it should co-exist with the enterprise security policies.		
10.	The bridge should have components such as the Web Server for Web RTC, Scheduler as part of the offering from day one.		
11.	Should support H.261, H.263, H.263+, H.263++, H.264, WebRTC video algorithms.		
12.	Should support video resolution from SD to Full HD to join into a conference.		
13.	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 and MPEG 4 AAC – LD.		
14.	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.		
15.	The bridge should support transcoding of different Audio/video Protocols.		
16.	The bridge should have H.239/BFCP protocol for sending and receiving dual video streams (Presenter + Presentation).		
17.	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.		
18.	The bridge must be a secure Non-PC Hardware with a strong operating system. The Hardware and software must be from the same OEM.		

#	Minimum Requirements	Bidder Compliance (Yes/No)	Product Documentation Reference
19.	The bridge should support 128 Bit strong AES encryption for calls and H.235 for authentication.		
20.	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.		
21.	They should be able to join the bridge using standards based VC endpoints using internet (as long as these endpoints are exposed to internet) securely.		
22.	It should be possible to connect 5 such external endpoints / locations concurrently at any given point of time.		
23.	It should use secure firewall traversal technology.		
24.	It should support any standards-compliant SIP or H.323 video conferencing endpoints.		
25.	It should support for H.323 SIP Interworking Encryption and H.323 SIP Interworking DuoVideo.		
26.	It should use standards based firewall traversal methods - H.460.18/19.		

4.2.15 Fixed Dome Camera for Indoor Surveillance

#	Parameter	Minimum Specifications or better	Bidder Compliance (Yes/No)	Product Documentation Reference
1.	Make		<to be provided by the bidder>	
2.	Model		<to be provided by the bidder>	
3.	Video Compression	H.264		
4.	Video Resolution	1920 X 1080		
5.	Frame rate	Min. 25 fps		
6.	Image Sensor	1/3" Progressive Scan CCD / CMOS		
7.	Lens Type	Varifocal, IR Correction Full HD lens compatible to camera imager		
8.	Lens#	Auto IRIS 2.8-10mm		

#	Parameter	Minimum Specifications or better	Bidder Compliance (Yes/No)	Product Documentation Reference
9.	Multiple Streams	Dual streaming with 2nd stream at minimum 720P at 30fps at H.264 individually configurable		
10.	Minimum Illumination	Colour: 0.1 lux, B/W: 0.01 lux (at 30 IRE)		
11.	IR Cut Filter	Automatically Removable IR-cut filter		
12.	Day/Night Mode	Colour, Mono, Auto		
13.	S/N Ratio	≥ 50 dB		
14.	Auto adjustment + Remote Control of Image settings	Colour, brightness, sharpness, contrast, white balance, exposure control, backlight compensation, Gain Control, Auto back focus		
15.	Wide Dynamic Range	True WDR upto 80 db		
16.	Audio	Full duplex, line in and line out, G.711, G.726		
17.	Local storage	microSDXC up to 32GB (Class 10) In the event of failure of connectivity to the central server the camera shall record video locally on the SD card automatically. After the connectivity is		
		restored these recordings shall be automatically merged with the server recording such that no manual intervention is required to transfer the SD card based recordings to server.		
18.	Protocol	HTTP, HTTPS, FTP, RTSP, RTP, TCP, UDP, RTCP, DHCP, ONVIF Profile S &G		
19.	Security	Password Protection, IP Address filtering, User Access Log, HTTPS encryption		
20.	Intelligent Video	Motion Detection & Tampering alert		

#	Parameter	Minimum Specifications or better	Bidder Compliance (Yes/No)	Product Documentation Reference
21.	Alarm I/O	Minimum 1 Input & Output contact for 3rd part interface		
22.	Operating conditions	0 to 50°C		
23.	Casing	NEMA 4X / IP-66 rated & IK 09		
24.	Certification	UL2802 / EN, CE ,FCC		
25.	Power	802.3af PoE (Class 0) and 12VDC/24AC		

4.3 Data Centre

4.3.1 Core/Internet Router

#	Item	Minimum Specifications	Bidder Compliance (Yes/No)	Product Documentation Reference
1.	Make		<to be provided by the bidder>	
2.	Model		<to be provided by the bidder>	
3.	General	Router shall be chassis		
4.		based with modular architecture for scalability with Redundant - Route Processor, Power supply, Switching fabric; and shall deliver multiple IP services over a flexible combination of interfaces.		
5.		Should have support for Data, Voice & Video services.		
6.		Router shall be configurable up to 64k MAC addresses		
7.		Core router shall have a total switching capacity of at least 2000 Gbps with minimum 200 Gbps per slot. The MSI shall size the port and		

#	Item	Minimum Specifications	Bidder Compliance (Yes/No)	Product Documentation Reference
		transceiver as per their detailed design.		
8.		The routers shall have a Mean Time Between Failure (MTBF) of at least 175,000 hours.		
9.		Router shall have event and system history logging capabilities. Router shall generate system alarms on events and capable of log analysis		
10.		Router should have power supply redundancy. There should not be any impact on the router performance in case one of the power supplies fails.		
11.	Ports	As per overall network architecture proposed by the bidder, the router should be populated with required number of LAN/WAN ports/ modules, with cable for connectivity to other network elements.		
12.	Interface modules	▪ Should support required number of 40G,10G and 1G interfaces based on design requirement ▪ Must have capability to interface with variety interfaces		
13.	Protocol Support	▪ support for TCP/IP, PPP, Frame relay and HDLC ▪ IPSEC VPN ▪ MPLS (Multi-Protocol Label Switching) ▪ SNMP		

#	Item	Minimum Specifications	Bidder Compliance (Yes/No)	Product Documentation Reference
14.		▪ Routing protocols of RIP, OSPF, and BGP. ▪ Support IPV4 and IPV6 ▪ IP Multicast		
15.	Manageability	Must be SNMP v2 or latest manageable		
16.	Scalable	The router should be scalable. For each slot multiple modules should be available. The chassis offered must have free slots to meet the scalability requirement of expansion of the project in the future.		
17.	Traffic control	Traffic Control and Filtering features for flexible user control policies		
18.	Bandwidth	Bandwidth on demand for cost effective connection performance enhancement		
19.		The device should have min 4GB of DRAM and support future scalability needs		
20.	Remote Access	Remote access features		
21.	Redundancy	▪ Redundancy in terms of Power supply(s). Power supply should be able to support fully loaded chassis ▪ All interface modules, power supplies should be hot- swappable		
22.	Security features	▪ MD5 encryption for routing protocol ▪ NAT ▪ URL based Filtering ▪ RADIUS Authentication		

#	Item	Minimum Specifications	Bidder Compliance (Yes/No)	Product Documentation Reference
		▪ Management Access policy ▪ IPSec / Encryption ▪ L2TP		
23.	QOS Features	▪ RSVP ▪ Priority Queuing ▪ Policy based routing ▪ Traffic shaping ▪ Time-based QoS Policy ▪ Bandwidth Reservation / Committed Information Rate		

4.3.2 Firewall

#	Item	Minimum Specifications	Bidder Compliance (Yes/No)	Product Documentation Reference
1.	Make		<to be provided by the bidder>	
2.	Model		<to be provided by the bidder>	
3.	Physical attributes	▪ Should be mountable on 19" Rack ▪ Modular Chassis ▪ Internal redundant power supply		
4.	Interfaces	▪ Minimum 2 * 10 Gig Port with necessary modules ▪ Should support 4 x 10GE and 4 x 40GE interfaces populated with transceivers as required ▪ Console Port 1 number		
5.	Performance and	▪ Encrypted throughput: of minimum 2Gbps		
6.	Availability	▪ Concurrent connections: at least 300,000 ▪ Simultaneous VPN tunnels: minimum 2000		
7.		Aggregate throughput of 10Gbps covering firewall, application visibility, intrusion prevention etc.		
8.	Routing Protocols	▪ Static Routes ▪ RIPv1, RIPv2 ▪ OSPF		

#	Item	Minimum Specifications	Bidder Compliance (Yes/No)	Product Documentation Reference
9.	Protocols	▪ TCP/IP, PPTP ▪ RTP, L2TP ▪ IPSec, DES/3DES/AES ▪ PPPoE, EAP-TLS, RTP ▪ FTP, HTTP, HTTPS ▪ SNMP, SMTP ▪ DHCP, DNS support for Ipv6		
10.	Other support	▪ 802.1Q, NAT, ▪ PAT, IP Multicast support, Remote Access VPN, Time based Access control lists, URL Filtering, support VLAN, Radius/ TACACS, IPSec, SSLVPN		
11.	QoS	QoS features like traffic prioritization, differentiated services, committed access rate. Should support for QoS features for defining the QoS policies.		
12.	Management	▪ Console, Telnet, SSHv2, Browser based configuration ▪ SNMPv1, SNMPv2 or latest		

4.3.3   Intrusion Prevention System (IPS)

#	Item	Minimum Specifications	Bidder Compliance (Yes/No)	Product Documentation Reference
1.	Make		<to be provided by the bidder>	
2.	Model		<to be provided by the bidder>	
3.	Performance	▪ Should have an aggregate throughput of no less than 1Gbps ▪ Minimum total Simultaneous Sessions – 10,000		
4.	Features	▪ Device should have Dual Power Supply ▪ IPS system should be transparent to network, not default gateway to Network ▪ IPS system should have Separate		

#	Item	Minimum Specifications	Bidder Compliance (Yes/No)	Product Documentation Reference
		interface for secure management ▪ IPS system should be able to protect Multi Segment in the network, should be able to protect 4 segments.		
5.	Real Time Protection	▪ Web Protection ▪ Mail Server Protection ▪ Cross Site Scripting ▪ SNMP ▪ Vulnerability ▪ Worms and Viruses ▪ Brute Force Protection ▪ SQL Injection ▪ Backdoor and Trojans		
6.	Stateful Operation	▪ TCP Reassembly ▪ IP Defragmentation ▪ Bi-directional Inspection ▪ Forensic Data Collection ▪ Access Lists		
7.	Signature Detection	Should have provision for Real Time Updates of Signatures, IPS Should support Automatic signature synchronization from database server on web Device should have capability to define User Defined Signatures		
8.	Block attacks in real time	▪ Drop Attack Packets ▪ Reset Connections ▪ Packet Logging ▪ Action per Attack		
9.	Alerts	▪ Alerting SNMP ▪ Log File ▪ Syslog ▪ E-mail		
10.	Management	▪ SNMP V1, 2C, 3 ▪ HTTP, HTTPS ▪ SSH, Telnet, Console		

#	Item	Minimum Specifications	Bidder Compliance (Yes/No)	Product Documentation Reference
11.	Security Maintenance	▪ Should support 24/7 Security Update Service ▪ Should support Real Time signature update ▪ Should support Provision to add static own attack signatures ▪ Should show real-time and History reports of Bandwidth usage per policy ▪ Should have provision for external bypass Switch		
12.	General	▪ To get layered approach to Security, Firewall and IPS should be of different OEM. ▪ Should not induce Latency into the Network, Latency should be less than 200 microseconds.		

4.3.4 Data Centre Core Switch

#	Parameter	Minimum Specifications	Bidder Compliance (Yes/No)	Product Documentation Reference
1.	Make		<to be provided by the bidder>	
2.	Model		<to be provided by the bidder>	
3.	Ports	The switch should support 1/10G SFP+, 1/10 G Base-T and 40G QSFP based port line cards. The switch must be scalable to support minimum 8 nos of 40 G QSFP ports or more spread across different line cards. Bidder to choose required ports as per their solution		

#	Parameter	Minimum Specifications	Bidder Compliance (Yes/No)	Product Documentation Reference
4.		Switch should have minimum of 24 x 1G/10G Ports Switch should have a minimum of 24 x 1G /10G BASE-T ports Switch should have a minimum of 8 x 40G QSFP+ ports		
5.	Switch type	Layer 3 supporting 24K Multicast route. Also should support minimum 50K ipv4 Route entries and 30K of IPv6 routes.		
6.	MAC	Support minimum 16K MAC address.		
7.	Backplane	Minimum 10 Tbps or more Switching fabric capacity (as per network configuration to meet performance requirements)		
8.	Port Features	Must support Port Mirroring, Port Trunking and 802.3ad LACP Link Aggregation port trunks		
9.	Flow Control	Support IEEE 802.3x flow control for full- duplex mode ports.		
10.	Protocols	▪ Support 802.1D, 802.1S, 802.1w, Rate limiting ▪ Support 802.1Q VLAN encapsulation, IGMP v1, v2 and v3 snooping ▪ 802.1p Priority Queues, port mirroring, DiffServ ▪ Support based on 802.1p priority bits with at least 8 queues ▪ DHCP support & DHCP snooping/relay/optional 82/ server support ▪ Shaped Round Robin (SRR) or WRR scheduling support. ▪ Support for Strict priority queuing & Sflow ▪ Support for IPV6 ready features with dual stack ▪ Support up-to 255 VLANs and up-to 4K VLAN IDs		
11.	Access Control	▪ Support port security ▪ Support 802.1x (Port based network access control).		

#	Parameter	Minimum Specifications	Bidder Compliance (Yes/No)	Product Documentation Reference
		- Support for MAC filtering. - Should support TACACS+ and RADIUS authentication		
12.	VLAN	Support 802.1Q Tagged VLAN and port based VLANs and Private VLAN		
13.	Protocol and Traffic	- Network Time Protocol or equivalent Simple Network Time Protocol support - Switch should support traffic segmentation - Traffic - classification should be based on user-definable application types: TOS, DSCP, Port - based, TCP/UDP port number		
14.	Management	- Switch needs to have RS-232/USB/RJ45 console port for management via a console terminal or PC - Must have support SNMP v1,v2 and v3 - Should support 4 groups of RMON - Should have accessibility using Telnet, SSH, Console access, easier software upgrade through network using TFTP etc. - Configuration management through CLI, GUI based software utility and using web interface		
15.	Others	The switches shall have a Mean Time Between Failure (MTBF) of at least 175,000 hours.		

4.3.5 Data Centre Switches

#	Parameter	Minimum Specifications	Bidder Compliance (Yes/No)	Product Documentation Reference
1.	Make		<to be provided by the bidder>	
2.	Model		<to be provided by the bidder>	
3.	Ports	▪ 24 or 48 (as per density required) 1G/ 10G Ethernet ports (as per internal connection requirements) and at least 5 or more numbers of Uplink ports (40GE) ▪ All ports can auto-negotiate between all allowable speeds, half-duplex or full duplex and flow control for half-duplex ports.		
4.	Switch type	Layer 3		
5.	MAC	Support 16K MAC address		
6.	Backplane	Capable of providing wire-speed switching		
7.	Backplane Throughput	2560 Gbps or better		
8.	Port Features	Must support Port Mirroring, Port Trunking and 802.3ad		
9.		LACP Link Aggregation port trunks		
10.	Flow Control	Support IEEE 802.3x flow control for full- duplex mode ports.		
11.	Protocols	▪ IPV4, IPV6 ▪ Support 802.1D, 802.1S, 802.1w, Rate limiting ▪ Support 802.1X Security standards ▪ Support 802.1Q VLAN encapsulation, IGMP v1, v2 and v3 snooping ▪ 802.1p Priority ▪ Queues, port mirroring, DiffServ ▪ DHCP support ▪ Support up to 1024 VLANs		

#	Parameter	Minimum Specifications	Bidder Compliance (Yes/No)	Product Documentation Reference
		▪ Support IGMP Snooping and IGMP Querying ▪ Support Multicasting ▪ Should support Loop protection and Loop detection, ▪ Should support Ring protection (optional)		
12.	Access Control	▪ Support port security ▪ Support 802.1x (Port based ▪ Network access control). ▪ Support for MAC filtering. ▪ Should support TACACS+ and RADIUS ▪ authentication		
13.	VLAN	Support 802.1Q Tagged VLAN and port based VLANs and Private VLAN		
14.	Protocol and Traffic	▪ Network Time ▪ Protocol or equivalent Simple Network Time Protocol support ▪ Switch should support traffic segmentation ▪ Traffic classification should be based on user-definable application types: TOS, DSCP, Port based, TCP/UDP port number		
15.	Management	▪ Switch needs to have a console port for management via a console terminal or PC ▪ Must have support SNMP v1,v2 and v3 ▪ Should support 4 groups of RMON ▪ Should have accessibility using Telnet, SSH, Console access,		

#	Parameter	Minimum Specifications	Bidder Compliance (Yes/No)	Product Documentation Reference
		easier software upgrade ▪ Through network using TFTP etc. Configuration management through CLI, GUI based software utility and using web interface		
16.	Resiliency	▪ Dual load sharing AC and DC power supplies ▪ Redundant variable-speed fans		
17.	Others	▪ The switches shall have a Mean Time Between Failure (MTBF) of at least 175,000 hours.		

4.3.6 Server Hardware Load Balancer

#	Item	Minimum Specifications	Bidder Compliance (Yes/No)	Product Documentation Reference
1.	Make		<To be provided>	
2.	Model		<To be provided>	
3.	Server Load Balancing Mechanism	▪ Cyclic, Hash, Least numbers of users ▪ Weighted Cyclic, Least Amount of Traffic ▪ NT Algorithm / Private Algorithm / Customizable Algorithm / Response Time		
4.	Redundancy Features	▪ Supports Active-Active and Active-Standby Redundancy ▪ Segmentation / Virtualization support along with resource allocation per segment, dedicated access control for each segment		
5.	Routing Features	▪ Routing protocols RIPv1/RIPv2/OSPF ▪ Static Routing policy support		

#	Item	Minimum Specifications	Bidder Compliance (Yes/No)	Product Documentation Reference
6.	Server Load Balancing Features	▪ Server and Client process coexist ▪ UDP Stateless ▪ Service Failover ▪ Backup/Overflow ▪ Direct Server Return ▪ Client NAT ▪ Port Multiplexing-Virtual Ports to Real Ports Mapping ▪ DNS Load Balancing		
7.	Load Balancing Applications	▪ Application/ Web Server, MMS, RTSP, Streaming Media ▪ DNS, FTP- ACTIVE & PASSIVE, REXEC, RSH, ▪ LDAP, RADIUS		
8.	Other requirements	• Content Intelligent SLB • HTTP Header Super Farm ▪ URL-Based SLB		
9.	Browser Type Farm	▪ Support for Global Server Load Balancing o Global Server Load Balancing Algorithms o HTTP Redirection, ▪ HTTP ▪ DNS Redirection, RTSP Redirection ▪ DNS Fallback Redirection, HTTP Layer 7 Redirection		
10.	Management options	▪ Secure Web Based Management ▪ SSH ▪ TELNET ▪ SNMP v1, 2, 3 Based GUI ▪ Command Line		

4.3.7 Blade Servers

#	Parameter	Minimum Specifications	Bidder Compliance (Yes/No)	Product Documentation Reference
1.	Make		<To be Provided>	
2.	Model		<To be Provided>	

#	Parameter	Minimum Specifications	Bidder Compliance (Yes/No)	Product Documentation Reference
3.	Processor	▪ Latest series/ generation of 64 bit x86 processor(s) with Ten or higher Cores ▪ Processor speed should be ▪ minimum 2.4 GHz ▪ Minimum 2 processors per each physical server MSI Should go for fully populated blade configuration.		
4.	Storage	Should have two Solid State Drives (SSD) minimum capacity 300 GB		
5.	Memory	Server should have at-least 8 GB per core DDR4 memory @1066 MHz or higher. After populating DIMMs, Each blade server should have 100% free memory DIMM slots remaining for future expansion		
6.				
7.	Network	Should support Converged Network Adapter, which aggregates both the Ethernet and FC connectivity on a single controller. It should support scalability upto 160 Gb Ethernet connectivity per server.		
8.	Operating System	Licensed version of 64 bit latest version of Enterprise Linux/Microsoft® Windows. Should support Cloud and virtualization.		
9.	Management	Should support remote KVM capability from an external keyboard, video monitor and mouse to all blades installed in the chassis through the management controllers		

#	Parameter	Minimum Specifications	Bidder Compliance (Yes/No)	Product Documentation Reference
10.		Remote KVM should support up to 4 active sessions		
11.	Others	Should be hot pluggable		

4.3.8 Blade Chassis

#	Parameter	Minimum Specification	Bidder Compliance (Yes/No)	Product Documentation Reference
1.	Make		<To be provided>	
2.	Model		<To be provided>	
3.	Blade Chassis	Blade chassis shall be 19" Electronic Industries Alliance Standard Width rack mountable and provide appropriate rack mount kit.		
4.	Power	The enclosure should be populated fully with power supplies of the highest capacity & energy efficiency of a minimum of 90%		
5.		The power subsystem should support N + N power redundancy (where N is at least equal to 2) for a fully populated chassis with all servers configured with the highest CPU configuration, maximum memory and IO configuration possible		
6.	Cooling	Each blade enclosure should have a cooling subsystem consisting of redundant hot pluggable fans or blowers enabled with technologies for improved power consumption and acoustics		
7.	Chassis connectivity	The chassis should support redundant modules for connectivity - Ethernet and Fiber Channel /Infiniband modules OR converged fabric modules in lieu thereof		

#	Parameter	Minimum Specification	Bidder Compliance (Yes/No)	Product Documentation Reference
8.	Ethernet Module	Chassis should have sufficient number of redundant 10gb based ethernet modules to provide a minimum of 10 Gbps per blade server and 5 Gbps sustained per blade server (with 1 module failure)for a fully populated chassis for LAN Traffic.		
9.	FC Module	Chassis should have sufficient number of redundant 8gb based ethernet modules to provide a minimum of 8 Gbps per blade server and 4 Gbps sustained per blade server (with 1 module failure)for a fully populated chassis for FC Traffic.		
10.	Converged Module	In lieu of above mentioned Ethernet and FC module, Chassis can also be provision to have sufficient number of redundant 10gb based converged modules to provide a minimum of 20 Gbps per blade server and 10Gbps sustained per blade server (with 1 module failure)for a fully populated chassis for LAN & SAN Traffic. It should also provide minimum 40Gbps FCOE downlink bandwidth from each module /switch to each x86 server		
11.	Management	Must be able to show the actual power usage and actual thermal measurement data of the servers across chassis		
12.		Administrators should have the ability to set a cap on the maximum power that the chassis / physical server can draw in order to limit power consumption for non-critical applications		

#	Parameter	Minimum Specification	Bidder Compliance (Yes/No)	Product Documentation Reference
13.		Redundancy should be built in the management subsystem so that if one management module fails other should be able to take over automatically. Integrated Management solution should be provided		

4.3.9   Storage

#	Minimum Storage Requirement	Specification
1.	Primary Storage	300 TB
2.	Secondary Storage	400 TB
3.	Backup Storage	As per requirement

Note:
- Bidder is expected to carry out the storage requirement estimation and supply as per the solution proposed, if the estimation is more than above specified.

4.3.9.1   *Primary Storage*

#	Parameter	Minimum Specifications	Bidder Compliance (Yes/No)	Product Documentation Reference
1.	Make	<to be provided by the bidder>		
2.	Model	<to be provided by the bidder>		
3.	Solution/ Type	IP Based/iSCSI/FC/NFS/ CIFS		
4.	Storage	▪ Storage Capacity should be as per Overall Solution Requirement (usable, after configuring in offered RAID configuration) ▪ RAID solution offered must protect against double disc failure. ▪ Disks should be preferably minimum of 1.2 TB capacity for SAS and 3 TB for SATA (combination as per performance and SLA requirements of overall solution) ▪ To store all types of data (Data, Voice, Images, Video, etc.)		

#	Parameter	Minimum Specifications	Bidder Compliance (Yes/No)	Product Documentation Reference
		▪ Proposed Storage System should be scalable (vertically/horizontally)		
5.	Hardware Platform	Rack mounted form- factor Modular design to support controllers and disk drives expansion		
6.	Controllers	▪ At least 2 Controllers in active/active mode ▪ The controllers / Storage nodes should be upgradable seamlessly, without any disruptions / downtime to production workflow for performance, capacity enhancement and software / firmware upgrades.		
7.	RAID support	Should support various RAID Levels		
8.	Cache	Minimum 64 GB of useable cache across all controllers. If cache is provided in additional hardware for the storage solution, then cache must be over and above 64 GB.		
9.	Redundancy and High Availability	The Storage System should be able to protect the data against single point of failure with respect to hard disks, connectivity interfaces, fans and power supplies		
10.	Management software	▪ All the necessary software (GUI Based) to configure and manage the storage space, RAID configuration, logical drives allocation, snapshots etc. are to be provided for the entire system proposed. ▪ Licenses for the storage management software should ▪ Include disc capacity/count of the complete solution and any additional disks to be plugged in in the future,		

#	Parameter	Minimum Specifications	Bidder Compliance (Yes/No)	Product Documentation Reference
		upto max capacity of the existing controller/units. ▪ A single command console for entire storage system. ▪ Should also include storage performance monitoring and management software ▪ Should provide the functionality of proactive monitoring of Disk drive and Storage system for all possible disk failures ▪ Should be able to take "snapshots" of the stored data to another logical drive for backup purposes		
11.	Data Protection	The storage array must have complete cache protection mechanism either by de-staging data to disk or providing complete cache data protection with battery backup for up to 4 hours		

4.3.9.2   *Secondary Storage*

#	Parameter	Minimum Specifications	Bidder Compliance (Yes/No)	Product Documentation Reference
1.	Make	<to be provided by the bidder>		
2.	Model	<to be provided by the bidder>		
3.	Solution/ Type	▪ Secondary Storage (Archival/Backup) can be on any media such as Disks, Disk systems etc. or its combination along with all associate software. (so as to arrive at lower cost per TB) ▪ Minimum 400 TB usable as secondary storage ▪ Should use de-duplication technology ▪ Compatible with primary storage		

#	Parameter	Minimum Specifications	Bidder Compliance (Yes/No)	Product Documentation Reference
		▪ Must use latest stable technology platform, with support available for next 5 years.		
4.	Backup Size	To store data as required, to meet the archival requirement for different type of data/information: 45 days of storage for surveillance camera feeds, 90 days of storage for traffic enforcement systems, 365 days of storage for ATCS systems		
5.	Hardware Platform	Rack mounted, Rack based Expansion shelves		
6.	Software Platform	Must include backup/archive application portfolio required		
7.	Retrieval time	Retrieval time for any data stored on secondary storage should be max. 4 hours for critical data & 8 hours for other data. This would be taken into account for SLA calculation. (Critical data means any data needing urgent attention by the RSCCL).		

4.3.9.3   Tape Library

#	Minimum technical specification	Bidder Compliance (Y/N)	Product Documentation Reference
1.	Make	<to be specified by the bidder>	
2.	Model	<to be specified by the bidder>	
3.	Shall support Native data capacity of 200TB (uncompressed) expandable to 400TB (compressed).		
4.	Shall be offered with Minimum of four LTO6 FC tape drive. Drive shall support encryption.		
5.	Shall be offered with minimum of 48 Cartridge slots and scalable to minimum 100 Cartridge		

#	Minimum technical specification	Bidder Compliance (Y/N)	Product Documentation Reference
6.	Tape Library shall provide 8 Gbps native FC connectivity to SAN switches.		
7.	Library shall be able to back up the encrypted keys in a redundant fashion		
8.	Tape Library shall provide web based remote management.		
9.	The library should have cartridge I/O slots for secure & easy off-site backup storage		
10.	1. Tape Library shall have GUI Panel 2. Shall be rack mountable. 3. Shall have option for redundant power supply		
11.	Should support industry leading backup software		
12.	40 LTO6 barcode labeled cartridges & 4 cleaning cartridges from the tape library OEM to be provided		

4.3.10 KVM Switch

#	Item	Minimum Specifications	Bidder Compliance (Yes/No)	Product Documentation Reference
1.	Make	<to be provided by the bidder>		
2.	Model	<to be provided by the bidder>		
3.	KVM Requirement	Keyboard, Video Display Unit and Mouse Unit (KVM) for the IT Infrastructure Management at Data Centre		
4.	Form Factor	19" rack mountable		
5.	Ports	minimum 8 ports		
6.	Server Connections	USB or KVM over IP.		
7.	Auto-Scan	It should be capable to auto scan servers		
8.	Rack Access	It should support local user port for rack access		
9.	SNMP	The KVM switch should be SNMP enabled. It should be operable from remote locations		
10.	OS Support	It should support multiple operating system		
11.	Power Supply	It should have dual power with failover and built-in surge protection		
12.	Multi-User support	It should support multi- user access and collaboration		

4.3.11 Server/Network Rack Specifications

#	Parameter	Minimum Specifications	Bidder Compliance (Yes/No)	Product Documentation Reference
1.	Make		<to be provided by the bidder>	
2.	Model		<to be provided by the bidder>	
3.	Type	19" 42U racks		
		mounted on the floor Floor Standing Server Rack - 42U with Heavy Duty Extruded Aluminum Frame for rigidity. Top cover with FHU provision. Top & Bottom cover with cable entry gland plates. Heavy Duty Top and Bottom frame of MS. Two pairs of 19" mounting angles with 'U' marking. Depth support channels - 3 pairs with an overall weight carrying Capacity of 500Kgs. All racks should have mounting hardware 2 Packs, Blanking Panel. Stationery Shelf (2 sets per Rack) All racks must be lockable on all sides with unique key for each rack Racks should have Rear Cable Management channels, Roof and base cable access		
4.	Wire managers	Two vertical and four horizontal		
5.	Power Distribution Units	2 per rack Power Distribution Unit - Vertically Mounted, 32AMPs with 25 Power Outputs. (20 Power outs of IEC 320 C13 Sockets & 5 Power outs of 5/15 Amp Sockets), Electronically controlled circuits for Surge & Spike protection, LED readout for the total current being drawn from the channel, 32AMPS MCB, 5 KV AC isolated input to Ground & Output to Ground		

#	Parameter	Minimum Specifications	Bidder Compliance (Yes/No)	Product Documentation Reference
6.	Doors	The racks must have steel (solid / grill / mesh) front / rear doors and side panels. Racks should NOT have glass doors / panels. Front and Back doors should be perforated with at least 63% or higher perforations. Both the front and rear doors should be designed with quick release hinges allowing for quick and easy detachment without the use of tools.		
7.	Fans and Fan Tray	Fan 90CFM 230V AC, 4" dia (4 Nos. per Rack) Fan Housing Unit 4 Fan Position (Top Mounted) (1 no. per Rack) - Monitored - Thermostat based - The Fans should switch on based on the Temperature within the rack. The temperature setting should be factory settable. This unit should also include - humidity & temperature sensor		
8.	Metal	Aluminum extruded profile		
9.	Side Panel	Detachable side panels (set of 2 per Rack)		

4.3.12 WAN Router

#	Item	Minimum Specifications	Bidder Compliance (Yes/No)	Product Documentation Reference
1.	Make		<to be provided by the bidder>	
2.	Model		<to be provided by the bidder>	
3.	Multi-Services	Should deliver multiple IP services over a flexible combination of interfaces		
4.		Minimum throughput capacity of 400 Gbps		
5.	Ports	As per overall network architecture proposed by the bidder, the router should be populated with required number of LAN/WAN		

#	Item	Minimum Specifications	Bidder Compliance (Yes/No)	Product Documentation Reference
		ports/modules, with cable for connectivity to other network elements.		
6.	Interface modules	▪ Must support up to 40G interfaces as per the design. Must have capability to connect with variety of interfaces.		
7.	Protocol Support	▪ Must have support for TCP/IP, PPP,, Frame relay and HDLC ▪ Must support VPN ▪ Must have support for integration of data and voice services		
8.		▪ Routing protocols of RIP, OSPF, and BGP. ▪ Support IPV4, IPV6 ▪ Support load balancing		
9.	Manageability	Must be SNMP manageable		
10.	Traffic control	Traffic Control and Filtering features for flexible user control policies		
11.	Bandwidth	Bandwidth on demand for cost effective connection performance enhancement		
12.	Remote Access	Remote access features		
13.	Redundancy	▪ Redundancy in terms of Power supply(s). Power supply should be able to support fully loaded chassis ▪ All interface modules, power supplies should be hot-swappable		
14.	Security features	▪ MD5 encryption for routing protocol ▪ NAT ,URL based Filtering ▪ RADIUS/AAA Authentication ▪ Management Access policy ▪ IPSec / Encryption		

#	Item	Minimum Specifications	Bidder Compliance (Yes/No)	Product Documentation Reference
		• L2TP		
15.	QOS Features	• RSVP • Priority Queuing • Policy based routing • Traffic shaping • Time-based QoS Policy • Bandwidth Reservation • / Committed Information Rate		

4.3.13 Layer 3 Gigabit Manageable Switch

#	Parameter	Minimum Specifications	Bidder Compliance (Yes/No)	Product Documentation Reference
1.	Make		<to be provided by the bidder>	
2.	Model		<to be provided by the bidder>	
3.	Ports	• 24 or 48 (as per requirements) 10/100/1000 Base-TX Ethernet ports and extra 2 nos of Base-SX/LX ports • All ports can auto- negotiate between 10Mbps/ 100Mbps/ 1000Mbps, half-duplex or full duplex and flow control for half-duplex ports. • Uplink ports supporting 1Gbps/10Gbps		
4.	Switch type	Layer 3		
5.	MAC	Support 16K MAC address.		
6.	Backplane	Switching fabric capacity should support non-blocking architecture back plane for numbers (as per network configuration to meet performance requirements)		
7.	Forwarding rate	Packet Forwarding Rate should be 70.0 Mpps or better		
8.	Port Features	Must support Port Mirroring, Port Trunking and 802.3ad LACP Link Aggregation port trunks		
9.	Flow Control	Support IEEE 802.3x flow control for full-duplex mode ports.		

#	Parameter	Minimum Specifications	Bidder Compliance (Yes/No)	Product Documentation Reference
10.	Protocols	▪ Support 802.1D, 802.1S, 802.1w, Rate limiting ▪ Support 802.1Q VLAN encapsulation, IGMP v1, v2 and v3 snooping ▪ 802.1p Priority Queues, port mirroring, DiffServ ▪ Support based on 802.1p priority bits with at least 8 queues ▪ DHCP support & DHCP snooping/relay/optional 82/ server support ▪ Shaped Round Robin (SRR) or WRR scheduling support. ▪ Support for Strict priority queuing & Sflow ▪ Support for IPV6 ready features with dual stack, Support upto 255 VLANs and upto 4K VLAN IDs		
11.	Access Control	▪ Support port security ▪ Support 802.1x (Port based network access control). ▪ Support for MAC filtering. ▪ Should support TACACS+ and RADIUS authentication		
12.	VLAN	▪ Support 802.1Q Tagged VLAN and port based VLANs and Private VLAN ▪ Dynamic Trunking protocol or equivalent		
13.	Protocol and Traffic	▪ Network Time Protocol or equivalent Simple Network Time Protocol support ▪ Switch should support traffic segmentation ▪ Traffic classification should be based on user- definable application types: TOS, DSCP, Port based, TCP/UDP port number		
14.	Management	▪ Switch needs to have console port for management via PC ▪ Must have support SNMP v1,v2 and v3		

#	Parameter	Minimum Specifications	Bidder Compliance (Yes/No)	Product Documentation Reference
		▪ Should support 4 groups of RMON ▪ Should have accessibility using Telnet, SSH, Console access, easier software upgrade through network using TFTP etc. Configuration management through CLI, GUI based software utility and using web interface		

4.3.14 Online UPS

#	Parameter	Minimum Specifications	Bidder Compliance (Yes/No)	Product Documentation Reference
1.	Make		<to be provided by the bidder>	
2.	Model		<to be provided by the bidder>	
3.	Capacity	Adequate capacity to cover all above IT Components at Dc for at-least 60 min		
4.	Output Wave Form	Pure Sine wave		
5.	Input Power Factor at Full Load	>0.90		
6.	Input	Three Phase 3 Wire for over 5 KVA		
7.	Input Voltage Range	305-475VAC at Full Load		
8.	Input Frequency	50Hz +/- 3 Hz		
9.	Output Voltage	400V AC, Three Phase for over 5 KVA UPS		
10.	Output Frequency	50Hz+/- 0.5% (Free running); +/- 3% (Sync. Mode)		

#	Parameter	Minimum Specifications	Bidder Compliance (Yes/No)	Product Documentation Reference
11.	Inverter efficiency	>90%		
12.	Over All AC-AC Efficiency	>85%		
13.	UPS shutdown	UPS should shutdown with an alarm and indication on following conditions 1)Output over voltage 2)Output under voltage 3)Battery low 4)Inverter overload 5)Over temperature 6)Output short		
14.	Battery Backup	60 minutes in full load at DC & Control room		
15.	Battery	VRLA (Valve Regulated Lead Acid) SMF (Sealed Maintenance Free) Battery		
16.	Indicators & Metering	Indicators for AC Mains, Load on Battery, Fault, Load Level, Battery Low Warning, Inverter On, UPS on Bypass, Overload, etc. Metering for Input Voltage, Output Voltage and frequency, battery voltage, output current etc.		
17.	Audio Alarm	Battery low, Mains Failure, Over temperature, Inverter overload, Fault etc.		
18.	Cabinet	Rack / Tower type		
19.	Operating Temp	0 to 50 degrees centigrade		
20.	Management Protocol	SNMP Support through TCP/IP		

4.3.15 Fire Proof Enclosure

The overall design of the safe should be suitable for safe storage of computer diskettes, tapes, smart cards and similar devices and other magnetic media, paper documents, etc. the safe should have adequate fire protection.

#	Item	Minimum Specifications	Bidder Compliance (Yes/No)	Product Documentation Reference
1.	Make		<to be provided by the bidder>	
2.	Model		<to be provided by the bidder>	
3.	Capacity	300 Litres		
4.	Temperature to Withstand	1000° C for at least 1 hour		
5.	Internal Temperature	30° C after exposure to high temperature For 1 hour		
6.	Locking	2 IO-lever high security cylindrical / Electronic lock		

4.3.16 Structured Cabling

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

4.3.17 Electrical cabling

#	Parameter	Minimum Specifications	Bidder Compliance (Yes/No)
1.	Standards	All electrical components shall be design manufactured and tested in accordance with relevant Indian Standard IECSs	

4.3.18 DG Set

#	Parameter	Minimum Specifications	Bidder Compliance (Yes/No)
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 ▪ Earth Terminal	

#	Parameter	Minimum Specifications	Bidder Compliance (Yes/No)
		▪ 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	

4.3.19 Enterprise Management System

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

1. SLA & Contract management System
2. Network Monitoring System
3. Server Monitoring System
4. Helpdesk System

The Monitoring system should be able to provide automated consolidated SLA reports for all the SLAs as mentioned in this RFP including real time status of various service levels achieved. The report to be available through a centralised web access / dash board the access for this to be given to at least 5 users of RSCCL.

MSI will implement dedicated EMS solution to meet the SLA monitoring and other requirements as mentioned in the RFP. The implemented EMS solution to help RSCCL in data driven decision making. The entire EMS implementation shall be certified by MSI

also for its correctness, adequacy to meet RFP requirements and measurement of SLAs & KPIs etc.

4.3.19.1 1. *SLA & Contract management System*

The SLA & Contract Management solution should enable RSSCL to capture all the System based SLAs defined in this Tender and then calculate quarterly (or for any duration) penalty automatically. Measuring service performance requires incorporation of a wide variety of data sources of the project. The SLA solution should support the collection data from various sources in order to calculate Uptime / Performance / Security SLAs. Various features required in this component to EMS are –

#	Description	Bidder Compliance (Yes/No)	Product Documentation Reference
1.	Make		<to be provided by the bidder>
2.	Model		<to be provided by the bidder>
3.	It must be a centralized monitoring solution for all IT assets (including servers, network equipment etc.)		
4.	The solution must have integrated dashboard providing view of non performing components / issues with related to service on any active components.		
5.	The solution must follow governance, compliance and content validations to improve standardization of service level contracts.		
6.	The solution should be pre-configured so as to allow the users to generate timely reports on the SLAs on various parameters.		
7.	The solution must support Service Level Agreements & Lifecycle Management including Version Control, Status Control, Effectively and audit Trail to ensure accountability for the project.		
8.	The solution must have the ability to define and calculate key performance indicators from an End to End Business Service delivery perspective related to Project.		

#	Description	Bidder Compliance (Yes/No)	Product Documentation Reference
9.	The solution should support requirements of the auditors requiring technical audit of the whole system.		
10.	The solution most have an integrated dashboard, view of Contract Parties & current SLA delivery levels and view of Services & current SLA performance.		
11.	The solution should support SLA alerts escalation process.		
12.	The solution should accept Data from a variety of formats; provide pre-configured connectors and adapters.		
13.	Support for defining and calculating service credit and penalty based on clauses in SLAs.		
14.	Reports (Indicative but not limited to) ▪ Ability to generate reports on penalty and credit due, to check on non-compliance of SLAs for the surveillance project ▪ Monetary penalties to be levied for non-compliance of SLA, thus the system must provide Service Level Performance Report over time, contract, service and more. ▪ Historical and concurrent service level reports for the surveillance project in order to ensure accountability of the service provider's performance ▪ Automatic Report creation, execution and Scheduling, must support variety of export formats including Spreadsheet, Word/Docs, Adobe PDF etc. ▪ Templates for report generation, Report Filtering and Consolidation and Context sensitive Drill-down on specific report data to drive standardisation and governance of the surveillance project		

#	Description	Bidder Compliance (Yes/No)	Product Documentation Reference
	▪ Drill-down capabilities in dashboard reports ensuring visibility for only relevant personnel of the surveillance project ▪ Real-time reports (like at-a-glance status) as well as historical analysis reports (like Trend, TopN, Capacity planning reports etc.) — Resource utilisation exceeding or below customer-defined limits — Resource utilisation exceeding or below predefined threshold limits		

4.3.19.2 Network Management System

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

#	Minimum Specification	Bidder Compliance (Yes/No)	Product Documentation Reference
1	Make		<to be provided by the bidder>
2	Model		<to be provided by the bidder>
3	The proposed solution must automatically discover manageable elements connected to the infrastructure and map the connectivity between them. Solutions should provide centralized monitoring console displaying network topology map.		
4	The system should provide discovery of heterogeneous physical network devices like Layer-2 & Layer-3 switches,		

#	Minimum Specification	Bidder Compliance (Yes/No)	Product Documentation Reference
	Routers and other IP devices and do mapping of LAN & WAN connectivity.		
5	The Solution should provide capability to monitor any device based on various versions of SNMP/IP.		
6	The Solution should monitor bandwidth utilization.		
7	The Solution must be capable of monitoring the availability, health, and performance of core networking devices including but not limited to CPU, memory, temperature.		
8	The Solution should have the ability to issues pings to check on availability of ports, devices.		
9	The Ping Monitoring should also support collection of packet loss, packet QOS, packet errors Latency and Jitters during ping checks.		
10	The Solution should automatically collect and store historical data so users can view and understand network performance trends.		
11	The solution should be capable of monitoring network delay and delay variation		
12	The solution should provide the ability to visually represent LAN/WAN links with displays of related real-time performance data including utilizations.		
13	Proposed solution should provide customizable reporting interface to create custom reports for collected data		
14	The system must use advanced root-cause analysis techniques and policy-based condition correlation technology (at network level) for comprehensive analysis of infrastructure faults.		
15	The system should be able to clearly identify configuration		

#	Minimum Specification	Bidder Compliance (Yes/No)	Product Documentation Reference
	changes and administrators should receive an alert in such cases.		
16	The solution should support multicast protocols too, if the overall project solution offered includes multicast.		
17	The system shall support monitoring of Syslog or equivalent.		
18	The solution should provide capability to add an IP device or IP Range or IP subnet with functionality supporting multiple SNMP strings.		
19	Proposed solution shall integrate with SLA & Contract Management system in order to supply KPI metrics like availability, utilisation, and performance in order to measure central SLA's and calculate penalties.		

4.3.19.3 Server Performance Monitoring

#	Description	Bidder Compliance (Yes/No)	Product Documentation Reference
1.	Make		<to be provided by the bidder>
2.	Model		<to be provided by the bidder>
3.	The proposed tool should integrate with network performance management system and support operating system monitoring for various platforms supplied as part of this Project.		
4.	Proposed solution shall integrate with SLA & Contract Management system in order to supply KPI metrics like availability, utilisation, and performance in order to measure central SLA's and calculate penalties.		

#	Description	Bidder Compliance (Yes/No)	Product Documentation Reference
5.	The proposed tool must provide information about availability and performance for target server nodes.		
6.	The proposed tool should be able to monitor various operating system parameters such as processors, memory, files, processes, file systems, etc. where applicable.		
7.	If the offered server/computing solution includes virtualization, then the server performance monitoring solution must include virtualization monitoring capabilities.		

4.3.19.4 Centralised Helpdesk

#	Description	Bidder Compliance (Yes/No)	Product Documentation Reference
1.	Make	<to be provided by the bidder>	
2.	Model	<to be provided by the bidder>	
3.	Helpdesk system should provide incident management, problem management templates along with helpdesk SLA system for tracking SLA's pertaining to incident resolution time for priority / non-priority incidents.		
4.	System should also automatically create tickets based on alarm type.		
5.	The proposed helpdesk solution must provide flexibility of logging, viewing, updating and closing incident via web interface for issues related to the project.		
6.	The proposed helpdesk solution must have a built-in workflow engine to define escalations or tasks to be carried out after issues or change order are logged pertaining to surveillance project.		
7.	Centralized Helpdesk System should have integration with Network and Server Monitoring Systems so that the Helpdesk Operators can to associate alarms with Service Desk tickets to help operators that for		

#	Description	Bidder Compliance (Yes/No)	Product Documentation Reference
	what particular alarms corresponding helpdesk tickets got logged.		
8.	IT Asset database should be built and managed by the bidder, in order to carry out the scope of work items.		
9.	Surveillance Network admin should be able to manually create tickets through Fault Management GUI.		
10.	System should provide a link to directly launch a Service Desk view of a particular ticket created by alarm.		

4.3.20 Centralised Antivirus & Anti-Spam Solution

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

#	Minimum technical specification	Bidder Compliance (Y/N)	Product Documentation Reference
1.	Make	<to be provided by the bidder>	
2.	Model/Version	<to be provided by the bidder>	
3.	Single Agent: Should be only single agent that combines all the critical components for total security on the endpoint. (Antivirus, Antimalware, Firewall, VPN Client, Virtual Browser etc.)		
4.	Personal Firewall: Firewall should block unwanted traffic, prevents malware from infecting endpoint systems, and makes them invisible to hackers.		
5.	Program Control with Program Advisor: Program Control ensures that only legitimate and approved programs are allowed to run on the endpoint. Program Advisor is a real-time Vendor knowledge base of over a million trustworthy applications and suspected malware used to automatically set the Program Control configuration.		
6.	Heuristic virus scan: Should Scan files and identifies infections based on behavioral characteristic of viruses		
7.	On-access virus scan :Should Scan files as they are opened, executed, or closed, allowing immediate detection and treatment of viruses		

#	Minimum technical specification	Bidder Compliance (Y/N)	Product Documentation Reference
8.	Deep scan: Should Scan Runs a detailed scan of every file on selected scan targets		
9.	Scan target drives: Should Specifies directories and file types to scan		
10.	Scan exclusions: Should Specify directories and file extensions not to be scanned		
11.	Treatment options: Should Enables choice of action agent should take upon detection of virus: Repair, rename, quarantine, delete		
12.	Intelligent quick scan: Should Check the most common areas of the file system and registry for traces of spyware		
13.	Full-system scan: Should Scans local file folders and specific file types		
14.	Deep-inspection scan: Should Scan every byte of data on the computer		
15.	Scan target drives: Should Specify which directories and file types to scan		
16.	Scan exclusions: should Specify directories and file extensions not to be scanned		
17.	Treatment options: Should Enable choice of action agents should take upon detection of virus: Automatic, notify, or confirm		
18.	**Browser Security**		
a.	Should Support latest versions leading web browsers i.e. IE, Mozilla, Chrome, Safari etc.		
b.	Should Provide a dual browser mode that segregates corporate data from the Internet		
c.	Should Allow users the freedom to surf with full protection against malicious software that is automatically downloaded and phishing attempts		
d.	Should Secure through unique browser virtualization, heuristic anti-phishing and malware site detection		
e.	Should Support Browser Virtualization		
f.	Should Support Signature & Heuristic Phishing Protection		
g.	Should Support Site Status Check		

#	Minimum technical specification	Bidder Compliance (Y/N)	Product Documentation Reference
h.	Should Support Centralized Browser Security Policy Management		
i.	Should Support Centralized Browser Security Event Logging & Reporting		
19.	**Management Platform Support**		
a.	Operating systems: Should Support Windows Server 2008, 2012, 2016		
b.	Browsers: Should Support Internet latest version of leading web browsers		
c.	Client Platform Support		
d.	Should Windows 8, 10 (32 & 64 bit), Linux		
20.	**Gateway Security**		
a.	Should provide fast protection at the gateway across multiple protocols for inbound and outbound web traffic		
b.	The solution should provide protection against malware threats on all Web 2.0 file transfer channels		
c.	The solution should offer in built URL filtering with flexible policy controls, and in-depth reporting and alerts (the URL filtering license is required)		
d.	Virus Gateway should have option to configure to respond to virus detection in several ways i.e. Delete the file, quarantine the file, Alert email		
e.	The solution should have advanced application control capabilities with ability to monitor and control usage by end-users spanning multiple applications		
f.	In terms of SMTP anti-pam scanning the solution should be capable of acting as mail relay or MTA by itself.		
g.	Should have facility to block files based on file extensions over HTTP, FTP, SMTP, POP3 as well as IMAP		
h.	The solution should be able to detect compromised endpoints by network fingerprinting and behavioral modeling and should be able to block these infected end points by resetting the connection attempts to their phone home sites.		

#	Minimum technical specification	Bidder Compliance (Y/N)	Product Documentation Reference
i.	System should classify traffic into protocols without relying on specific port numbers (for example, port 80 for HTTP)		
j.	The solution should support load balancing for scanning, so that the traffic which needs to be scanned can be load balanced across the boxes in the cluster		
k.	Comprehensive Web reporting and alerting should be available out of box and should offer following reports:- Most accessed Web sites Most active users Spyware-infected computers Most common malware Network attacks Infection sources		
l.	Reports should be available by IP address or user if active directory integration is done		
21.	**Web Content Filtering**		
a.	Should be an integrated solution within the firewall or a standalone hardware appliance.		
b.	web content filtering solution should work independently without the need to integrate with proxy server		
c.	Web based management through https and command line interface support		
d.	should have facility to block URL' based on categories		
e.	The solution proposed should support at least 45+ million URLs categorized into 60+ default website categories across 50 different languages and 100+ protocol applications.		
f.	URL Database should be updated regularly		
g.	Solution should have dedicated categories for Adult material, gambling, Instant messaging, proxy avoidance, spyware ,malicious websites, Bots, phishing , key logger		
h.	should have configurable parameters to block/allow unrated sites		

#	Minimum technical specification	Bidder Compliance (Y/N)	Product Documentation Reference
i.	should have configurable options to allow/deny access to web sites in case if the URL rating service is unavailable		
j.	should have options to customize the block message information send to end users		
k.	Should have facility to schedule the configurations so that non work related sites are blocked during office hrs. and allow access to all sites except non harmful sites during non-office hrs.		
l.	Should have facility to configurable policy options to block web sites based on content		
m.	The solution should provide capabilities to customize URL, either it is in the URL database or not, into user defined categories.		
n.	Should have configurable policy options to define the URLs what needs to be blocked.		
o.	should have configurable policy options to define the URL exempt list		
p.	The solution should be able to block spywares/adwares etc.		
q.	The solution should have options to block java applets, activeX as well as cookies		
r.	The solution should have options to configure in such a way that in case if the primary fails the secondary becomes active without manual intervention		
s.	The solution should have options to block download of files over internet based on file extension (e.g. *.avi, *.mpeg, *.mp3 etc.)		
22.	**URL Filtering Features**		
a.	The solution should provide security related website categories to address specific security concerns include, but not limit to : a. Malicious Websites b. Key-loggers c. Phishing and Other Online Frauds d. Spyware – including drive-by spyware download and back channel		

#	Minimum technical specification	Bidder Compliance (Y/N)	Product Documentation Reference
	communication by spyware installed on local client. e. Potentially Unwanted software f. Bot Network g. The solution proposed should have capabilities to block back channel communication from spyware / key-logger infected machines to hacker host sites h. The solution should have the ability to apply different policies to different users, different client IP address and address range and different user groups i. The solution should have the capability for Embedded URLs in selected search engines can also be filtered individually j. The solution should support Time based Quota policies for URL categories, users, IP, networks, user groups etc. k. The solution should have the ability for users to define ─Regular Expressions‖ to precisely identify targeted URL. l. Solution should have dedicated categories for Adult material, gambling, Instant messaging, proxy avoidance, spyware ,malicious websites, Bots, phishing , key loggers m. The solution should provide capabilities to customize URL, either it is in the URL database or not, into user defined categories. n. The solution should support risk classes for Security, Legal Liability, Productivity Loss, Bandwidth Loss and Business Usage at least so that predefined URL categories can be associated with these risk classes o. Ability to collect certain uncategorized or security related URLs to feedback, improve URL categorization and security effectiveness		

#	Minimum technical specification	Bidder Compliance (Y/N)	Product Documentation Reference
	p. The solution should support display of web based block pages and the block pages should be customizable		
23.	**Spam Filtering**		
a.	The proposed solution should Stop spam, denial-of-service attacks, and other inbound email threats using industry-leading technologies and response capabilities, leverage adaptive reputation management techniques that combine global and local sender reputation analysis to reduce email infrastructure costs by dropping up to 90% of spam at the connection level, Filter email to remove unwanted content, demonstrate regulatory compliance, and protect against intellectual property and data loss over email, Secure and protect other protocols, such as public IM communications, using the same management console as email, Obtain visibility into messaging trends and events with minimal administrative burden.		
b.	The proposed solution should automatically back up all configuration and quarantine databases on the appliance at specified intervals. Administrators should be given an option to store data on the local machine or a remote server.		
c.	should be able to detect spam mails in SMTP, POP3 as well as IMAP protocols		
d.	The proposed solution should have inspection facility on the header and body of the mail to check for spam URI content and identify whether the mail is a spam mail or not.		
e.	option should be available to manually configure multiple RBL& ORDBL servers to check for spam mail		
f.	should have options to configure white list as well black list based on IP address and validate against the same to detect whether a mail is spam mail or not		

#	Minimum technical specification	Bidder Compliance (Y/N)	Product Documentation Reference
g.	Should have configurable parameter to enable HELO DNS lookup to check whether a mail is a spam or not.		
h.	Should have configurable parameter to enable return email DNS lookup to check whether a mail is a spam or not.		
i.	Should have provision to define banned key words and check against that key words to identify spam mails.		
j.	Should have options to define mime headers and check against the same to identify spam mail.		
k.	The solution should have Global sender reputation and local sender reputation analysis to reduce email infrastructure costs by restricting unwanted connections.		
l.	Solution must be scalable to incorporate the following with no installation of component on clients should need be in future:		
m.	Email archiving, mail box archiving, file archiving, personal folders (.pst files) consolidation, journaling, discovering mails		
n.	Integration with data loss prevention technologies to check loss of data through mails at gateway		
o.	The proposed solution should have an option to restore an appliance to its original image configuration.		
p.	Should have configurable spam actions for detected spam mails (e.g. tag the mail, delete the spam mail etc.).		

4.3.21 Mailing and Messaging Solution

#	Minimum technical specification	Bidder Compliance (Y/N)	Product Documentation Reference
1.	Make	<to be provided by the bidder>	
2.	Model	<to be provided by the bidder>	
3.	**General**		
a.	Network/Server edition should run on Linux /Windows.		

b.	Desktop client should run on Mac, Linux and Windows.			
c.	Solution should be based on open standards			
d.	Should support advanced search and file indexing for large inboxes			
e.	Ability to use custom logos in the web interface			
f.	Should support e-mail, Address Book, Calendar, Task & File Server			
g.	Should support real-time backup and restore			
h.	Should support clustering/High-Availability			
i.	Ability to access the Mail server via IMAP clients, with the option to connect over SSL/TLS			
j.	Ability to access the Mail server via POP clients, with the option to connect via SSL/TLS			
k.	Comprehensive suite of standards-based web services APIs enabling seamless integration with other applications			
l.	Ability to utilize Active Directory for user authentication and/or Global Address List			
m.	Admin can configure an initial password in the migration wizard and import wizard for newly provisioned accounts			
n.	Should support multi-tenancy			
o.	Should support e-mail Archiving & Discovery			
p.	Should have rich, interactive, web-based interface for end user functions (access via HTTP or HTTPS)			
q.	Ability to customize the colors and appearance of the web interface			
r.	Option to check and correct spelling in a mail message, calendar appointment, or web Document			
s.	Ability to share Address Books, Calendars, and Notebooks (Documents) with internal users and groups (read or write access)			
t.	Ability to share Address Books, Calendars, and Notebooks (Documents)			

	with external users via a custom password (read access)		
u.	Ability to quickly categorize messages, contacts, and/or documents by attaching "Tags" with user-defined names and colors		
v.	Option to quickly view attachments in HTML format		
w.	Should support conversations span folders		
x.	Ability to create personal folders and folder hierarchies		
y.	Ability to print a message and see a print preview		
z.	Ability to sort messages based on subject, date, or sender		
aa.	Ability to flag/unflag messages/conversations for follow up		
bb.	Ability to define filter rules and priorities for incoming messages		
cc.	Ability to enable/disable a custom away message		
dd.	Ability to add a custom signature to a message		
ee.	Option to popup a separate window when composing a message		
ff.	Ability to save in-progress messages to a Drafts folder		
gg.	Ability for a user to set an automatic forwarding address and choose whether to leave a copy in the primary mailbox		
hh.	Option to Reply or Reply-All while retaining the attachments from the original message		
ii.	Right-clicking a message displays a menu of actions to take on that message (e.g. Mark Read, Reply, Delete)		
jj.	Right-clicking an email address displays a menu of actions to take on that address (e.g. view website, add/edit contact, create filter, search for messages)		
kk.	Ability to export a set of messages as a ZIP file		
ll.	Ability to toggle between Reply and Reply-All while composing a reply		

mm.	Users can set their default preference for viewing messages in the reading pane		
nn.	Users can set the default font family, font size and font color to use when composing email messages and Documents pages		
oo.	Users can share their mailbox folders and set the permission levels to manage or to view-only.		
pp.	Users can insert inline images in email messages and calendar appointments		
qq.	Admins can configure the maximum number of characters used in a signature		
rr.	Admin can define expiration policy for individual mailbox folders		
ss.	Users will receive an email message warning of quota usage based on a threshold defined by administrator		
tt.	Users can attach a URL to an email message		
uu.	Users can double-click on a message in message view to expand the view pane to full view		
vv.	Users can define multiple email signatures to use		
ww.	Users can check multiple emails in the list view to mark as read/unread/tag, delete, or to move to a different folder		
xx.	When sending a message, the priority is normal, but it can be set to high or low as well		
yy.	Users can get immediate notification of new mail		
zz.	Multiple messages can be selected and forwarded in one email		
aaa.	Users can right click on a folder to see the number of messages and the total size of items in folder		
4.	**Address Book**		
a.	Business card view of Contacts		
b.	List view of Contacts with preview pane		
c.	Ability to import/export Contacts in .csv format		
d.	Ability to import/export contacts in vCard (.vcf) format		

e.	Ability to print a single Contact or list of Contacts and see a print preview		
f.	Right-clicking a Contact displays a menu of actions to take on the Contact (e.g. compose message, search for messages)		
g.	Ability to drag a Contact to a mini-calendar date to create an appointment with that Contact		
h.	Ability to create multiple Address Books in a single mailbox		
i.	Ability to move/copy contacts from one Address Book to another (based on access privileges)		
j.	Ability to create group contact lists in their user Address Books		
k.	Address book displays individual contact information in tabbed view		
l.	Photos and images can be uploaded to contacts in Address Books		
5.	**Calendar**		
a.	Ability to schedule personal appointments		
b.	Ability to schedule meetings and view attendees' free/busy information		
c.	Ability to create recurring meetings and exceptions to recurring meetings		
d.	Ability to book resources (locations, equipment, etc.) for a meeting		
e.	Ability to configure a resource to auto-respond to scheduling requests based on availability		
f.	Option to enable an alert popup for upcoming appointments		
g.	Appointments/schedules are automatically displayed in the users current time zone		
h.	Ability to set an explicit time zone for an appointment		
i.	Ability to view calendars in Day, Week, Work Week, or Month views		
j.	User setting for the first day of the week; value chosen impacts the Week calendar view		
k.	Ability to create an appointment and/or drag an appointment's boundaries inline in calendar views		

l.	Ability to quickly mark Accept/Tentative/Decline from calendar views		
m.	Declined appointments display faded so that the user remains aware of their occurrence		
n.	Ability to print calendars in day, week, work week, or month views and see a print preview		
o.	Hovering over an appointment in calendar view displays additional appointment details		
p.	Option to display a miniature calendar at all times		
q.	Hovering over a date in the mini-cal displays calendar information for that date		
r.	Right-clicking on the mini-cal displays a menu of actions to take on the associated date (e.g. add appointment, search for messages)		
s.	Ability for a user to create multiple calendars within a single account		
t.	Ability for a user to designate which calendars will be included in the user's free/busy calculations		
u.	Ability to subscribe to an external calendar in iCalendar (.ics) format		
v.	Ability to publish/export a calendar in iCalendar (.ics) format		
w.	Ability for a user to view multiple calendars overlaid in the same view, which each calendar optionally represented by a different color		
x.	When viewing multiple calendars, option to view that indicates the degree of conflict at each potential time slot		
y.	Users can import calendar iCalendars (.ics)		
z.	Appointments can be marked as private or public.		
aa.	Administrators can configure the Calendar feature to be able to create only personal appointments		
bb.	Users can search for appointments within their calendars		
cc.	Public calendars display in HTML read-only format		

6.	**Tasks**		
a.	Add tasks and set the start and due date, set the priority and keep track of the progress and percentage complete		
b.	Share task lists with internal and external users and set permission levels to manage or to view-only		
c.	Users can organize task lists into folders		
d.	Users can sort tasks by Status or Due Date		
e.	Users can set the priority of tasks to high, normal or low		
f.	Individual tasks can be tagged		
g.	Files can be attached to a tasks		
7.	**Documents**		
a.	Ability to create rich web Documents with WYSIWYG or HTML editing		
b.	Ability to create a notebooks as a Document repository and as a mechanism for navigating through Documents		
c.	Ability to create multiple notebooks in a single mailbox		
d.	Ability to create a notebook that is shared by everyone within a domain		
e.	Ability to insert links in Documents to other Documents or to external URLs		
f.	Ability to upload Attachments as Documents		
g.	Ability to embed rich content objects as independently editable items inside a web Document		
h.	Ability to embed an image as an ALE object inside a web Document		
i.	Ability to embed a spreadsheet as an ALE object inside a web Document		
j.	Ability to print a Document and see a print preview		
k.	Pages show when last modified and version		
l.	Users can upload files to their mailbox and can access them from any computer		
m.	Users can add email attachments to a selected folder		
8.	**Search**		
a.	Server-side indexing of mailbox content, enabling fast and efficient search from g g g the web interface		

b.	Ability for a search to include any number of conditions combined via Boolean-like expressions (AND, OR, NOT, etc.)		
c.	Ability to use text commands to execute searches		
d.	Advanced interface for building searches		
e.	Ability to search for a specific item type (Mail, Contacts, Documents, etc.) or across item types		
f.	Ability to search using a prefix plus a wildcard		
g.	When using Search Builder, the search result set updates continuously as search conditions are changed		
h.	Ability to save searches for subsequent one-click re-execution		
i.	Ability to search for items that contain specific keywords		
j.	Ability to search for items with a specific date or within a specific date range		
k.	Ability to search for items that contain an attachment		
l.	Ability to search for items that contain an attachment of a certain type(s)		
m.	Ability to search for items that have a specific flagged/unflagged status		
n.	Ability to search for items that are in a specific folder		
o.	Ability to search for items based on storage size		
p.	Ability to search for items based on read/unread status		
q.	Ability to search for items with specific recipients in the To /Cc fields		
r.	Ability to search for items from a specific sender		
s.	Ability to search for items based on subject		
t.	Ability to search for items that include a specific Tag(s)		
u.	Ability to search for items that were sent to or received from a specific domain		
v.	Ability to search for Contacts in a Shared Address Book		
w.	Ability to search for content inside attachments		

x.	Can search for appointments in calendars up (up to 180 days)		
y.	Administrator can disable the indexing of junk mail		
9.	**Domain-Level Management**		
a.	Ability to create and manage multiple mail domains within a single instance of Messaging Solution		
b.	Ability to use different Global Address Lists for each domain		
c.	Ability to use different authentication stores for each domain		
d.	Ability to delegated domain-level administrators to manage users and other settings specific to a domain		
e.	Ability to create domain-specific custom branding of the web interface		
f.	Ability to enable a domain admin to update account quotas up to a maximum set value		
g.	Ability to set quota for each domain (either unlimited or a maximum value per account)		
h.	Ability to move a domain		
i.	Ability to search across mailboxes from the administration console		
10.	**Storage**		
a.	Messages (including attachments) sent to multiple users are stored once to optimize storage space		
b.	Ability to set quotas for mailbox size and number of Contacts		
c.	View of mailboxes sortable by quota, total mailbox size, or % quota consumed		
d.	Ability to define retention policies for all messages, trashed messages, and/or junk messages		
e.	Ability to move a mailbox(es) from one server to another without requiring system downtime or affecting other mailboxes		
f.	Ability to run a regularly scheduled process that moves older messages to a secondary storage volume		
11.	**System Health & Security**		
a.	Should have native anti-virus & anti-spam mechanism		

b.	Administrator interface setting to specify spam quarantine and kill thresholds		
c.	Messages that users mark as Junk / Not Junk are automatically fed into the spam training engine		
d.	Administrator interface setting to define the update frequency for virus signatures		
e.	Ability to enforce client authentication to the SMTP server before relaying mail (with option to require authentication over TLS)		
f.	Graphical display of system activity including disk usage, message volume, and AS/AV results		
g.	Ability to monitor the status of all core system servers/services in a single view		
h.	Ability to block attachments based on criteria such as attachment type or size		
i.	Ability to enforce that attachments be viewed as HTML, enabling risk-free attachment viewing without requiring attachment-native applications on the viewer's machine		
j.	Install and manage certificates from the administration console		
12.	**Compatibility & Interoperability**		
a.	MAPI-based synchronization of mail, contacts, and calendar data between Outlook and the proposed solution server		
b.	Online/offline status is automatically detected, enabling the user to work without having to specify their connection status		
c.	Synchronization operations are cached and synchronized as an asynchronous process, enabling optimal Outlook performance		
13.	**Mobile Devices**		
a.	AJAX Mobile Web Browser		
b.	iPhone Email, Contact, Calendar sync		
c.	Windows Mobile and other smartphone Email		
d.	BlackBerry Email, Contact, Calendar sync		

4.3.22 Identity Access Management

SL. No.	Description	Bidder Compliance (Yes / No)	Product Documentation Reference
1	Make	<to be provided by the bidder>	
2	Model	<to be provided by the bidder>	
3	**Identity Management**		
3.1	The Identity and access management should be able to provide complete user lifecycle identity management for all types of users.		
3.2	The solution should provide identity management, governance and Identity management portal, including entitlement certification and role management		
3.3	The proposed solution should provide user provisioning and de-provisioning on all target systems, automatic account provisioning, removal, and approval processes throughout the user's entire lifecycle.		
3.4	The proposed solution should have customizable workflows to support the unique way environment approves, alerts, and schedules these activities.		
3.5	The proposed solution should provide centralized control of identities, users, roles and policies across on-premise and cloud applications.		
3.6	The proposed solution should provide User self-service to manage attributes of their own identities, reset passwords and request access to resources.		
3.7	The proposed solution should support Password Synchronization to reflect changes in identity management systems and target applications		
3.8	The proposed solution provide Privilege cleanup by examining existing system entitlements and highlights excessive or unnecessary privileges. Delivers details such as such as how often a resource was accessed or if an entitlement causes a security policy violation.		
3.9	The proposed solution should provide Identity and access governance policies using centralized engine that helps establish and enforce a consistent set of business and regulatory compliance policies.		

SL. No.	Description	Bidder Compliance (Yes / No)	Product Documentation Reference
3.10	The proposed solution should support Entitlements certification by providing easy to use interface through which managers or resource owners can view and certify that privileges are appropriate or should be removed, thus helping meet compliance requirements.		
3.11	The proposed solution should support Role modelling analysis to efficiently sort through extremely large volumes of user and privilege information to discover potential roles.		
3.12	The system should be able to detect any changes in the target systems via the concept of reverse synchronization and associate various actions upon detection		
3.13	The solution should have ability perform bulk jobs for example user changes, scheduled jobs		
3.14	The proposed solution should offer an easy-to-use, configurable user-centric Risk Model that identifies areas of risk caused by users with high risk scores.		
4	**Single Sign on under Identity Management**		
4.1	The solution should have a capability which helps to prevent unauthorized users from hijacking legitimate sessions with stolen cookies and assures that the client who initiated the session is the same client that is requesting access.		
4.2	The solution should have capability to support various SSO architectures that can be used independently or mixed and match to meet various business needs such as: — Agent-based policy enforcement points — Centralized gateway enforcement points — Support for today's open standards including SAML, OAuth, OpenID and WS-Federation — Agent-less based approach to securely pass claims to applications without the use of proprietary APIs — REST and SOAP-based Web APIs to allow applications to remotely call Single Sign-On as a Web service for authentication or authorization		
4.3	The solution should provide secure single sign-on and flexible web access management to		

SL. No.	Description	Bidder Compliance (Yes / No)	Product Documentation Reference
	applications and Web services either on-premise, in the cloud, from a mobile device or at a partner's site.		
4.4	The solution shall support SSO by passing the user's identity among heterogeneous servers securely. No additional authentication is required.		
4.5	The solution should provide session assurance.		
4.6	The solution should provide centralized session management to securely manage a user's online session.		
5	**Privilege Access Management Under Identity Management**		
5.1	The proposed solution should be appliance based and provide the capability to manage Password Vault, Access Management, Session Recording, Application to Application (allows dynamic password access from applications), etc. within a single hardened platform.		
5.2	The proposed solution should supports a process to automatically synchronize with a DR site over a WAN and provide built-in replication of the password vault aiding disaster recovery		
5.3	The Proposed solution should have ability to define a zero trust, explicitly allow only access methodology.		
5.4	The proposed solution should provide built in Active-Active High Availability and Load Balancing along with built-in clustering without the use of a traffic load balancer.		
5.5	The Proposed solution should have ability to provide real-time data synchronization among a cluster.		
5.6	The proposed solution should not require using third party software or hardware such as Operating Systems, Databases, High Availability, Load Balancers, etc.		
5.7	The proposed solution should be browser independent and there shouldn't be any browser dependency to manage and record the sessions.		
5.8	The proposed solution should provide highly efficient integrated video session recording with low storage requirements.		

SL. No.	Description	Bidder Compliance (Yes / No)	Product Documentation Reference
5.9	The proposed solution should provides in-line command filtering using white lists/black lists for SSH, network devices command line operations.		
5.10	The proposed solution should be able to support application based session via RDP protocol in which the user can be confined, rather than requiring RDP to a full desktop.		
5.11	The proposed solution should support to require an approval by designated users as a condition of accessing the credentials for managed accounts. The Solution should also enforce users to specify reason when requesting access for a privileged account.		
5.12	The proposed solution should provide tools/APIs for enabling applications that require access to privileged accounts to access credentials programmatically, eliminating the need to "hard code" credentials into the script or application. Password should be rotated automatically.		
5.13	The Proposed solution should have ability to manage target OS, Databases, Network, security devices, Virtual and cloud environments local administrator credentials through single appliance.		
5.14	The proposed solution should provide threat analytics that provides a continuous, intelligent monitoring capability that helps enterprises detect and stop hackers and malicious insiders before they cause damage.		
6	**Host Based Access Control Under Identity Management**		
6.1	The proposed solution should provide granular access control on critical Servers to protect the access even if the servers are accessed directly from the console.		
6.2	The proposed solution should support all Unix, Linux and Windows platforms and should be agent based.		
6.3	The proposed solution should control and monitor privileged user access to files, folders, processes and registries, enabling accountability, incoming/outgoing TCP/IP protection, integrity monitoring and segregation of duties.		

SL. No.	Description	Bidder Compliance (Yes / No)	Product Documentation Reference
6.4	The proposed solution should restrict superuser privileges with finer level of granularity than what is available in the host operating system.		
6.5	The proposed solution should support authentication to Linux and Unix using Windows AD credential and also provide User ID management (including UNIX files and NIS)		
7	**Authentication under Identity Management**		
7.1	The proposed solution should provide PKI and Risk Based authentication. It should also support mobile OTP.		
7.2	The proposed solution should have tight integration with proposed SSO solution		
7.3	The proposed solution should have Pre-built rules that cover typical fraud patterns.		
7.4	The proposed solution should support customization of pre-built rules or creation of new rules quickly and easily.		
7.5	The proposed solution should Self-learning scoring engine based on statistical modeling		
7.6	The proposed solution should have Device identification mechanism using multiple variable device fingerprinting		
7.7	The risk based engine should also use geo location criteria		
7.8	The proposed solution should have policy-based system to flag and manage cases of suspicious activity.		
7.9	The proposed solution should Integrate data from multiple channels.		
7.10	The proposed solution should learn end user behavior and suggests step-up authentication when there is a deviation from normal behavior.		
7.11	The proposed solution should support out of band authentication via SMS, Email and Voice including mobile push.		

4.3.23 Enterprise Database

#	Description	Bidder Compliance (Yes/No)	Product Documentation Reference
1.	Make	<to be provided by the bidder>	
2.	Model	<to be provided by the bidder>	
3.	Database License should be un-restricted and perpetual, to prevent any noncompliance in an event of customization & integration.		
4.	Databases shall support multi-hardware platform.		
5.	RDBMS should support Unicode with Indian Language support		
6.	RDBMS should have spatial capability and should be capable of storing vector (2D, 3D), raster data as well as the metadata.		
7.	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.		
8.	Database shall have built-in backup and recovery tool, which can support the online backup.		
9.	RDBMS should support of seamless data transformation from on premise to public cloud and from public cloud to on premise.		
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.		
11.	Database shall support for central storage of data with multiple instances of database in a clustered environment access the single /multiple database.		
12.	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		

#	Description	Bidder Compliance (Yes/No)	Product Documentation Reference
	performance, availability and management.		
13.	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		
14.	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.		
15.	Ability to recover the node on fly or with limited timelines with-out Unloading/ reloading data.		
16.	RDBMS should provide continuous availability features to address hardware failures, instance failures, human errors like accidental deletion of data, tables etc.		
17.	Database shall provide native functionality to store and retrieve XML, Images and Text data types.		
18.	Database shall provide native functionality to store XML, within the database and support search, query functionalities.		
19.	RDBMS should support spatial data types.		
20.	Database shall have Active-Passive or Active-Active failover clustering with objectives of scalability and high availability.		
21.	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.		
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.	Database shall be having native auditing capabilities for the database.		

#	Description	Bidder Compliance (Yes/No)	Product Documentation Reference
24.	Database shall be having built-in provision to Administer database / database clusters, Monitor performance, Maintain database, Backup and recovery, Recovery management, Disaster recovery management.		
25.	Availability of recovery/restart facilities of the DBMS.		
26.	Automated recovery/restart features provided that do not require programmer involvement or system reruns.		
27.	Program restart should be provided from the point of failure.		
28.	RDMS should have the ability to manage recovery/restart facilities to reduce system overhead.		
29.	Provides extra utilities to back up the databases by faster means than record by record retrieval.		
30.	The database should provide controls over who, when, where and how applications, data and databases can be accessed.		
31.	RDBMS should be possible to prevent privileged IT users such as DBAs and administrators from accessing and modifying the data.		
32.	The database should provide multi-factor authentication based controls and policies preferably taking account of application context etc.		
33.	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.		
34.	System should record the date and time stamp for all records generation/modification.		
35.	Solution should offer spatial analytic functions for data mining applications, such as binning, spatial correlation, co-location mining, spatial clustering, and location prospecting		

4.3.24 Enterprise Backup Software

#	Description	Bidder Compliance (Yes/No)	Product Documentation Reference
1.	Make	<to be provided by the bidder>	
2.	Model	<to be provided by the bidder>	
3.	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.		
4.	The solution should offer centralized, web-based administration with a single view of all back up servers		
5.	The proposed backup solution should allow creating tape clone facility after the backup process.		
6.	Scheduled unattended backup using policy-based management for all Server and OS platforms		
7.	The proposed Backup Solution has in-built frequency and calendar based scheduling system.		
8.	The software should support on-line backup and restore of various applications and Databases		
9.	The backup software should be capable of having multiple back-up sessions simultaneously		
10.	The proposed backup solution should be capable of taking back up of SAN environment as well as LAN based backup.		
11.	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		
12.	The backup software should support different types of user interface such as GUI, Web- based interface		
13.	The proposed Backup Solution has in-built media management and supports cross		

#	Description	Bidder Compliance (Yes/No)	Product Documentation Reference
	platform Device & Media sharing in SAN environment.		
14.	Backup Software is able to rebuild the Backup Database/Catalogue from tapes in the event of catalogue loss/corruption.		
15.	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.		
16.	Backup Solution shall be able to copy data across firewall.		
17.	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		
18.	The backup software should be able to support versioning and should be applicable to individual backed up objects.		

4.3.25 Directory Services

#	Description	Bidder Compliance (Yes/No)	Product Documentation Reference
1.	Make	<to be provided by the bidder>	
2.	Model	<to be provided by the bidder>	
3.	Should be compliant with LDAP v3		
4.	Support for integrated LDAP compliant directory services to record information for users and system resources		
5.	Should provide authentication mechanism across different client devices / PCs		
6.	Should provide support for Group policies and software restriction policies		
7.	Should support security features, such as Kerberos, Smart Cards, Public Key Infrastructure (PKI), etc.		
8.	Should provide support for X.500 naming standards		
9.	Should support that password reset capabilities for a given group or groups of		

#	Description	Bidder Compliance (Yes/No)	Product Documentation Reference
	users can be delegated to any nominated user		
10.	Should support that user account creation/deletion rights within a group or groups can be delegated to any nominated user		
11.	Should support that user account creation/deletion rights within a group or groups can be delegated to any nominated user		
12.	Should support directory services integrated DNS zones for ease of management and administration /replication.		

4.4 Integrated Traffic Management System (ITMS)

4.4.1 Adaptive Traffic Control System (ATCS)

4.4.1.1 Functional Requirements - Adaptive Traffic Control System (ATCS)

#	Building Blocks	Bidder Compliance (Yes/No)	Product Reference
1.	Traffic Signal Controller		
2.	Camera based Vehicle Detectors		
3.	Countdown timer		
4.	Communication Network		
5.	Software Application		

4.4.1.1.1 Functional Requirements -Traffic Signal Controller

#	Description	Bidder Compliance (Yes/No)	Proposed Solution and Product Reference
1.	Make	<to be provided by the bidder>	
2.	Model	<to be provided by the bidder>	
3.	The Traffic Signal Controller equipment is a 32 bit or 64 bit microcontroller with solid state traffic signal lamp switching module with the ability to program any combination of traffic signal stages, phases and junction groups. The controller will ideally have a conflict monitoring facility to ensure that conflicting, dangerous are pre-flagged		

#	Description	Bidder Compliance (Yes/No)	Proposed Solution and Product Reference
	at the programming stage and these are disallowed even during manual override phase.		
4.	The Traffic Signal Controller will be adaptive so that it can be controlled through the central traffic control Centre as an individual junction or as part of group of traffic junctions along a corridor or a region. The signal controller design must be flexible for the junction could be easily configured to be part of any corridor or group definition and could be changed through central command controller easily		
5.	Site specific configuration data shall be stored in a non-volatile memory device (FLASH memory) easily programmable at the site through keypad or laptop. A minimum of 512KB flash memory and 128KB RAM shall be provided. Volatile memory shall not be used for storing the junction specific plans or signal timings.		
6.	All timings generated within a traffic signal controller shall be digitally derived from a crystal clock which shall be accurate to plus or minus 100 milliseconds.		
7.	The controller shall provide a real time clock (RTC) with battery backup that set and update the time, date and day of the week from the GPS. The RTC shall have minimum of 10 years battery backup with maximum time tolerance of +/- 2 sec per day.		
8.	The controller shall have the facility to update the RTC time from ATCS server, GPS and through manual entry.		
9.	The traffic signal system including controller shall have provision audio output tones and should be disabled friendly for.		
10.	The controller shall be capable of communicating with the ATCS server through Ethernet on a managed leased line network or any other appropriate stable communication network.		

4.4.1.1.1.1 Police Panel

The controller shall provide the following facilities in a separate panel with provision for lock and key arrangements for use by the authorized persons.

#	Description	Bidder Compliance (Yes/No)	Proposed Solution and Product documentation Reference
1.	Four Hurry Call switches: The Hurry Call mode will provide the means to force the controller to a defined stage, without violating safety clearances. A preemption input may be used to demand the Hurry Call mode to give right of way to emergency vehicles. It should be possible to configure the Hurry Call switches to any stage as per site requirements.		
2.	One Forced Flash Switch: Activation of this switch should force the signal to Flashing Amber / Flashing Red.		
3.	One Auto / Manual Switch: Activation of this switch should enable manual operation of the controller. Deactivation of the manual switch shall continue from the current stage without interruption.		
4.	One Manual Advance Pushbutton Switch: In manual operation mode, the stages appear in the sequence specified in the signal plan timetable. Activating the pushbutton switch shall terminate the currently running stage and start the next, without violating safety clearances.		
5.	One Junction OFF Switch: Activating this switch should put OFF all signal lamps. On deactivation of the switch the traffic signal controller shall resume its normal operation without violating any safety clearances.		

4.4.1.1.1.2 Modes of Operation

The traffic signal controller shall have the following modes of operation:

#	Description	Bidder Compliance (Yes/No)	Proposed Solution and Product documentation Reference
1.	Fixed Time: In fixed time (pre-timed) mode the traffic signal controller shall execute stage timings according to the site specific timetable maintained in the traffic signal controller FLASH memory. Inputs from vehicle detectors shall be ignored in this mode and no preemption		

#	Description	Bidder Compliance (Yes/No)	Proposed Solution and Product documentation Reference
	shall be made on any stage. Cycle time remains constant in every cycle execution for a given time period.		
2.	Vehicle Actuation with All Stages Preemption: In the vehicle actuation with all stages preemption mode, the traffic signal controller shall execute stage timings as per demand from vehicle detectors within the constraints of Minimum Green, Maximum Green running period for the stage and Cycle time stored in the traffic signal controller FLASH memory. Preemption shall be possible for all demand actuated stages. Cycle time may vary in every cycle execution.		
3.	Semi-Actuation: In the semi-actuation mode, the traffic signal controller shall execute stage timings in the vehicle actuated stages as per demand from vehicle detectors within the constraints of Minimum Green, Maximum Green running period for the stage and Cycle time stored in the traffic signal controller FLASH memory. All other stages shall execute the Maximum green time configured for the stage. Preemption shall be possible for all demand actuated stages. Cycle time may vary in every cycle execution.		
4.	Stage Skipping: The traffic signal controller shall not execute the stage enabled for skipping when there is no vehicle demand registered for the stage till clearance amber time of the previous stage.		
5.	Vehicle Actuation with Fixed Cycle length: In vehicle actuation with fixed cycle length mode, the traffic signal controller shall execute stage timings as per demand from vehicle detectors within the constraints of Minimum Green, Maximum Green running period for the stage and Cycle time shall be maintained constant during a given timeslot. Preemption for all demand actuated stages except for Priority Stage shall be possible.		

#	Description	Bidder Compliance (Yes/No)	Proposed Solution and Product documentation Reference
6.	Full ATCS (FATCS): In FATCS mode, the traffic signal controller shall execute stage timings as per demand within the constraints of Minimum Green, Maximum Green running period for the stage and Cycle time specified by the Central Computer during every cycle switching. Preemption for all demand actuated stages except Priority Stage shall be possible in this mode. The traffic signal controller shall identify a communication failure with the central computer within a specified time period. In such an event the signal plan timings shall be executed from the local timetable stored in the traffic signal controller FLASH memory. Fallback mode of the traffic signal controller shall be vehicle actuated. On restoration of the communication with central computer the traffic signal controller shall automatically resort to FATCS mode. The traffic signal controller shall accept commands for remote selection / de-selection of the following from the Central Computer at CCCC. Hurry Call Flashing Amber / Flashing Red Junction Off If not reverted to the normal operation within the time period listed below, the traffic signal controllers shall timeout the commands and operate normally ▪ Hurry Call – 5 Minutes ▪ Flashing Amber / Flashing Red – 30 Minutes Junction Off – 30 Minutes The traffic signal controller shall report the following to the Central Computer through the communication network every cycle or on an event as appropriate. Green time actually exercised for each approach (stage preemption timing)		

#	Description	Bidder Compliance (Yes/No)	Proposed Solution and Product documentation Reference
	against the Green running period set for the approach by the central c omputer. Mode of Operation Lamp failure, if any Output short circuit, if any Detector failure, if any		

4.4.1.1.1.3 Traffic Signal Controller Operating Parameters

Phases - The controller shall have facility to configure 32 Phases either for vehicular movement, filter green, indicative green, pedestrian movement or a combination thereof.

#	Description	Bidder Compliance (Yes/No)	Proposed Solution and Product documentation Reference
1.	It shall be possible to operate the filter green (turning right signal) along with a vehicular phase. The filter green signal shall flash for a time period equal to the clearance amber period at timeout when operated with a vehicular phase.		
2.	The pedestrian phase signal shall be configured for flashing red or flashing green aspect during pedestrian clearance.		
3.	It shall be possible to configure any phase to the given lamp numbers at the site.		
4.	Stages – The controller shall have facility to configure 32 Stages		
5.	Cycle Plans – The controller shall have facility to configure 24 Cycle Plans and the Amber Flashing / Red Flashing plan. It shall be possible to define different stage switching sequences in different cycle plans. The controller shall have the capability for a minimum of 32 cycle-switching per day in fixed mode of operation.		
6.	Day Plans – The controller shall have facility to configure each day of the week with different day plans. It shall also be possible to set any of the day plans to any day of the week. The controller shall have the capability to configure 20 day plans.		

#	Description	Bidder Compliance (Yes/No)	Proposed Solution and Product documentation Reference
7.	Special Day Plans – The controller shall have facility to configure a minimum of 20 days as special days in a calendar year.		
8.	Starting Amber – During power up the controller shall initially execute the Flashing Amber / Flashing Red plan for a time period of 3 Seconds to 10 Seconds. The default value of this Starting Amber is 5 Seconds. Facility shall be available to configure the time period of Starting Amber within the given limits at the site.		
9.	Inter-green – Normally the inter-green period formed by the clearance Amber and Red extension period will be common for all stages. However, the controller shall have a facility to program individual inter-green period from 3 Seconds to 10 Seconds.		
10.	Minimum Green – The controller shall allow programming the Minimum Green period from 5 Seconds to 10 Seconds without violating the safety clearances. It should not be possible to preempt the Minimum Green once the stage start commencing execution.		
11.	All Red – Immediately after the Starting Amber all the approaches should be given red signal for a few seconds before allowing any right of way, as a safety measure. The controller shall have programmability of 3 Seconds to 10 Seconds for All Red signal.		
12.	Signal lamps monitoring – The controller shall have inbuilt circuitry to monitor the lamp status		
13.	Green – Green Conflict Monitoring – The controller shall have a facility to list all conflicting phases at an intersection. The controller should not allow programming of these conflicting phases in a Stage. A hardware failure leading to a conflict condition (due to faulty devices or short circuit in the output) shall force the signal into Flashing Amber / Flashing Red.		
14.	Cable less Synchronization – It shall be possible to synchronize the traffic signal controllers installed in a corridor in the		

#	Description	Bidder Compliance (Yes/No)	Proposed Solution and Product documentation Reference
	following modes of operation, without physically linking them and without communication network. GPS enabled RTC shall be the reference for the cable less synchronization.		
15.	Fixed Time mode with fixed offsets		
16.	Vehicle Actuated mode with fixed offsets		

4.4.1.1.1.4 Input and Output facilities

#	Description	Bidder Compliance (Yes/No)	Proposed Solution and Product Reference
1.	Lamp Switching: The controller shall have maximum 64 individual output for signal lamp switching, configurable from 16 to 32 lamps. The signal lamps shall be operating on appropriate DC/AC voltage of applicable rating		
2.	Detector Interface: A minimum of 16 vehicle detector inputs shall be available in the controller. All detector inputs shall be optically isolated and provided with LED indication for detection of vehicle.		
3.	Communication Interface: The traffic signal controller shall support Ethernet interface to communicate with the ATCS server		
4.	Power Saving: The traffic signal controller shall have a facility to regulate the intensity of signal lamps during different ambient light conditions thereby saving energy.		
5.	Real-time Clock (RTC): The GPS receiver for updating time, date and day of the week information of the traffic signal controller should be an integral part of the traffic signal controller.		
6.	The traffic signal controller shall update the date, time and day of the week automatically from GPS during power ON and at scheduled intervals.		
7.	Manual entry for date, time and day of week shall be provisioned for setting the traffic signal controller RTC (Real Time Clock).		
8.	It shall be possible to set the RTC from the Central Server when networked		

#	Description	Bidder Compliance (Yes/No)	Proposed Solution and Product Reference
9.	Keypad (optional): The traffic signal controller shall have a custom made keypad or should have provision for plan upload and download using PC/laptop/Central Server		
10.	Operator Display (optional): The traffic signal controller shall optionally have a LED backlit Liquid Crystal Display (LCD) as the operator interface.		

4.4.1.1.2 Functional Requirement - Camera based Vehicle Detector

The detector equipment is a separate logic unit, which may be integrated into the controller, or alternatively mounted in its own housing. The outputs of the detectors indicate the presence of vehicles and are used to influence the operation of the traffic signal controller and shall generate counts, demands and extensions for right-of-way. Means shall be provided so that a detector may be connected to demand and / or extend a phase movement as specified.

#	Description	Bidder Compliance (Yes/No)	Proposed Solution and Product Reference
1.	Make	<to be provided by the bidder>	
2.	Model	<to be provided by the bidder>	
3.	MSI shall clearly specify the placement of the detector (upstream, downstream, stop-line, exit etc.) for independent straight and right turn signals.		
4.	The detector shall be able to count vehicles in non-lane based mixed traffic flow conditions. The accuracy of counts shall be bigger than 90% over all light and weather conditions. The contractor shall clearly specify how this is accomplished.		
5.	MSI shall give an estimate of the total number of vehicle presence detection zones and vehicle detectors required and the type of detection system recommended.		
6.	A detector that does not change its status at least once during a stage execution shall be notified to the Central Computer (in ATCS mode) at the termination of the associated stage.		

4.4.1.1.3 Functional Requirement -Countdown Timer

Countdown Timer shall be installed at each traffic junction under ITMS & City Surveillance System Project.

#	Description	Bidder Compliance (Yes/No)	Proposed Solution and Product Reference
1.	Make	<to be provided by the bidder>	
2.	Model	<to be provided by the bidder>	
3.	Count Down Timer to be configured in Vehicular Mode.		
4.	The Vehicular countdown timer should be dual color,; Red for Stop or STP and Green color for Go		
5.	There should be alternate Red and Balance phase time for STOP or STP in Flashing		
6.	Alternate Green and Balance Phase Time for Go in Flashing		

4.4.1.1.4 Functional Requirement -Communication Network

Function of the Communication network is for remote monitoring of the intersection and its management. Real time data (like RTC time, stage timing, mode, events, etc.) from the traffic signal controller is required to be sent to the Central Computer in CCCC. Central Computer running the ATCS application shall calculate and send optimum signal timings to all intersections in the corridor. MSI shall clearly specify the bandwidth requirements and the type of network recommended for the ATCS.

The contractor shall specify the networking hardware requirements at the CCCC and remote intersections for establishing the communication network.

4.4.1.1.5 Functional Requirement - ATCS Software Application

Objective of the ATCS is to minimize the stops and delays in a road network to decrease the travel time with the help of state-of-the-art technology. The adaptive traffic control system shall operate in real time with the capacity to calculate the optimal cycle times, effective green time ratios, and change intervals for all system traffic signal controllers connected to it. These calculations will be based up on assessments carried out by the ATCS application software running on a Central Computer based on the data and information gathered by vehicle detectors at strategic locations at the intersections controlled by the system.

The ATCS application software shall do the following:

#	Description	Bidder Compliance (Yes/No)	Proposed Solution and Product Reference
1.	Make	<to be provided by the bidder>	
2.	Model	<to be provided by the bidder>	
3.	Identify the critical junction of a corridor or a region based on maximum traffic demand and saturation.		
4.	The critical junction cycle time shall be used as the group cycle time i.e. cycle time common to all intersection in that corridor or region.		
5.	Stage optimization to the best level of service shall be carried out based on the traffic demand.		
6.	Cycle optimization shall be carried out by increasing or decreasing the common corridor cycle time based on the traffic demand within the constraints of Minimum and Maximum designed value of cycle time.		
7.	Offset correction shall be carried out to minimize number of stops and delays along the corridor for the priority route. Offset deviation measured using distance and speed between successive intersections shall be corrected within 5 cycles at a tolerance of +/- 5 seconds maximum.		
8.	The system shall have provision to configure priority for upstream signals as default. The ATCS software shall continuously check the traffic demand for upstream and downstream traffic and automatically assign the priority route to the higher demand direction.		
9.	Develop appropriate stage timing plans for each approach of every intersection under the ATCS, based on real time demand		
10.	Propose timing plans to every intersection under the ATCS in every Cycle		
11.	Verify the effectiveness of the proposed timing plans in every cycle		
12.	Identify Priority routes		
13.	Synchronize traffic in the Priority routes		
14.	Manage and maintain communication with traffic signal controllers under ATCS		
15.	Maintain database for time plan execution and system performance		
16.	Maintain error logs and system logs		
17.	Generate Reports on request		

#	Description	Bidder Compliance (Yes/No)	Proposed Solution and Product Reference
18.	Graphically present signal plan execution and traffic flow at the intersection on desktop		
19.	Graphically present time-space diagram for selected corridors on desktop		
20.	Graphically present network status on desktop		
21.	Make available the network status and report viewing on Web		
22.	The ATCS shall generate standard and custom reports for planning and analysis		
23.	It shall be possible to interface the ATCS with a popular microscopic traffic flow simulation software for pre and post implementation analysis and study of the proposed ATCS control strategy		
24.	Shall have the ability to predict, forecast and smartly manage the traffic pattern across the signals over the next few minutes, hours or 3-5 days and just in the current real time.		
25.	Shall provide a decision support tool for assessing strategies to minimize congestion, delays and emergency response time to events via simulation and planning tools liked with real time traffic data fusion and control of traffic signaling infrastructure on ground.		
26.	Shall collect continuously information about current observed traffic conditions from a variety of data sources and of different kind (traffic states, signal states, vehicle trajectories, incidents, road works, etc.).		
27.	Shall infer a coherent and comprehensive observed traffic state (speeds, vehicular densities, and presence of queues) on all network elements, from abovementioned observations, including vehicle trajectories, through a number of map matching, data validation, harmonization and fusion processes).		
28.	Shall extend the measurements made on only a number of elements both on the rest of the unmonitored network, and over time, thus obtaining an estimation of the traffic state of the complete network and the evolution of this traffic state in the future.		

#	Description	Bidder Compliance (Yes/No)	Proposed Solution and Product Reference
29.	Shall forecast the traffic state with respect to current incidents and traffic management strategies (e.g. traffic signal control or variable message signs), improving the decision making capabilities of the operators even before problems occur.		
30.	Shall calculate customizable Key Performance Indicators (KPI) to quickly assess the results		
31.	Shall provide calculated traffic flows estimation and forecast, queues and delays to Urban Control and Adaptive Signal Control Systems, allowing for proactive Traffic Management and Control		
32.	Shall generate alerts to the operator that trigger on customizable conditions in the network (starting with simple drops in flow, up to total queue lengths along emission sensitive roads surpassing a definable threshold)		
33.	Shall distribute both collected and calculated traffic information via a variety of communication protocols and channels, ensuring high interoperability degree and thus acting as a "traffic data and information hub"		
34.	Shall create a traffic data warehouse for all historic traffic information gathered from the hardware installed on the road network.		
35.	Shall operate in real time that is continuously updating the estimates on the state of the network and the travel times on the basis of data collected continuously over time.		
36.	Shall operate the traffic lights with the adaptive traffic controls, based on the current and forecasted traffic demand and the current incidents, thus optimizing the green waves continuously throughout the network		
37.	Enable a smart public transport priority respecting the delays for all road users at once with the adaptive signal controller		
38.	Reports: a. Intersection based reports ✓ 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		

#	Description	Bidder Compliance (Yes/No)	Proposed Solution and Product Reference
	stages of all cycles for a day. The saturation is defined as the ratio between the available stage timings to the actual stage timing executed by the traffic signal controller for the stage (stage preemption time). ✓ Cycle Timing report – The report shall give details of time at which every cycle has taken place. The report shall show the cycle sequence and cycle timings for all the cycles in a day. ✓ 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. The report shall show the cycle sequence and cycle timings for the cycle in a day. ✓ 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. ✓ Intensity Change – The report shall show the brightness of the signal lamp is changed according to the light intensity either manually through keypad or automatically by LDR with time stamp. ✓ Plan Change – The report shall show the time of change of plan either through keypad or remotely through a PC or Server.		

#	Description	Bidder Compliance (Yes/No)	Proposed Solution and Product Reference
	✓ RTC Failure – The report shall show the time when RTC battery level goes below the threshold value. ✓ Time Update – The report shall show the time when the Master controller updated its time either manually through keypad, automatically by GPS or through remote server. ✓ Mode Change – The report shall show the time when Master controller's operating mode is changed either manually through keypad or a remote server. The typical modes are FIXED, FULL VA SPLIT, FULL VA CYCLE, FLASH, LAMP OFF and HURRY CALL. ✓ Lamp Status Report – The report shall show lamp failure report with date and time of failure, colour of the lamp and associated phase. ✓ Loop 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. b. Corridor Performance Report – The report shall show the saturation of all the intersections in a corridor for every cycle executed for the corridor and the average corridor saturation for a day c. Corridor Cycle Time Report – The report shall show the Corridor cycle time, Intersection cycle time, Mode of operation and degree of saturation of all the intersections in a corridor for every cycle for a day.		
39.	Graphical User Interface - The application software shall have the following Graphical User Interface (GUI) for user friendliness. ✓ User login – Operator authentication shall be verified at this screen with login name and password		

#	Description	Bidder Compliance (Yes/No)	Proposed Solution and Product Reference
	✓ 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. ✓ 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. ✓ Junction names shall be identified with each plot. ✓ Facility shall be available to plot the time-space diagram from history. ✓ Currently running stage and completed stages shall be identified with different colours. ✓ Stages identified for synchronization shall be shown in a different colour. ✓ Speed lines shall be plotter for stages identified for synchronization to the nearest intersection in both directions. ✓ It should be possible to freeze and resume online plotting of Time-Space diagram. ✓ The system shall have other graphical interfaces for configuring the ATCS, as appropriate.		

4.4.1.2 Technical Specifications - Adaptive Traffic Control System

4.4.1.2.1 Adaptive Traffic Control- Traffic Sensor

Appropriate camera based traffic sensors may be chosen to provide the operational levels and accuracy as required for successful function of the ATCS system as per the SLAs defined.

4.4.1.2.2 Adaptive Traffic Control- Traffic Controller

Appropriate controller technology may be chosen to provide the operational levels and accuracy as required for successful function of the ATCS system as per the SLAs defined. The proposed traffic controller shall be disabled friendly and shall also provide audio tones output.

4.4.1.2.3 Adaptive Traffic Control- Traffic Lights

#	Minimum required specifications	Bidder Compliance (Yes/No)	Proposed Solution and Product Reference
1.	Make	<to be provided by the bidder>	
2.	Model	<to be provided by the bidder>	
3.	Key Features: a. lowest power consumption for all colors b. Meets or exceeds intensity, colour and uniformity specifications c. Temperature compensated power supplies for longer LED life d. Uniform appearance light diffusing e. Should be Intertek/ETL/EN certified f. All units operate at voltage of 230Vac +/- g. 10% and frequency 50 +/-5Hz h. LED shall be single source narrow beam type with clear lens & Luminance uniformity of 1:15 i. Pedestrian traffic lights should be j. provided with clearly audible signals for the benefit of pedestrians with visual impairments k. Phantom Class 5 or equivalent. IP Rating: IP65		
4.	LED aspects: a. Red, Amber, Green-Full (300 mm b. diameter) : Hi Flux c. Green-arrow (300 mm diameter): Hi flux d. c. Animated Pedestrian-Red and Green Animated c/w countdown (300 mm) Hi Brite with diffusions		
5.	LED Retrofit Specifications:		

#	Minimum required specifications	Bidder Compliance (Yes/No)	Proposed Solution and Product Reference
	a. Power supply:230 Vac +/- 10% and frequency 50+/-5Hz b. Standards: EN 12368 certified c. Convex Tinted Lens: Available d. Fuse and Transients: Available e. Operating Temperature Range: 0 degree Celsius to 55 degree Celsius Turn Off/Turn On Time: 75 milliseconds max f. Total Harmonic Distortion: <20% g. Electromagnetic interference: Meets FCC Title 47,Subpart B, Section 15 Regulation or equivalent EN/IRC standard h. Blowing Rain/Dust Spec: MIL 810F or Equivalent EN/IRC standard complaint i. Minimum Luminous Intensity (measured at intensity point)(cd): Red 400 Amber 400 Green 400 j. Dominant Wavelength (nm): Red 630 Amber 590 Green 490 k. Lamp conflict compatibility system: Compatible with lamp failure and conflict detection		

4.4.1.2.4 Adaptive Traffic Control- Countdown Timer

#	Parameter	Minimum required specifications	Bidder Compliance (Yes/No)	Product Reference
1.	Make	<to be provided by the bidder>		
2.	Model	<to be provided by the bidder>		
3.	CPU	Micro Controller		
4.	Mechanical Specifications			
a.	Structural Material	Polycarbonate strengthened against UV rays		
b.	Body Color	Light Grey/Black		
c.	Dimensions	360mm x 370mm x 220mm		
5.	Display Specification			
a.	Lamp Diameter	300mm		
b.	Digit Height	150 -165mm		
c.	Display Type	Dual Coloured (Red & Green)		

#	Parameter	Minimum required specifications	Bidder Compliance (Yes/No)	Product Reference
d.	No. of Digit	3		
6.	LED Specifications			
a.	LED Diameter	5mm LED		
b.	Viewing Angle	30°		
c.	LED Wave Length	630-640nm (Red), 505nm - 520nm (Blue-Green)		
d.	LED Dice Material	AIInGap (Red), InGaN (Blue-Green)		
e.	LED Warranty period	5 years		
7.	Technical Features			
8.	Power Consumption	20 - 30 Watt Per Lamp		
9.	Input Power	85-260V AC, 50Hz		
10.	Operating Temperature	-20 to + 60 °C		
11.	Humidity	0% to 95% Relative Humidity		
12.	Water & Dust Ingress	IP65		
13.	Standard	En12966		

4.4.1.2.5 Poles for Traffic Signals

#	Minimum required specifications	Bidder Compliance (Yes/No)	Product Reference
1.	Make	<to be provided by the bidder>	
2.	Model	<to be provided by the bidder>	
3.	Material: GI Class 'B' pipe		
4.	Paint: Pole painted with two coats of zinc chromate primer and two coats of golden yellow Asian apostolate paint or otherwise as required by architect and in addition bituminous painting for the bottom 1.5 m portion of pole.		

4.4.1.2.6 Cables for Traffic Signals

#	Minimum required specifications	Bidder Compliance (Yes/No)	Product Reference
1.	Make	<to be provided by the bidder>	
2.	Model	<to be provided by the bidder>	
3.	No's of cores: 7 and 14 core 1.5 sq. mm.; 3 Core 2.5 sq. mm.		

#	Minimum required specifications	Bidder Compliance (Yes/No)	Product Reference
4.	Materials: PVC insulated and PVC sheathed armored cable with copper conductor of suitable size.		
5.	Certification: ISI Marked		
6.	Standards: Indian Electricity Act and Rules		
7.	IS:1554 - PVC insulated electric cables (heavy duty)		

4.4.2   Surveillance System

MSI has to supply, install, commission and maintain the required number of camera in the location as mentioned in Annexure. MSI has to provision for poles, switch, UPS and other equipment for installing the camera. The MSI should do necessary cabling for electrical supply and connectivity required for the field devices. MSI will also implement the following software to enable monitoring through the surveillance cameras; Video Management System (VMS) and Video Analytics System.

4.4.2.1   Functional Requirement - Surveillance System

#	Minimum required specifications	Bidder Compliance (Yes/No)	Proposed Solution and Product Reference
1.	Make	<to be provided by the bidder>	
2.	Model	<to be provided by the bidder>	
3.	Video Management System shall be used for centralized management of all field devices, servers and client users.		
4.	VMS shall support a flexible rule-based system driven by schedules and events.		
5.	VMS shall be supported for fully distributed solution for monitoring and control function, designed for limitless multi-site and multiple server installations requiring 24/7 surveillance with, support for devices from different vendors.		
6.	VMS shall support IP cameras from major vendors.		
7.	System should support LDAP (Lightweight Directory Access Protocol) server		
8.	VMS shall be enabled for any standard storage technologies and video wall system integration.		
9.	VMS shall be enabled for integration with any external Video Analytics Systems.		

#	Minimum required specifications	Bidder Compliance (Yes/No)	Proposed Solution and Product Reference
10.	VMS shall be capable of being deployed in a virtualized environment without loss of any functionality.		
11.	VMS server shall be deployed in a clustered server environment for high availability and failover.		
12.	All CCTV cameras locations shall be overlaid in graphical map in the VMS Graphical User Interface (GUI). The cameras selection for viewing shall be possible via clicking in the camera location on the graphical map. The graphical map shall be of high resolution enabling operator to zoom-in for specific location while selecting a camera for viewing.		
13.	The VMS shall have an administrator interface to set system parameters, manage codecs, manage permissions and manage storage.		
14.	VMS day to day control of cameras and monitoring on client workstations shall be controlled through the administrator interface.		
15.	Whilst live control and monitoring is the primary activity of the Operator workstations, video replay shall also be accommodated on the GUI for general review and also for pre and post alarm recording display.		
16.	Solution design for the VMS shall provide flexible video signal compression, display, storage and retrieval.		
17.	All CCTV camera video signal inputs to the system shall be provided to Command Control and Communication Centre, and the transmission medium used shall best suit the relative camera deployments and access to the CCTV Network.		
18.	VMS shall be capable of transferring recorded images to recordable media (such as CD/DVD and/or DAT tapes) in tamper evident and auditable form.		
19.	All the streams shall be available in real-time (expecting the network latency) and at full resolution. Resolution and other related parameters shall be configurable by the administrator in order to provide for network constraints.		
20.	VMS shall support field sensor settings.		

#	Minimum required specifications	Bidder Compliance (Yes/No)	Proposed Solution and Product Reference
21.	VMS shall support the following minimum operations: ▪ Adding an IP device ▪ Updating an IP device ▪ Updating basic device parameters ▪ Adding\Removing channels ▪ Adding\Removing output signals ▪ Updating an IP channel ▪ Removing an IP device ▪ Enabling\Disabling an IP channel ▪ Refreshing an IP device (in case of firmware upgrade)		
22.	VMS shall support retrieving data from edge storage. Thus when a lost or broken connection is restored, it shall be possible to retrieve the video from SD card and store it on central storage.		
23.	VMS shall support bookmarking the videos. Thus, allowing the users to mark incidents on live and/or playback video streams.		
24.	VMS shall allow the administrator to distribute camera load across multiple recorders and be able shift the cameras from one recorder.		
25.	VMS shall support automatic failover for recording.		
26.	VMS shall support manual failover for maintenance purpose.		
27.	VMS shall support access and view of cameras and views on a smartphone or a tablet (a mobile device).		
28.	VMS shall support integration with the ANPR application.		
29.	VMS shall support integration with other online and offline video analytic applications.		
30.	CCTV Camera Management – Shall enables management of cameras associated with the VMS.		
31.	Video recording, retrieval and archiving – Shall manages live camera viewing, recording of live feeds for future review, search and retrieval of recorded feeds and archiving of recorded video feeds for optimum utilization of resources.		
32.	Video Analytics (VA) alert management – Shall enable defining of rules for handling of alerts		

#	Minimum required specifications	Bidder Compliance (Yes/No)	Proposed Solution and Product Reference
	using the VA handling of events as per the defined rules.		
33.	MIS and Reporting – Shall provide users with business analytics reporting and tools to organize evaluate and efficiently perform day to day operations.		
34.	Security and Roles – Shall manages role definitions for internal as well as external access.		
35.	VMS shall be Codec and IP camera agnostic such that it can support devices that are not supplied by the manufacturer/developer of the VMS software and Codec hardware.		
36.	All cameras locations shall be overlaid in graphical map in Graphical User Interface (GUI). The cameras selection for viewing shall be possible via clicking in the camera location on the graphical map. The graphical map shall be of high resolution enabling operator to zoom-in for specific location while selecting camera for viewing.		
37.	VMS shall support tamper detection for all cameras to warn of accidental or deliberate acts that disable the surveillance capability.		
38.	For alarm interfacing requirements, The designated primary camera shall be automatically displayed as a main GUI CCTV screen. The VMS shall also, on alarm, present associated pre/post event video allowing the Operator to assess the alarm cause. Other associated cameras, when called up, shall be displayed as split-screen images on the other monitor of the operator workstation.		
39.	Playback of any alarm related video, (including pre and post alarm video) shall start at the beginning or indexed part alarm sequence.		
40.	Video management software incorporates online video analytics on live video images. It shall include the following video analytics detection tools: ▪ Presence detection for moving and stopped vehicles ▪ Directional sensitive presence detection ▪ Congestion Detection ▪ Loitering detection		

#	Minimum required specifications	Bidder Compliance (Yes/No)	Proposed Solution and Product Reference
	▪ Improper Parking ▪ Camera Tampering ▪ Abandoned objects detection		
41.	System needs to have the capability to deploy intelligent video analytics software on any of selected cameras. This software should have the capability to provide various alarms & triggers. The solution should offer following triggers from Day1: ✓ Parking Violation ✓ Wrong Direction ✓ People loitering ✓ Camera Tampering (In case this is an inherent feature of the camera, this may not be provided as a separate line item in VA) ✓ Unattended Object ✓ Crowd detection ✓ Traffic flow/Congestion ✓ Traffic Volume estimation and statistical counts ✓ People tracking		
42.	VA should be equipped with motion detection component that automatically detects moving objects in the field of view of a camera, and is capable of filtering out movement in configurable directions and movement due to camera motion (e.g. from wind)		
43.	Video clips of specific events via the VA or by the operator action shall be capable of being separately stored and offloaded by operator with appropriate permissions on to recordable media		
44.	System shall provide the capability to select duration and resolution of storage by camera, time and activity event and user request. Frequency/trigger of transfer shall be configurable by user.		
45.	Live video viewing: The system shall allow the viewing of live video from any camera on the system at the highest rate of resolution and frame rate that the camera shall support on any workstation on the network.		
46.	Recorded video viewing: The system shall allow the viewing of recorded video from any		

#	Minimum required specifications	Bidder Compliance (Yes/No)	Proposed Solution and Product Reference
	camera on the system at whatever rate the camera was recorded.		
47.	The system shall provide the capability to manage the video storage to allow selective deletions, backups, and auto aging.		
48.	VMS shall have an extensive reporting capability with ability for administrator to define reports in a user friendly manner.		
49.	The user interface shall be via a GUI providing multiple video streams simultaneously on multiple monitors.		
50.	The GUI shall have the minimum capability of naming locations, users, and cameras events be displayed correctly on users screen.		
51.	The system shall have the capability to store and record operator specific options.		
52.	The GUI shall conform to standard Windows conventions.		
53.	The system shall provide unified GUI camera control at an operator's workstation for all types of cameras installed whether existing or new or connected via another agency.		
54.	Unified control of the following functions shall be provided: ▪ Selection ▪ Display ▪ PTZ ▪ Setup and adjustment ▪ Determination of pre-sets		
55.	**SMS Gateway Integration** MSI shall carry out SMS Gateway Integration with the Surveillance System and develop necessary applications to send mass SMSs to groups/individuals, which can be either manual or system generated. Any external/third party SMS gateway can be used, but this needs to be specified in the Technical Bid, and approved during Bid evaluation.		
56.	All user interfaces shall support English language and shall confirm to standard Windows protocols and practices and allow the control of all functions via a simple easy to use interface.		
57.	The system shall support a mode of operation whereby a map of all or part of the map (at		

#	Minimum required specifications	Bidder Compliance (Yes/No)	Proposed Solution and Product Reference
	operator request) is displayed on a separate or same screen and that status information can be provided via an icon, and access to any cameras shall be accessible by means of an icon on that screen.		
58.	These Maps shall be defined so that an operator may make a selection from the same source of mapping that is available to the other systems within the Command and Control Centre suite of systems displaying whichever Map or section the operator needs, and it shall be displayed within one (1) second.		
59.	The System should support Maps integration in future with below features; ▪ Adding Image Layers to the location map. ▪ Define the location map for each location. ▪ Add cameras to the map images. ▪ Add image layers to the map. ▪ Add a Maps Server ▪ System should support raster format images of jpeg/jpg and png file and Vector (shape files)		
60.	The VMS configuration tool shall define: ▪ Cameras (whether via codec units or directly connected IP cameras) and text based names ▪ Camera Groups ▪ User Groups ▪ Monitors ▪ Codec parameters ▪ Alarms ▪ Workstations ▪ Storage		
61.	The configuration utility shall allow the system administrator to: ▪ Install new devices ▪ Configure all aspects of existing devices ▪ Configure and set up users/user groups and their rights/permissions/priorities ▪ To define multiple camera groups ▪ Each group to be defined for combinations of viewing and control rights ▪ Individual Operators to be assigned multiple groups		

#	Minimum required specifications	Bidder Compliance (Yes/No)	Proposed Solution and Product Reference
	▪ Each group to be allocated to multiple Operators ▪ Each camera may be in multiple groups ▪ Program camera/monitor selection and configuration of the video wall(s) in response to an incoming alarm		
62.	User permissions/privileges, to be allocated, shall extend from full administrator rights down to basic operation of the system, and shall include the ability to designate workstations to an operator, and to designate one or more camera groups to an operator for viewing and/or control.		
63.	The configuration utility shall store all changes to the system,		
64.	A copy of the system configuration shall be stored external to the system to allow system restoration in case of hardware failure. External would mean another site, to be agreed with RSCCL during detail design.		
65.	The (MSI) shall request a detailed User Prioritization List (UPL) from the RSCCL during the project. The UPL shall enable the programming of the CCTV management system with the agreed user prioritization.		
66.	Over and above user priority, users shall be enabled for the following in varying combinations: ▪ Image viewing ▪ Image recording ▪ PTZ control		
67.	PTZ Control: ▪ All PTZ control shall be user-restricted. ▪ Users shall be able to simultaneously pan and tilt a PTZ camera displayed in a video pane in any direction and at varying speed by moving the PC mouse on the video pane. ▪ Users shall be able to zoom a PTZ camera in or out using the PC mouse. ▪ Users shall be able to simultaneously pan, tilt and zoom a PTZ camera displayed in a video pane or monitor using a joy stick on one of the supported CCTV keyboards.		

#	Minimum required specifications	Bidder Compliance (Yes/No)	Proposed Solution and Product Reference
	▪ Users shall be able to adjust the focus of a PTZ camera using the on screen PTZ controls or a CCTV keyboard: ▪ Focus near ▪ Focus far ▪ Auto-focus ▪ Users shall be able to adjust the iris of a PTZ camera using the on screen PTZ controls or a CCTV keyboard: Open iris-Close-Auto-iris. ▪ Users shall be able to move a PTZ camera to a preset position using the on screen PTZ controls or a CCTV keyboard. ▪ Users shall be able to perform a custom command on a PTZ camera using the on screen PTZ controls (e.g. operate wipers.). ▪ Users shall be able to enter the menu on a PTZ camera using the on screen PTZ controls or a CCTV keyboard (menu options navigated using pan and tilt.). ▪ Users shall be able to hold onto connections to PTZ cameras to prevent other users taking control if not moved (overrides the 5 second timeout). ▪ Users shall be able to take control of a PTZ camera if user has a higher priority than the user currently moving it (overrides PTZ hold.). ▪ Inform user when can't take control of a PTZ camera because another user with a higher priority is controlling it. ▪ Users shall be able to show or hide the on screen PTZ controls. ▪ The Video Management System shall support the following for cameras using the ONVIF interface or Camera Gateway: ○ Pan, tilt and zoom control with mouse and joystick ○ Go to preset ○ Set preset		
68.	Audio in Live Video: ▪ Users shall be able to listen to audio from multiple cameras through PC speakers ▪ Users shall be able to speak to one or more cameras through a PC microphone		

#	Minimum required specifications	Bidder Compliance (Yes/No)	Proposed Solution and Product Reference
	▪ Users shall be able to listen to audio from a camera through monitor's speakers ▪ Users shall be able to speak to a camera displayed on monitor through a microphone connected to a decoder ▪ Users shall be able to mute a client speaker ▪ The Video Management System shall have an option to allow or prevent simultaneous listen and speak (full duplex audio). If full duplex audio is off, the direction of audio will be switched automatically when the user listens or speaks ▪ • Users shall be able to listen to audio streams that do not have associated video.		
69.	The system shall accommodate the definition and implementation of adequate priority levels or equivalent feature		
70.	All images shall be recorded centrally as a background process at configurable parameters.		
71.	It shall not be possible to interrupt, stop, delay or interfere with the recording streams in any way, without the appropriate user rights.		
72.	The CCTV recording system shall enable pre and post event (PPE) recording, presentation and storage, initiated automatically in response to system alarm sources received by the VMS.		
73.	The PPE recording clips shall be provided by the VMS and retrieved from the central video archive on the buffer storage system.		
74.	The information stored shall be full real-time and full resolution from each incoming camera channel. In the absence of a trigger from a manual input or from a programmed alarm source, the PPE video recording shall be written to buffer storage on a FIFO basis.		
75.	In the event of a trigger, the VMS shall ensure that the programmed sections of pre and post event video are immediately presented to the Operator to complement the alarm display and simultaneously saved as an identified indexed video clip, complete with time/date stamp, in a reserved and protected area of the storage		

#	Minimum required specifications	Bidder Compliance (Yes/No)	Proposed Solution and Product Reference
	system. Such PPE recording shall then be capable of later retrieval via search criteria.		
76.	Once tagged and saved, the PPE video clip shall NOT be overwritten except by an operator with the required permissions i.e. it is excluded from the normal FIFO regime of the bulk storage system. Recording shall also be initiated on-demand by manual triggers from system operators e.g. keyboard key-stoke.		
77.	The VMS shall support the following recording modes: a. Total recording –VMS shall allow for continuous recording of all video inputs b. Event based recording –VMS shall record the video input only in case an event has occurred		
78.	VMS shall support the following triggers to initiate a recording ▪ Scheduler – the recorder will record the video inputs based on a specified schedule. ▪ VMS shall allow recording based on a time schedule for all or some of the video channels ▪ VMS shall allow for multiple recording periods per day, per channel ▪ VMS shall have the option to set any available trigger in the system (VMD/TTL/Soft Trigger and/or API) to trigger the channel ▪ VMS shall have the option for individual channel setup of pre/post-alarm recording for defined interval ▪ VMS shall have the ability to enable/disable triggers through a daily time schedule ▪ Manual – the user shall be able to initiate a manual recording upon request. ▪ VMS shall work in conjunction to the any previous alarm operations ▪ VMS shall allow API Triggers ▪ All trigger information shall be stored with the video information in the VMS data set and shall be made available for video search		

#	Minimum required specifications	Bidder Compliance (Yes/No)	Proposed Solution and Product Reference
79.	VMS recording and replay management systems shall support the following features and operations: ▪ Play back shall not interfere with recording in any way ▪ Support either analogue cameras connected via Codecs or IP-cameras directly connected to the network ▪ Stream live images through the network using IP Multi-cast techniques ▪ Store the recording stream from all cameras simultaneously with no degradation to any ▪ individual camera recorded image stream unless the system is configured by administrator to allow for change in quality ▪ Deliver live video to VMS workstation within a period of one second from manual call up ▪ Deliver live video to VMS workstation within a period of three seconds from automatic alarm receipt on alarm interface ▪ Storage of each camera's images at a rate and resolution as defined in the Codec or IP camera configuration. The system VMS programming shall automatically vary these rates in response to time profiles, alarm inputs ▪ Support streaming of recorded files using IP Unicast directly to hardware decoders for display on analogue monitors or software decoder when/if required ▪ Playback multiple, synchronized recorded streams at differing speeds and frame rates ▪ playback a video stream simultaneously at differing speeds and frame rates ▪ Time stamping of every recorded video field based upon Network Time Protocol (NTP) time ▪ Selectable on-screen-display of time and camera title during playback ▪ Configurable granularity of video files ▪ Generate alarm when storage medium has fallen below a user selectable threshold		

#	Minimum required specifications	Bidder Compliance (Yes/No)	Proposed Solution and Product Reference
	▪ Stored video files can be "down-loaded" to the systems and then directly CD ROM and/or ▪ DVD or WORM for replay using the VMS video replay application, and shall incorporate ▪ proof of authenticity ▪ ⬜ Download video records in common (e.g. AVI) file format for remote, cursory review and assessment prior to generating tamper-evident auditable copies		
80.	Video alarm handling shall provide the following facilities for the handling and management of video images generated by alarms associated with other systems integrated with the VMS.		
81.	VMS shall also accommodate operator-initiated recording of a given cameras.		
82.	VMS shall be integrated within a consolidated GUI that would include other Command and Control Centre systems as well. All events, activations and alarms that occur with the VMS and its sub systems will: ▪ Interact seamlessly between the Command and Control Centre sub systems as required shall be sent and Open Source Programming Console3 (OPC1) interface or using Software Development Kit (SDK)		
83.	VMS shall enable handling of 200 cameras, on day one, as well as future scalability up-to 2000 cameras as may be required.		
84.	VMS Interfaces to Other Geographic Information System (GIS) – ▪ Camera definitions that would be overlaid on GIS map ▪ Camera Map and locations		
85.	VMS shall have the capability to utilize unified storage server configurations, in any combination, and shall support a dual redundant system enabling instant control to the standby (slave) server in the event of the main server failure.		
86.	Software to manage the dual redundant modes shall be located in the DC at Command and Control Centre and shall monitor the main		

#	Minimum required specifications	Bidder Compliance (Yes/No)	Proposed Solution and Product Reference
	(master) server and its parameters. It shall also judge the health of the recording system elements (unified storage) by maintaining and monitoring a database of the status of relevant server parameters.		
87.	Software shall also determine when to switch a drive, should a drive or server failure be detected, in order to maintain the integrity of recording of images. This change-over shall be fully automatic but the system shall signal a failure warning to designated Operator workstations or within the GIS (or equivalent) to allow rectification to be initiated.		
88.	Software that manages the server conditions shall either be part of the VMS (i.e. a module) or independent but integrated within the VMS itself, if provided separately.		
89.	VMS shall provide the capability to configure, monitor and diagnose all CCTV hardware including cameras and encoders. This will include real time errors and warnings generation on operator console.		
90.	VMS shall have the capability to utilize unified storage server configurations, in any combination, and shall support a dual redundant system enabling instant control to the standby (slave) server in the event of the main server failure.		
91.	Software to manage the dual redundant modes shall be located in the DC at Command Control and Communication Centre and shall monitor the main (master) server and its parameters. It shall also judge the health of the recording system elements (unified storage) by maintaining and monitoring a database of the status of relevant server parameters.		
92.	Software shall also determine when to switch a drive, should a drive or server failure be detected, in order to maintain the integrity of recording of images. This change-over shall be fully automatic but the system shall signal a failure warning to designated Operator workstations or within		

#	Minimum required specifications	Bidder Compliance (Yes/No)	Proposed Solution and Product Reference
	the GIS (or equivalent) to allow rectification to be initiated.		
93.	VMS shall feature a diagnostics package that provides operation and maintenance personnel with a single interface to review all VMS operating parameters, failure messages and system alarms.		
94.	The system shall support and be configured to send SNMP (Simple Network Management Protocol) traps that may be monitored to enable a centralized first line support service. VMS shall support minimum SNMP.		
95.	The diagnostics package shall allow for easy system fault analysis in the event of loss of video, system control or network failure.		
96.	System shall also provide the ability to log all operational functions for future investigations and reports. System shall be fully configurable allowing a selection of parameters that can be optionally logged. Both pre-defined and custom reports shall be available for generation from all system logs and then optionally exported to standard Windows format programs.		
97.	VMS systems shall be provided with a method of backing up their software and data bases such that the system can be rebuilt in its entirety from these stored components. This shall be via a specific purpose device and not that used below for the video archiving.		
98.	System shall also be provided with a method of imaging each server and workstation so as to allow a convenient fast restore shall be required. The mechanism shall be shared with the backup device outlined above but not the devices used for video archiving.		
99.	A wide array of video analytics shall be deployed based on efficacy of the analytics on-field and their need in Ranchi. The minimal functionality expected includes: ▪ Presence detection for moving and stopped vehicles ▪ Directional sensitive presence detection ▪ Congestion Detection ▪ Loitering detection		

#	Minimum required specifications	Bidder Compliance (Yes/No)	Proposed Solution and Product Reference
	▪ Improper Parking ▪ Camera Tampering ▪ Abandoned objects detection All cameras should support motion detection, camera tampering.		

4.4.2.2 Outdoor/Fixed Box cameras (High Definition)

#	Parameter	Minimum Specifications	Bidder Compliance (Y/N)	Product and Documentation Reference
1.	Make		<to be provided by the bidder>	
2.	Model		<to be provided by the bidder>	
3.	Video Compression	H.264 or better		
4.	Video Resolution	1920 X 1080		
5.	Frame rate	Min. 25 fps		
6.	Image Sensor	1/3" Progressive Scan CCD / CMOS		
7.	Lens Type	Varifocal, C/CS Mount, IR Correction		
8.	Lens#	Auto IRIS 8 – 50 mm, F1.4		
9.	Minimum Illumination	Colour: 0.5 lux, B/W: 0.1 lux (at 30 IRE)		
10.	IR Cut Filter	Automatically Removable IR-cut filter		
11.	Day/Night Mode	Colour, Mono, Auto		
12.	S/N Ratio	≥ 50 Db		
13.	Auto adjustment + Remote Control of Image settings	Colour, brightness, sharpness, contrast, white balance, exposure control, backlight compensation, Gain Control, Wide Dynamic Range		
14.	Audio	Audio Capture Capability		
15.	Local storage	Minimum 64 GB Memory card in a Memory card slot		
16.	Protocol	IPV4, IPV6, HTTP, HTTPS, FTP, RTSP, RTP,		

#	Parameter	Minimum Specifications	Bidder Compliance (Y/N)	Product and Documentation Reference
		TCP, UDP, RTCP, DHCP, UPnP, QoS		
17.	Security	Password Protection, IP Address filtering, User Access Log, HTTPS encryption		
18.	Operating conditions	0 to 50°C (temperature), 50 to 90% (humidity)		
19.	Casing	NEMA 4X / IP-66 rated		
20.	Certification	UL/EN, CE,FCC		
21.	Field of View	Shall have at least 70 degrees field of view (horizontal)		

4.4.2.3   Pan, Tilt and Zoom cameras (PTZ)

#	Parameter	Minimum Specifications	Bidder Compliance (Y/N)	Product and Documentation Reference
1.	Make		<to be provided by the bidder>	
2.	Model		<to be provided by the bidder>	
3.	Video Compression	H.264 or better		
4.	Video Resolution	1920 X 1080		
5.	Frame rate	Min. 25 fps		
6.	Image Sensor	1/3" Progressive Scan CCD / CMOS		
7.	Lens#	Auto-focus, 4.7 - 94 mm (corresponding to 20x)		
8.	Minimum Illumination	Colour: 0.5 lux, B/W: 0.1 lux (at 30 IRE)		
9.	IR Cut Filter	Automatically Removable IR-cut filter		
10.	Day/Night Mode	Colour, Mono, Auto		
11.	S/N Ratio	≥ 50 Db		
12.	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)		

#	Parameter	Minimum Specifications	Bidder Compliance (Y/N)	Product and Documentation Reference
		▪ 20x optical zoom and 10x digital zoom ▪ 64 preset positions ▪ Auto-Tracking ▪ Pre-set tour		
13.	Auto adjustment + Remote Control of Image settings	Colour, brightness, sharpness, contrast, white balance, exposure control, backlight compensation, Gain Control, Wide Dynamic Range		
14.	Local storage	Minimum 64 GB Memory card in a Memory card slot		
15.	Protocol	IPV4, IPV6, HTTP, HTTPS, FTP, RTSP, RTP, TCP, UDP, RTCP, DHCP, UPnP, QoS		
16.	Security	Password Protection, IP Address filtering, User Access Log, HTTPS encryption		
17.	Operating conditions	0 to 50°C (temperature), 50 to 90% (humidity)		
18.	Casing	NEMA 4X / IP-66 rated		
19.	Certification	UL/EN, CE,FCC		
20.	Field of view	Shall have at least 70 degrees field of view (horizontal)		

4.4.2.4   Infrared Illuminators

The infrared illuminators are to be used in conjunction with the Fixed Box cameras specified above to enhance the night vision.

#	Parameter	Minimum Specifications	Bidder Compliance (Y/N)	Product and Documentation Reference
1.	Make		<to be provided by the bidder>	
2.	Model		<to be provided by the bidder>	
3.	Range	Min. 100 meters, with adjustable angle to cover the complete field of view at specified locations		
4.	Minimum Illumination	High sensitivity at Zero Lux		
5.	Power	Automatic on/off operation		

6.	Casing	NEMA 4X / IP-66 rated		
7.	Operating conditions	-5° to 60°C		
8.	Certification	UL/EN/CE/FCC		

4.4.3 Automatic Number Plate Recognition (ANPR) System

4.4.3.1 Functional Requirement - ANPR

ANPR System shall enable monitoring of vehicle flow at strategic locations. The system shall support real-time detection of vehicles at the deployed locations, recording each vehicle, reading its number plate, database lookup from central server and triggering of alarms/alerts based on the vehicle status and category as specified by the database. The system usage shall be privilege driven using password authentication.

#	Description	Bidder Compliance (Yes/No)	Proposed Solution and Product documentation Reference
1.	Make	<to be provided by the bidder>	
2.	Model	<to be provided by the bidder>	
3.	The ANPR System shall enable monitoring of vehicle flow at strategic locations. The system shall support real-time detection of vehicles at the deployed locations, recording each vehicle, reading its number plate, database lookup from central server and triggering of alarms/alerts based on the vehicle status and category as specified by the database. The system usage shall be privilege driven using password authentication		
4.	Cameras shall cover single lanes of 3.5m each. For places where more than two lanes is to be monitored, the lane cameras to be increased in proportion to the lane.		
5.	The system shall have IR illuminators to provide illumination for night-time scenario. Camera with IR illuminators should be deployed at heights between 20 feet to allow HMV (high motor vehicle) to pass underneath it, and to minimize occlusion.		
6.	System should have the facility to provide the live feed of the camera at the command control and communication center or as per user requirement.		
7.	System should be able to provide video clips of the transaction from the ANPR lane cameras as evidence.		

#	Description	Bidder Compliance (Yes/No)	Proposed Solution and Product documentation Reference
8.	Vehicle Detection by Color ▪ The system shall detect the color of all vehicles in the camera view during daytime and label them as per the predefined list of configured system colors. The system will store the color information of each vehicle along with the license plate information for each transaction in the database. ▪ The system shall have options to search historical records for post event analysis by the vehicle color or the vehicle color with license plate and date time combinations		
9.	Alert Generation ▪ The system should have option to input certain license plates according to the hot listed categories like "Wanted", "Suspicious", "Stolen", etc. by authorized personnel. ▪ The system should be able to generate automatic alarms to alert the control room personnel for further action, in the event of detection of any vehicle falling in the hot listed categories.		
10.	Vehicle Status Alarm Module ▪ On successful recognition of the number plate, system should be able generate automatic alarm to alert the control room for vehicles which have been marked as "Wanted", "Suspicious", "Stolen", "Expired". (System should have provision/expansion option to add more categories for future need). ▪ The Instantaneous and automatic generation of alarms. In case of identity of vehicle in any category which is define by user. Vehicle Log Module		
11.	Vehicle Log Module ▪ The system shall enable easy and quick retrieval of snapshots, video and other data for post incident analysis and investigations. ▪ The system should be able to generate suitable MIS reports that will provide		

#	Description	Bidder Compliance (Yes/No)	Proposed Solution and Product documentation Reference
	meaningful data to concerned authorities and facilitate optimum utilization of resources. These reports shall include. ▪ Report of vehicle flow at each of the installed locations for Last Day, Last Week and Last Month. ▪ Report of vehicles in the detected categories at each of the installed locations for Last Day, Last Week and Last Month. ▪ Report of Vehicle Status change in different Vehicle Categories. ▪ The system shall have Search option to tune the reports based on license plate number, date and time, site location as per the need of the authorities. ▪ The system shall have option to save custom reports for subsequent use. The system shall have option to export report being viewed to common format for use outside of the ANPRS or exporting into other systems. ▪ The system should provide advanced and smart searching facility of License plates from the database. There should be an option of searching number plates almost matching with the specific number entered (up to 1 and 2 character distance)		
12.	Vehicle Category Editor ▪ The system should have option to input certain license plates according to category like "Wanted", "Suspicious", "Stolen", "Expired" etc. by Authorized personnel. ▪ The system should have an option to add new category by authorized personnel. ▪ The system should have option to update vehicle status in specific category by authorized personnel e.g. on retrieval of stolen vehicle, system entry should be changed from "Stolen" to "Retrieved".		

#	Description	Bidder Compliance (Yes/No)	Proposed Solution and Product documentation Reference
	▪ System should have option to specify maximum time to retain vehicle records in specific categories.		
13.	Central Management Module ▪ The Central Management Module shall run on the ANPRS Central Server in control booth. It should be possible to view records and edit hotlists from the Central Server. ▪ ANPR Specification ▪ Base Specification of Fixed Box Cameras ▪ Camera Housing ▪ IP66 standard with sunshield vandal proof Housing		
14.	Systems requirement ▪ Local Server at Intersection: The system must run on a Commercial Off the Shelf Server (COTS). Outdoor IP 66 Quad core processor based server should be able to cover at least 8 lanes. Temperature rating of the server should be at least 60 degree. ▪ Operating system: The system must be based on open platform and should run on Linux or windows Operating system. ▪ Workstation: Workstation must run on latest available OS		

4.4.3.2 Technical Specifications: ANPR Systems

#	Parameter	Minimum technical Specifications	Bidder Compliance (Yes/No)	Proposed Solution and Product Documentation Reference
1.	Make	<to be provided by the bidder>		
2.	Model	<to be provided by the bidder>		
3.	General	The system should be capable of generating a video & minimum 5 snapshot in any of the standard industry formats (MJPEG, JPG, avi, mp4, mov, etc.) with at least 10		

#	Parameter	Minimum technical Specifications	Bidder Compliance (Yes/No)	Proposed Solution and Product Documentation Reference
		frames per second. The video shall be from t-5 to t+5 sec of the violation and should also be recorded (being the instant at which the infraction occurred).		
		The system should perform ANPR on all the vehicles passing the site and send alert to the command control and communication centre on detection of any Hot-listed Vehicles (whose numbers have been marked as Stolen, Wanted, etc. at the Central server).		
		With the detected number plate text, picture should also be sent of hot listed vehicle. It is highly likely to misread similar alphabets like 7/1/L or 8/B		
4.		The system should have ANPR/ OCR to address the Alpha numerical character of irregular font sizes.		
5.	Digital Network Camera			
a.	Video Compression	H.264		
b.	Video Resolution	1920 X 1080		
c.	Frame rate	Min. 30 fps		
d.	Image Sensor	1/3" Progressive Scan CCD / CMOS		
e.	Lens Type	Varifocal, C/CS Mount, IR Correction full HD lens		
f.	Lens#	Auto IRIS 5~50mm /8 – 40 mm, F1.4		
g.	Minimum Illumination	Colour: 0.5 lux, B/W: 0.1 lux (at 30 IRE)		
h.	IR Cut Filter	Automatically Removable IR-cut filter		
i.	Day/Night Mode	Colour, Mono, Auto		
j.	S/N Ratio	≥ 50 Db		

#	Parameter	Minimum technical Specifications	Bidder Compliance (Yes/No)	Proposed Solution and Product Documentation Reference
k.	Auto adjustment + Remote Control of Image settings	Colour, brightness, sharpness, contrast, white balance, exposure control, backlight compensation, Gain Control, Ture Wide Dynamic Range		
l.	Audio	Audio Capture Capability, G.711, G.726		
m.	Local storage	Micro SDXC up to 64GB (Class 10) In the event of failure of connectivity to the central server the camera shall record video locally on the SD card automatically. After the connectivity is restored these recordings shall be automatically merged with the server recording such that no manual intervention is required to transfer the SD card based recordings to server.		
n.	Protocol	IPV4, IPV6, HTTP, HTTPS, FTP/SMTP, RTSP, RTP, TCP, UDP, RTCP, DHCP, UPnP, NTP, QoS, ONVIF Profile S		
o.	Security	Password Protection, IP Address filtering, User Access Log, HTTPS encryption		
p.	Operating conditions	0 to 50°C (temperature), 50 to 90% (humidity)		
q.	Casing	NEMA 4X / IP-66, IK10 Rated		
r.	Intelligent Video	Motion Detection & Tampering alert		
s.	Alarm I/O	Minimum 2 Input & 1 Output contact for 3rd part interface		
t.	Certification	UL/EN, CE,FCC		
6.	On site-out station processing unit communication & Electrical Interface (Junction Box)			
a.	Data Storage on site	The system should be equipped with appropriate storage capacity for 7 days 24X7 recording, with overwriting		

#	Parameter	Minimum technical Specifications	Bidder Compliance (Yes/No)	Proposed Solution and Product Documentation Reference
		capability. The images should be stored in tamper proof format only.		
b.	Network Connectivity	Wired/GPRS based wireless technology with 3G upgradable to 4G capability.		
c.	Minimum 2(two) USB Port to support the latest external mass storage devices and Ethernet (10/100) Port for possible networking. However all logs of data transfer through the ports shall be maintained by the system.			
d.	System should be capable of working in ambient temperature range of 0⁰C to 60⁰C.			
e.	Lightening arrester shall be installed for safety of system (As per BIS standard IS 2309 of 1989).			
f.	The housing(s) should be capable of withstanding vandalism and harsh weather conditions and should meet IP66, IK10 standards (certified).			
6.	Violation Transmission and Security			
a.	Encrypted data, images and video pertaining to Violations at the Onsite processing station should be transmitted to the CCCC electronically			
b.	Advanced Encryption Standard (AES) shall be followed for data encryption on site and CCCC, and its access will protected by a password.			
c.	The vendor shall ensure that the data from the onsite processing unit shall be transferred to CCCC within one day.			
7.	Video Recording			
a.	The system should be capable of continuous video recording in base station for 7 days. The system shall automatically overwrite the data after 7 days. It should be noted that at any point of time the local storage at the base station should have the data of previous 30 days.			
b.	Direct extraction through any physical device like USB flash drive, Portable Hard disk etc. shall be possible			
8.	The system should capture standard vehicle's number plates with an accuracy of at least 70%			

#	Parameter	Minimum technical Specifications	Bidder Compliance (Yes/No)	Proposed Solution and Product Documentation Reference
		at day time and at least with an accuracy of 60% at night time. (On basis of number of vehicles)		

4.4.4 Red Light Violation Detection (RLVD) System

4.4.4.1 Functional Requirements - Red Light Violation Detection System

#	Description	Bidder Compliance (Yes/No)	Proposed Solution and Product Documentation Reference
1.	Make	<to be provided by the bidder>	
2.	Model	<to be provided by the bidder>	
3.	General		
a.	One single installation system should consist of cameras out of which one camera should be an overview camera providing evidence of the violation by capturing the offending vehicle and status of the traffic light in the same field of view.		
b.	System should have the facility to provide the live feed of the camera at the central command centre as per user requirement.		
c.	System should generate Alarms at control room software if any signal is found not turning RED within a specific duration of time.		
d.	The following Traffic violations to be automatically detected by the system by using appropriate Non- Intrusive sensors technology: The system should have both provisions to detect red light status by taking the signal feed from the traffic signal controller as well as by video analytics method using another camera (Evidence Camera) focused at the red light. The Evidence camera should also be used for evidence snap generation. ▪ Red Light Violation ▪ Stop Line Violation ▪ Wrong left turn violation ▪ Wrong direction driving violation		
e.	The system should be capable of capturing multiple infracting vehicles simultaneously		

	in Different lanes on each arm at any point of time with relevant infraction data like: ▪ Type of Violation ▪ Date, time, Site Name and Location of the Infraction ▪ Registration Number of the vehicle through ANPR Camera system for each vehicle identified for infraction.		
f.	The system should be equipped with a camera system to record a digitized image and video of the violation, covering the violating vehicle with its surrounding and current state of signal (Red/Green/Amber) by which the system should clearly show nature of violation and proof thereof :- ▪ When it violates the stop line. ▪ When it violates the red signal. Besides, a closer view indicating readable registration number plate patch of the violating vehicle for court evidence for each violation. The system must have in-built tool to facilitate the user to compose detail evidence by stitching video clips from any IP camera in the junction (including but not limited to the red light violation detection camera, evidence camera), and any other surveillance cameras in the vicinity of the spot of incidence. The entire evidence should be watermarked and encrypted to stand the court of law.		
g.	The system shall be able to detect all vehicles infracting simultaneously in each lane/ arm at the junction as per locations provided. It should also be able to detect the vehicles infracting serially one after another in the same lane. The vehicles should be clearly identifiable and demarcated in the image produced by the camera system.		
h.	The Evidence image produced by the system should be wide enough to give the exact position of the infracting vehicles with respect to the stop line and clearly indicate colour of the Traffic light at the instant of Infraction even if any other means is being used to report the colour of the light.		
i.	The system should interface with the traffic controller to validate the colour of the		

	traffic signal reported at the time of Infraction so as to give correct inputs of the signal cycle.		
j.	The system shall be equipped with IR Illuminator to ensure clear images including illumination of the Number Plate and capture the violation image under low light conditions and night time.		
k.	Free Left Violation – The non-intrusive system should identify the violation where either the Free Left is blocked by other vehicles or violation occurred when no free left is allowed. ▪ The system should be capable to mark the free left junctions (through exceptions in case fewer number exists) ▪ In case of blocking the "Free Left", the system should capture multiple IVD for the vehicles in the front area of the free left blocking the road. ▪ • In case of "No Free Left", the system should be able to capture multiple IVD's.		
l.	Speed Violations ▪ The nonintrusive system shall be capable of measuring speed of vehicles and capture over speed vehicles The Speed measurement should support multiple methods for calculation of speed – either Average or Instantaneous Speed Measurement methods. ▪ The system shall have the provision of setting different speed thresholds for different class of vehicles. ▪ The speed violations system should be installed on mid-blocks or designated areas as identified during design stage.		
m.	Wrong Direction Vehicle Movement – The non-intrusive system should be installed at critical junctions to capture the wrong direction vehicle movement. The system should identify and capture multiple IVD. The E-Challan standard procedure should be triggered.		
4	Recording & display information archive medium		
a.	The recording and display of information should be detailed on the snapshot of the infracting vehicle as follows:		

b.	Computer generated unique ID of each violation		
c.	Date (DD/MM/YYYY)		
d.	Time (HH:MM:SS)		
e.	Equipment ID		
f.	Location ID		
g.	Carriageway or direction of violating vehicle		
h.	Type of Violation (Signal/Stop Line)		
i.	Lane Number of violating vehicle		
j.	Time into Red/Green/Amber		
k.	Registration Number of violating vehicle		
5	On site-out station processing unit communication & Electrical Interface		
a.	The system should automatically reset in the event of a program hang up and restart on a button press. However the system should start automatically after power failure.		
b.	The system should have secure access mechanism for validation of authorised personnel.		
c.	Deletion or addition and transfer of data should only be permitted to authorised users.		
d.	A log of all user activities should be maintained in the system.		
e.	Roles and Rights of users should be defined in the system as per the requirements of the client		
f.	All formats of the stored data with respect to the infractions should be Non Proprietary.		
g.	The communication between the on-site outstation processing unit housed in the junction box and the detection systems on the cantilever shall be mounted through appropriate secured technology.		
h.	The system should have the capability to transfer the data to CCCC through proper encryption in real time and batch mode for verification of the infraction and processing of challan. Call forwarding architecture shall be followed to avoid any data loss during transfer.		
i.	In the event that the connectivity to the CCCC is not established due to network/connectivity failures, then all data pertaining to the infraction shall be stored on site and will be transferred once the		

	connectivity is re- established automatically. There shall also be a facility of physical transfer of data on portable device whenever required. There should be a provision to store minimum one week of data at each site on a 24x7 basis.		
6	Mounting structure		
a.	Should be cantilever mounted and shall have minimum 6 Mtrs. height with appropriate vertical clearance under the system from the Road surface to ensure no obstruction to vehicular traffic.		
b.	It should be capable to withstand high wind speeds and for structural safety, the successful bidder has to provide structural safety certificate from qualified structural engineers approved/ certified by Govt. Agency.		
c.	It shall be painted with one coat of primer and two coats of PU paint. The equipment including poles, mountings should have an aesthetic feel keeping in mind the standards road Infrastructure (e.g. Poles, Navigation boards etc.) currently installed at these locations. The equipment should look "one" with the surroundings of the location and not look out of place.		
d.	Rugged locking mechanism should be provided for the onsite enclosures and cabinets.		
7	RLVD Application		
a.	It should be capable of importing violation data for storage in database server which should also be available to the Operator for viewing and retrieving the violation images and data for further processing. The programme should allow for viewing, sorting, transfer & printing of violation data.		
b.	It should generate the photograph of violations captured by the outstation system which include a wider view covering the violating vehicle with its surrounding and a closer view indicating readable registration number plate patch of the violating vehicle or its web link on notices for court evidence.		
c.	All outstation units should be configurable using the software at the Central Location.		

d.	Violation retrieval could be sorted by date, time, location and vehicle registration number and the data structure should be compatible with Ranchi Police database structure. It should also be possible to carry out recursive search and wild card search.		
e.	The operator at the back office should be able to get an alarm of all fault(s) occurring at the camera site (e.g. sensor failure, camera failure, failure of linkage with traffic signal, connectivity failure, Camera tampering, sensor tampering).		
f.	The automatic number plate recognition Software will be part of the supplied system, Success rate of ANPR will be taken as 85% or better during the day time and 65% or better during the night time with a standard number plate.		
g.	The application software should be integrated with the E-Challan/Vahaan software for tracing the ownership details of the violating vehicle and issuing/printing notices. Any updates of the software (OS, Application Software including any proprietary software), shall be updated free of cost during the contract period by MSI.		
h.	Image zoom function for number plate and images should be provided. In case the number plate of the infracting vehicle is readable only through the magnifier then in such cases the printing should be possible along with the magnified image.		
i.	Various users should be able to 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.		
j.	Apart from role based access, the system should also be able to define access based on location.		
k.	Rights to different modules / Sub-Modules / Functionalities should be role based and proper log report should be maintained by the system for such access.		
l.	Components of the architecture must provide redundancy and ensure that there are no single points of failure in the key		

	project components. Considering the high sensitivity of the system, design shall be in such a way as to be resilient to technological sabotage. To take care of remote failure, the systems need to be configured to mask and recover with minimum outage.		
m.	The architecture must adopt an end-to-end security model that protects data and the infrastructure from malicious attacks, theft 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.		
n.	The evidence of Infraction should be encrypted and protected so that any tampering can be detected.		
o.	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.		
p.	System shall use open standards and protocols to the extent possible and declare the proprietary software wherever used.		
q.	The user interface should be user friendly and provide facility to user for viewing, sorting and printing violations. The software should also be capable of generating query based statistical reports on the violation data.		
r.	The data provided for authentication of violations should be in an easy to use format as per the requirements of user.		

s.	User should be provided with means of listing the invalid violations along with the reason(s) of invalidation without deleting the record(s).		
t.	Basic image manipulation tools (zoom etc.) should be provided for the displayed image but the actual recorded image should never change.		
u.	Log of user actions be maintained in read only mode. User should be provided with the password and ID to access the system along with user type (admin, user).		
v.	Image should have a header/footer depicting the information about the site IP and violation details like date, time, equipment ID, location ID, Unique ID of each violation, lane number, Regn. Number of violating vehicle and actual violation of violating vehicle etc. so that the complete lane wise junction behaviour is recorded including (Red Light violation and Stop Line Violation)		
w.	Number plate should be readable automatically by the software/interface. There should be user interface for simultaneous manual authentication / correction and saving as well.		
x.	Interface for taking prints of the violations (including image and above details).		

4.4.4.2   Technical Specifications - Red Light Violation Detection Systems

#	Parameter	Minimum technical Specifications	Bidder Compliance (Yes/No/Equivalent)	Proposed Solution and Product Documentation Reference
1.	Make	<to be provided by the bidder>		
2.	Model	<to be provided by the bidder>		
3.	General	The system should be capable of generating a video & minimum 3 snapshot in any of the standard industry formats (MJPEG, JPG, avi, mp4, mov, etc.) with at least 10 frames		

#	Parameter	Minimum technical Specifications	Bidder Compliance (Yes/No/Equivalent)	Proposed Solution and Product Documentation Reference
		per second. The video shall be from t-5 to t+5 sec of the violation and should also be recorded (being the instant at which the infraction occurred).		
4.	Digital Network Camera			
a.	Video Compression	H.264		
b.	Video Resolution	1920 X 1080		
c.	Frame rate	Min. 30 fps		
d.	Image Sensor	1/3" Progressive Scan CCD / CMOS		
e.	Lens Type	Varifocal, C/CS Mount, IR Correction full HD lens		
f.	Lens#	Auto IRIS 5~50mm /8 – 40 mm, F1.4		
g.	Minimum Illumination	Colour: 0.5 lux, B/W: 0.1 lux (at 30 IRE)		
h.	IR Cut Filter	Automatically Removable IR-cut filter		
i.	Day/Night Mode	Colour, Mono, Auto		
j.	S/N Ratio	≥ 50 Db		
k.	Auto adjustment + Remote Control of Image settings	Colour, brightness, sharpness, contrast, white balance, exposure control, backlight compensation, Gain Control, Ture Wide Dynamic Range		
l.	Audio	Audio Capture Capability, G.711, G.726		
m.	Local storage	Micro SDXC up to 64GB (Class 10) In the event of failure of		

#	Parameter	Minimum technical Specifications	Bidder Compliance (Yes/No/Equivalent)	Proposed Solution and Product Documentation Reference
		connectivity to the central server the camera shall record video locally on the SD card automatically. After the connectivity is restored these recordings shall be automatically merged with the server recording such that no manual intervention is required to transfer the SD card based recordings to server.		
n.	Protocol	IPV4, IPV6, HTTP, HTTPS, FTP/SMTP, RTSP, RTP, TCP, UDP, RTCP, DHCP, UPnP, NTP, QoS, ONVIF Profile S		
o.	Security	Password Protection, IP Address filtering, User Access Log, HTTPS encryption		
p.	Operating conditions	0 to 60°C (temperature), 50 to 90% (humidity)		
q.	Casing	NEMA 4X / IP-66, IK10 Rated		
r.	Intelligent Video	Motion Detection & Tampering alert		
s.	Alarm I/O	Minimum 2 Input & 1 Output contact for 3rd part interface		
t.	Certification	UL/EN, CE,FCC		
5.	On site-out station processing unit communication & Electrical Interface (Junction Box)			
a.	Data Storage on site	The system should be equipped with appropriate storage		

#	Parameter	Minimum technical Specifications	Bidder Compliance (Yes/No/Equivalent)	Proposed Solution and Product Documentation Reference
		capacity for 7 days 24X7 recording, with overwriting capability. The images should be stored in tamper proof format only.		
b.	Network Connectivity	Wired/GPRS based wireless technology with 3G upgradable to 4G capability.		
c.		Minimum 2(two) USB Port to support the latest external mass storage devices and Ethernet (10/100) Port for possible networking. However all logs of data transfer through the ports shall be maintained by the system.		
d.		System should be capable of working in ambient temperature range of 0ºC to 60ºC.		
e.		Lightening arrester shall be installed for safety of system (As per BIS standard IS 2309 of 1989).		
f.		The housing(s) should be capable of withstanding vandalism and harsh weather conditions and should meet IP66, IK10 standards (certified).		
6.	Violation Transmission and Security			
a.		Encrypted data, images and video pertaining to Violations at the Onsite processing station should be transmitted to the CCCC electronically through GPRS based wireless technology with 3G upgradable to 4G, or wired connectivity if available in Jpeg format		
b.		Advanced Encryption Standard (AES) shall be followed for data encryption on site and CCCC, and its access will protected by a password.		
c.		The vendor shall ensure that the data from the onsite processing unit		

#	Parameter	Minimum technical Specifications	Bidder Compliance (Yes/No/Equivalent)	Proposed Solution and Product Documentation Reference
		shall be transferred to CCCC within one day.		
7.	Video Recording			
a.		The system should be capable of continuous video recording in base station for 30 days. The system shall automatically overwrite the data after 30 days. It should be noted that at any point of time the local storage at the base station should have the data of previous 30 days.		
b.		Direct extraction through any physical device like USB flash drive , Portable Hard disk etc. shall be possible		

4.4.5 Speed Violation Detection (SVD) System

4.4.5.1 Functional Requirements of the Speed Violation Detection System

#	Description	Bidder Compliance (Yes/No)	Proposed Solution and Product Reference
1	Make	<to be provided by the bidder>	
2	Model	<to be provided by the bidder>	
3	General		
a.	The Speed Violations should be automatically detected by the system by using appropriate sensors technology.		
b.	The system should be capable of capturing multiple infracting vehicles simultaneously in defined lanes at any point of time simultaneously with relevant infraction data like: ▪ Type of Violation ▪ Speed of violating vehicle ▪ Notified speed limit ▪ Date, time, Site Name and Location of the Infraction ▪ Registration Number of the vehicle through ANPR Camera system for each vehicle identified for infraction.		
c.	The system should be equipped with a camera system to record a digitized image or video frames of the violation, covering the violating vehicle with its surrounding.		
d.	The system shall provide the No. of vehicles infracting simultaneously in each lane. The vehicles will be clearly identifiable and demarcated in the image produced by the camera system.		
e.	The system shall be equipped with IR Illuminator to ensure clear images including illumination of the number plate and capture the violation image under low light conditions and night time.		
4	Speed		
a.	Speed measurement may be made by using non-intrusive technology such as Radar/sensor/camera/virtual based or any other appropriate certified technology. CE and homologation certificate from Ministry of Traffic or equivalent department from respective country of origin, document authenticated by Indian		

#	Description	Bidder Compliance (Yes/No)	Proposed Solution and Product Reference
	Embassy (to authenticate that systems are legalized and tested for infractions to avoid legal issues) or Certificate from internationally accredited metrology laboratories (approved for speed calibration) is acceptable		
5	On site-out station processing unit communication & Electrical Interface		
a.	The system should automatically reset in the event of a program hang up and restart after power failure.		
b.	The system should have secure access mechanism for validation of authorised personnel		
c.	Deletion or addition and transfer of data should only be permitted to authorised users.		
d.	A log of all user activities should be maintained in the system		
e.	Roles and Rights of users should be defined in the system		
f.	The data shall be transferred to the CCCC in real time for verification of the infraction and processing of challan.		
g.	In the event that the connectivity to the CCCC is not established then all data pertaining to the infraction shall be stored on site and will be transferred once the connectivity is re-established automatically.		
6	Mounting structure		
a.	Should be cantilever mounted and shall have minimum 6 Mtrs. height with appropriate vertical clearance under the system from the Road surface to ensure no obstruction to vehicular traffic.		
b.	It should be capable to withstand high wind speeds and for structural safety, the successful bidder has to provide structural safety certificate from qualified structural engineers approved/ certified by Govt. Agency.		
c.	Rugged locking mechanism should be provided for the onsite enclosures and cabinets.		
7	Speed Violation Application		
a.	It should be capable of importing violation data for the Operator for viewing and retrieving the violation images and data for further processing. The programme should provide for sort, transfer & print command.		

#	Description	Bidder Compliance (Yes/No)	Proposed Solution and Product Reference
b.	It should generate the photograph of violations captured by the outstation system which include a wider view covering the violating vehicle with its surrounding and a closer view indicating readable registration number plate patch of the violating vehicle or its web link on notices for court evidence.		
c.	All outstation units should be configurable using the software at the Central Location		
d.	Violation retrieval could be sorted by date, time, location and vehicle registration number and data structure should be compatible with Ranchi Traffic Police database and Ranchi Transport department database structure.		
e.	The operator at the back office should be able to get an alarm of any possible fault(s) at the camera site (outstand) (e.g. sensor failure, camera failure, failure of linkage with traffic signal, connectivity failure, Camera tampering , sensor tampering)		
f.	The automatic number plate recognition Software may be part of the supplied system, or can be provided separately as add on module to be integrated with violation detection. a.) Success rate of ANPR will be taken as 80% or better during the day time and 60% or better during the night time on standard number plates.		
g.	Image zoom function for number plate and images should be provided. Any updates of the software available, shall be updated free of cost during the contract period by the vendor and will integrate the same with existing application and database of Ranchi Traffic Police and Ranchi Transport department.		
h.	The application software should be integrated with the notice branch software for tracing the ownership details of the violating vehicle and issuing/printing notices.		
i.	Various users should be access the system using single sign on and should be role based. Different roles which could be defined (to be finalized at the stage if SRS) could be Administrator, Supervisor, Officer, Operator, etc.		
j.	Apart from role based access, the system should also be able to define access based on location.		
k.	Rights to different modules / Sub-Modules / Functionalities should be role based and proper		

#	Description	Bidder Compliance (Yes/No)	Proposed Solution and Product Reference
	log report should be maintained by the system for such access		
l.	Important technical components of the architecture must support scalability to provide continuous growth to meet the growing demand of Ranchi Police. The system shall support vertical scalability so that depending on changing requirements from time to time, the system may be scaled upwards. There must not be any system imposed restrictions on the upward scalability. Main technological components requiring scalability are Storage, Bandwidth, Computing Performance (IT Infrastructure), Software / Application performance and advancement in proposed system features.		
m.	The system shall also support horizontal scalability so that depending on changing requirements from time to time, the system may be scaled horizontally.		
n.	Components of the architecture must provide redundancy and ensure that are no single point of failures in the key project components. Considering the high sensitivity of the system, design shall be in such a way as to be resilient to technological sabotage. To take care of remote failure, the systems need to be configured to mask and recover with minimum outage.		
o.	The architecture must adopt an end-to-end security model that protects data and the infrastructure from malicious attacks, theft, natural disasters etc. provisions for security of field equipment as well as protection of the software system from hackers and other threats shall be a part of the proposed system. Using Firewalls and Intrusion detection systems such attacks and theft shall be controlled and well supported (and implemented) with the security policy. The virus and worms attacks shall be well defended with Gateway level Anti-virus system, along with workstation level Anti- virus mechanism. 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		

#	Description	Bidder Compliance (Yes/No)	Proposed Solution and Product Reference
	shall be properly stored & archived for future analysis and forensics whenever desired.		
p.	Ease of configuration, ongoing health monitoring, and failure detection are vital to the goals of scalability, availability, and security and must be able to match the growth of the environment.		
q.	System shall use open standards and protocols to the extent possible		
r.	The user interface should be user friendly and provide facility to user for viewing, sorting and printing violations. The software should also be capable of generating query based statistical reports on the violation data.		
s.	The data provided for authentication of violations should be in an easy to use format as per the requirements of user unit.		
t.	User should be provided with means of listing the invalid violations along with the reason(s) of invalidation without deleting the record(s).		
u.	Basic image manipulation tools (zoom etc.) should be provided for the displayed image but the actual recorded image should never change.		
v.	Log of user actions be maintained in read only mode. User should be provided with the password and ID to access the system along with user type (admin, user).		
w.	Image should have a header and footer depicting the information about the site IP and violation details like viz. date, time, equipment ID, location ID, Unique ID of each violation, lane number, Registration Number of violating vehicle and actual violation of violating vehicle etc. so that the complete lane wise junction behaviour is recorded viz. (Speed of violating vehicle, notified speed limit, Speed Violation with Registration Number Plate Recognition facility. Number plate of cars, buses/HTVs should be readable automatically by the software/interface. There should be user interface for simultaneous manual authentication / correction and saving as well		
x.	Number plate of cars, buses/HTVs should be readable automatically by the software/interface. There should be user interface for simultaneous manual authentication / correction and saving as well.		

#	Description	Bidder Compliance (Yes/No)	Proposed Solution and Product Reference
	Interface for taking prints of the violations (including image and above details).		

4.4.5.2 Technical Specifications: Speed Violation Detection System

#	Description		Bidder Compliance (Yes/No)	Proposed Solution and Product documentation reference
1.	Make	<to be provided by the bidder>		
2.	Model	<to be provided by the bidder>		
3.	The system should be capable of generating a video & minimum 3 snapshot in any of the standard industry formats (MJPEG, JPG, avi, mp4, mov, etc) with at least 10 frames per second. The video shall be from t-5 to t+5 sec of the violation and should also be recorded (being the instant at which the infraction occurred).			
4.	General requirements- ▪ The system should be designed to detect both reflective and non-reflective types of license plates. ▪ The system should provide a disaster recovering mechanism including automatic restart function after system failure. ▪ All cameras captured images and other data should be digitally watermarked & encrypted to avoid tampering			
5.	Speed			
a.	Unit of Speed Measurement	Kmph		
b.	Speed detection system to Capture speed	200Kmph ± 5%		
c.	Speed Threshold	(Vendor should provide manufacturer certificate/ third party test report in support of their claim)		

#	Description		Bidder Compliance (Yes/No)	Proposed Solution and Product documentation reference
d.	Speed Enforcement Technology	Radar/Laser/Others		
6.	Digital Network Camera			
a.	Video Compression	H.264		
b.	Video Resolution	1920 X 1080		
c.	Frame rate	Min. 60 fps		
d.	Image Sensor	1/3" Progressive Scan CCD / CMOS		
e.	Lens Type	Varifocal, C/CS Mount, IR Correction full HD lens		
f.	Lens#	Auto IRIS 5~50mm /8 – 40 mm, F1.4		
g.	Minimum Illumination	Colour: 0.5 lux, B/W: 0.1 lux (at 30 IRE)		
h.	IR Cut Filter	Automatically Removable IR-cut filter		
i.	Day/Night Mode	Colour, Mono, Auto		
j.	S/N Ratio	≥ 50 Db		
k.	Auto adjustment + Remote Control of Image settings	Colour, brightness, sharpness, contrast, white balance, exposure control, backlight compensation, Gain Control, Ture Wide Dynamic Range		
l.	Audio	Audio Capture Capability, G.711, G.726		
m.	Local storage	Micro SDXC up to 64GB (Class 10) In the event of failure of connectivity to the central server the camera shall record video locally on the SD card automatically. After the connectivity is restored these recordings shall be automatically merged with the server recording such that no manual intervention is required to transfer the SD		

#	Description		Bidder Compliance (Yes/No)	Proposed Solution and Product documentation reference
		card based recordings to server.		
n.	Protocol	IPV4, IPV6, HTTP, HTTPS, FTP/SMTP, RTSP, RTP, TCP, UDP, RTCP, DHCP, UPnP, NTP, QoS, ONVIF, Profile S		
o.	Security	Password Protection, IP Address filtering, User Access Log, HTTPS encryption		
p.	Operating conditions	0 to 50°C (temperature), 50 to 90% (humidity)		
q.	Casing	NEMA 4X / IP-66, IK10 Rated		
r.	Intelligent Video	Motion Detection & Tampering alert		
s.	Alarm I/O	Minimum 1 Input & 1 Output contact for 3rd part interface		
t.	Certification	UL/EN, CE,FCC		
7.	Recording & display information archive medium			
a.	The system should be capable of recording the following details of the infracting vehicles			
b.	Computer generated unique ID of each violation ▪ Date (DD/MM/YYYY) ▪ Time (HH:MM:SS) ▪ Equipment ID ▪ Location ID ▪ Carriageway or direction of violating vehicle ▪ In cases when multiple infracting vehicles are detected in one instant the system should be capable to provide the following data for all Infracting vehicles detected ▪ Type of Violation ▪ Notified speed limit (in Kmph) ▪ Speed of violating vehicle (in Kmph) ▪ Lane Number of violating vehicle ▪ Registration Number of violating vehicle			
8.	On site-out station processing unit communication & Electrical Interface			
a.	Data Storage on site	The system should be equipped with appropriate storage capacity for 7 days		

#	Description		Bidder Compliance (Yes/No)	Proposed Solution and Product documentation reference
		24X7 recording, with overwriting capability. The images should be stored in tamper proof format only.		
b.	Network Connectivity	Wired/GPRS based wireless technology with 3G upgradable to 4G capability.		
c.	Minimum 2(two) USB Port to support the latest external mass storage devices and Ethernet (10/100) Port for possible networking. However all logs of data transfer through the ports shall be maintained by the system.			
d.	The system should be capable of working in ambient temperature range of 0 degree C to 60 degree C			
e.	At-least one hour UPS power back up to keep the system functional in case of power failure without any break in recording the violation.			
f.	Lightening arrester shall be installed for safety of system (As per BIS standard IS 2309 of 1989)			
g.	The housing(s) should be capable of withstanding vandalism and harsh weather conditions and should meet IP66, IK10 standards (certified).			
9.	Violation Transmission and Security			
a.	Encrypted data, images and video pertaining to Violations at the Onsite processing station should be transmitted to the CCCC electronically through GPRS based wireless technology with 3G upgradable to 4G or wired connectivity, in Jpeg format.			
b.	Advanced Encryption Standard (AES) shall be followed for data encryption on site and CCCC, and its access will protected by a password.			
c.	The vendor shall ensure that the data from the onsite processing unit shall be transferred to CCCC within one day.			
10.	Video Recording			
a.	The system should be capable of continuous video recording in base station for 7 days.			

#	Description	Bidder Compliance (Yes/No)	Proposed Solution and Product documentation reference
	The system shall automatically overwrite the data after 7 days. It should be noted that at any point of time the local storage at the base station should have the data of previous 30 days.		
b.	Direct extraction through any physical device like USB, Hard disk shall be possible.		

4.4.6 Traffic Accident Reporting System (TARS)

#	Description	Bidder Compliance (Yes/No/Equivalent)	Proposed Solution and Product documentation reference
1.	Make	<to be provided by the bidder>	
2.	Model	<to be provided by the bidder>	
3.	TARS solution should provide: ▪ Accident reporting system ▪ Accident recording system ▪ Analysis of accidents ▪ Dissemination of data		
4.	Solution shall provide accident database that will support collecting high quality information on all aspects of road traffic collisions and incorporate best practices of Road Accident Investigation.		
5.	Solution shall support authorities in quickly and accurately reconstructing collisions and analysing the data to develop standards to prevent future collisions or mitigate injuries.		
6.	Solution shall support information gathering and dissemination as per various stakeholder requirements for accident data, namely, RSCCL, police, decision makers etc.		
7.	Information to be captured shall include, but not limited to: a. how the accident happened, b. detailed information about the vehicle(s) involved c. type and extent of human impact d. human factors involved (inebriation, etc.) e. nature of any injuries, f. type and extent of property damage, g. socio-economic data of the people involved, h. primary & secondary causes of the accident i. incident photos j. drawing of accident analysis k. • information on analysing agency and personnel		

4.4.7 Network Video Recorder (NVR)

Selection of Master System Integrator (MSI) for Implementation of Command Control and Communication Centre (C4) under Smart City Mission in Ranchi

#	Description	Bidder Compliance (Yes/No/Equivalent)	Proposed Solution and Product documentation reference
1.	Make	<to be provided by the bidder>	
2.	Model	<to be provided by the bidder>	
3.	The Network Video Recorder (NVR) will be connected via a Gigabit Ethernet network.		
4.	NVR shall be of N+N configuration with RAID 6 configuration.		
5.	All equipment shall be designed to provide a usable life of not less than 10 years.		
6.	The NVRs shall have a self-diagnostic feature including disk status, CPU usage, motherboard temperature, network status and fan status.		
7.	The NVRs shall be support interface using 10/100/1000BaseTX. It shall support a total throughput of at least 700 Mbps. The NVR shall be powered using 100-240VAC/50Hz. TR 4.32.		
8.	The NVR shall support both Linux and Windows platform.		
9.	The NVR shall be capable of digitally signing stored video and digitally sign exported video to ensure chain of trust.		
10.	The NVR shall have failover and redundancy built in with seamless playback without manual intervention.		
11.	The NVR shall support a minimum of 200 recorded video streams and 20 playback streams with minimum playback of 400 Mbps.		
12.	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.		
13.	Normal state (non-alarm) recording configuration to provide for "Detection" as defined by ULC-317-1997 and as follows: ▪ Resolution HD ▪ Normal Frame rate of 25 FPS		
14.	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		

4.5 Variable Message Sign boards

4.5.1 Functional Requirements of the Variable Message Signage System

#	Description	Bidder Compliance (Yes/No/Equivalent)	Proposed Solution and Product documentation reference
1	Make	<to be provided by the bidder>	
2	Model	<to be provided by the bidder>	
3	**System Requirements**		
a.	The system should be capable to display warnings, traffic advice, route guidance and emergency messages to motorists from the CCCC in real time.		
b.	The system should also be capable to display warnings, traffic advice, route guidance and emergency messages to motorist by using local PC/Laptops.		
c.	The VMSB should display text and graphic messages using Light Emitting Diode (LED) arrays.		
d.	The System should be able to display failure status of any LED at CCCC.		
e.	The System should support Display characters in true type fonts and adjustable based on the Operating system requirement.		
f.	The VMSB workstation at the CCCC should communicate with the VMS controller through the network. It should send out command data to the variable message sign controller and to confirm normal operation of the signboard. In return, the VMS workstation should receive status data from the VMS controller.		
g.	VMSB controllers should continuously monitor the operation of the VMS via the provided communication network.		

#	Description	Bidder Compliance (Yes/No/Equivalent)	Proposed Solution and Product documentation reference
h.	Operating status of the variable message sign should be checked periodically from the CCCC.		
i.	It shall be capable of setting an individual VMSB or group of VMSB's to display either one of the pre-set messages or symbols entered into the computer via the control computer keyboard or by another means.		
j.	It shall be capable of being programmed to display an individual message to a VMSB or a group of VMSB's at a pre-set date and time.		
k.	A sequence of a minimum of 10 messages/pictures/ pre-decided sign or group of signs shall be possible to assign for individual VMS or group of VMS's.		
l.	It shall also store information about the time log of message displayed on each VMS. The information stored shall contain the identification number of the VMS, content of the message, date and time at which displayed message/picture starts and ends.		
m.	The central control computer shall perform regular tests (pre-set basis) for each individual VMS. Data communication shall be provided with sufficient security check to avoid unauthorized access.		
4	**Variable Message Sign Board application**		
a.	Central Control and Communication Software should allow controlling multiple VMS from one console.		
b.	Capable of programming to display all types of Message/ advertisement having alphanumeric character in English,		

#	Description	Bidder Compliance (Yes/No/Equivalent)	Proposed Solution and Product documentation reference
	Hindi, and combination of text with pictograms signs. The system should have feature to manage video / still content for VMS display. The system should have capability to divide VMS screen into multi-parts to display diverse form of information like video, text, still images, advertisements, weather info, city info etc. The system should also provide airtime management and billing system for paid content management		
c.	Capable of controlling and displaying messages on VMS 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 VMS.		
e.	Capable of controlling brightness & contrast through software.		
f.	Capable to continuously monitor the operation of the Variable Message sign board, implemented control commands and communicate information to the CCCC 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 VMS will be plotted on GIS Map with their functioning status which can be automatically updated.		
k.	Report generation facility for individual/group/all VMSs with		

#	Description	Bidder Compliance (Yes/No/Equivalent)	Proposed Solution and Product documentation reference
	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 VMS 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 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.		
q.	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		

#	Description	Bidder Compliance (Yes/No/Equivalent)	Proposed Solution and Product documentation reference
	systems such attacks and theft shall be controlled and well supported (and implemented) with the security policy. The virus and worms attacks shall be well defended with Gateway level Anti-virus system, along with workstation level Anti- virus mechanism. There shall also be an endeavor to make use of the SSL/VPN technologies to have secured communication between Applications and its end users. Furthermore, all the system logs shall be properly stored & archived for future analysis and forensics whenever desired.		
r.	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.		
s.	System shall use open standards and protocols to the extent possible		
t.	Solution shall be integrated with the environmental monitoring system for automatically displaying information from environmental sensors.		
u.	Facility to export reports to excel and PDF formats.		
5.	**Remote Monitoring**		
a.	All VMSB shall be connected/configured to CCCC for remote monitoring through network for two way communication between VMS 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.		

4.5.2 Technical Specifications: Variable Message Signage System

#	Technical Specification	Bidder Compliance (Yes/No)	Proposed Solution and Product documentation Reference
1.	Make	<to be provided by the bidder>	
2.	Model	<to be provided by the bidder>	
3.	Dimensions		
a.	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.	Auto dimming capability to adjust to ambient light level (sensor based automatic control)		
c.	Photoelectric sensor shall be positioned at the sign front and sign rear to measure ambient light. Capable of being continually exposed to direct sunlight without impairment of performance.		
d.	Message shall be readable even in broad daylight without any shade & displayed image shall not appear to flicker to the normal human eye (>5500 cd/m2).		
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		
a.	At least 300mm as per IRC /EN 12966 standards		
b.	Full Matrix: Number of lines & characters adjustable, active area: 2.88mX1.2m at-least		
c.	Synchronized Dot to Dot display.		
b.	Capable of displaying real time message generated by CCCC.		

#	Technical Specification	Bidder Compliance (Yes/No)	Proposed Solution and Product documentation Reference
c.	Special frontal design to avoid reflection.		
d.	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.	VMS 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 sign even when diodes are not illuminated.		
c.	All periodic self-test results shall be relayed to the CCCC in real time to update the status of the VMS		
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 and any other suitable		
17.	Communication (connectivity): Wired & GPRS based wireless technology with 3G upgradable to 4G capability.		
18.	Ambient Operating Temperature: should be capable of working in ambient temperature range of 0ºC to 55ºC.		
19.	Humidity (RH): Operating ambient humidity: 10% - 95% Rh or better.		
20.	Protection against Pollution/dust/water: Complete VMS should be of IP 65 protection level from front and IP54 from side and rear. As per EN60529 or equivalent Standard.		
21.	Power		
a.	170-250V AC (more than 90% power factor) or DC as per equipment requirement.		

#	Technical Specification	Bidder Compliance (Yes/No)	Proposed Solution and Product documentation Reference
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: UPS for one hour power back-up with auto switching facility. The enclosure of UPS and battery should be pole mountable with IP 65 protected housing and lockable. Batteries with solar charging options can also be provided as back up		
23.	Material for VMS frame: at least 2mm aluminum or Non-corrosive, water resistant or better. Frame of the VMS 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 VMS sign 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 side 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: WL9 as per EN12966 to withstand high wind speeds and its own load.		
26.	Cabling, connections and Labelling		

#	Technical Specification	Bidder Compliance (Yes/No)	Proposed Solution and Product documentation Reference
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 VMS.		
f.	The successful bidder has to provide safety certificate from qualified Electrical engineers approved/certified by Govt. Agency.		
27.	Local Storage in VMS: Embedded VMS controller should be capable to store at-least 100 messages and symbols/pictograms to allow display to run in isolated mode on a predefined structures/timings, in case of connectivity failure.		
28.	The MTBF of DDS shall not be less than 100,000 hours.		

4.6 Public Address (PA) System

#	Parameter	Minimum Specifications or better	Bidder Compliance (Yes/No)	Proposed solution and Product Documentation Reference
1.	Make		<to be provided by the bidder>	
2.	Model		<to be provided by the bidder>	

#	Parameter	Minimum Specifications or better	Bidder Compliance (Yes/No)	Proposed solution and Product Documentation Reference
3.	PAS system	▪ Should have the capability to control individual PAS i.e. to make an announcement at select location (1:1) and all locations (1: many) simultaneously. ▪ The PAS should also support both, Live and Recorded inputs		
4.	Speaker	Minimum 2 speakers, To be used for Public Address System		
5.	Connectivity	IP Based		
6.	Access Control	Access control mechanism would be also required to establish so that the usage is regulated.		
7.	Integration	With VMS and Command and Control Centre		
8.	Construction	Cast Iron Foundation and M.S. Pole, Sturdy Body for equipment		
9.	Battery	Internal Battery with different charging options (Solar/Mains)		
10.	Power	Automatic on/off operation		
11.	Casing	IP-55 rated for housing		
12.	Operating conditions	0° to 50°C		

4.7 Emergency Call Box (ECB) System

#	Parameter	Minimum Specifications or better	Bidder Compliance (Yes/No)	Proposed Solution and Product Documentation Reference
1.	Make		<to be provided by the bidder>	
2.	Model		<to be provided by the bidder>	
3.	Construction	Cast Iron/Steel Foundation, Sturdy Body for equipment		

#	Parameter	Minimum Specifications or better	Bidder Compliance (Yes/No)	Proposed Solution and Product Documentation Reference
4.	Call Button	Watertight Push Button, Visual Feedback for button press		
5.	Speaker	To be used for Public Address System		
6.	Connectivity	GSM/PSTN/Ethernet as per solution offered		
7.	Sensors	For tempering/ vandalism		
8.	Battery	Internal Battery with different charging options (Solar/Mains)		
9.	Power	Automatic on/off operation		
10.	Casing	IP-55 rated for housing		
11.	Operating conditions	0° to 50°C		

4.8 Smart Parking Management System (SPMS)

4.8.1 Functional Requirement of SPMS

#	Description	Bidder Compliance (Yes / No)	Product Documentation Reference
1.	The smart parking solution is envisaged for both closed parking lots and open parking lots. ▪ Indoor Parking Spaces- Such parking spaces are managed by RMC through sub contracted vendors and the parking lots have boundary walls, closed terrace and a defined entry and exit points. ▪ Outdoor Parking Spaces- Such locations are managed by RMC through sub contracted vendors and have a boundary wall and defined entry and exit points. These kind of parking spaces have specified number of slots available, typically on an open ground or road. ▪ On street Parking Spaces- Such locations are managed by RMC through sub contracted vendors and do not have a boundary wall and defined entry and exit points. These kind of parking spaces have specified number of slots available, typically on an open ground or road		
2.	Solution must geo-reference all the parking lots and shall have the ability to add more locations in future.		
3.	Solution should be able to tally the entry and exit car counts and calculate the available parking in that parking structure.		
4.	Solution may use video camera based analytics or other sensor based solutions to determine number of vehicles entering and exiting parking lots. The smart parking solution should do so at each floor, in case of multilevel parking and communicate the data.		
5.	Solution shall also include provision to capture image of vehicle including license plate number of every vehicle entering and leaving any of the parking spaces and the all the information related to the same shall be stored at a central server.		
6.	Compliance		

#	Description	Bidder Compliance (Yes / No)	Product Documentation Reference
	a. The smart parking solution should retain videos of car entering /exiting the parking zone as per the security parameters defined by RSCCL b. MSI must ensure that all parking slots are individually and clearly marked. Solution should enable accounting and mapping of individual parking spots. All newly proposed parking spots must have one-to-one mapping with parking sensors. From existing ones, except for the very small ones, all rest will eventually have one-to-one mapping with parking sensor by phase-2 of implementation as suggested in both options of implementation strategy. c. c. There should be a provision to increase or decrease the number of parking spaces that can be reserved online through web client or mobile App, and same must reflect on web clients or mobile apps.		
7.	Visibility of vacant parking spaces ▪ Total number of slots and free slots for parking must be displayed on a digital signboard , Mobile App, Web portal ▪ Solution should report occupancy of parking lots to a central software application deployed at the Integrated Command and Control Center. ▪ Solution should enable RSCCL to obtain real time situational awareness about the occupancy of parking lot through smart dashboard. ▪ Solution should enable citizens to obtain real time space availability.		
8.	Parking Guidance subsystem for motorists		
a.	i. Accessibility of real time Parking space availability over Web client and Mobile App a. The smart parking solution should provide real time location based view to citizens about proximity of parking lots and availability of parking lots. b. The smart parking solution should have a mobile and a web delivery channel for citizens to get real time parking availability.		

#	Description	Bidder Compliance (Yes / No)	Product Documentation Reference

	c. A mobile application and web based user interface should be provided with the following features:
	  i. The application should have citizen module and officer module.
	  ii. The citizen should be able to see all the parking lots with exact available space in a real time mode.
	  iii. While locating nearest parking lot, the most updated parking slot availability should be given to the user.
	  iv. Through the citizen module, the user should be able to locate nearest parking lot and also pre –book based on his geographical coordinates. The same information must be made available on map with routing information.
	  v. Citizens should be able to generate MIS report to view their occupancy of parking lots over a defined time period.
	  vi. The administrators should be able to generate MIS report to view occupancy, collection and other usage statistics over a defined time period.		

b.	Solution should be able to communicate parking availability information at each parking lot on a LCD displays deployed at key points of interest in the city.		
c.	The Citizen App and Web Portal shall have module for Parking Solution. Solution should optimally make parking data available to a smart phone application that citizens might use to get real time parking availability.		
9.	Vehicle and License Plate Image Capture		
a.	▪ Solution shall have capability to automatically capture details of the license plates of the vehicles at every entry and exit of each parking lot. ▪ Appropriate cameras shall be installed at entry and exit of each Parking Lot.		
10.	Real-time Monitoring and Dynamic MIS Reporting		
a.	▪ System shall include central reporting system establishing the connection		

#	Description	Bidder Compliance (Yes / No)	Product Documentation Reference
	between the devices and sensors, and the C4. ▪ Solution shall include reporting dashboards with location specific thresholds to be set for generating customized reports ▪ CannzTolution shall be capable of monitoring the number of vehicles that entered or exited the parking premises during any given time ▪ Reports shall be available in all standard acceptable formats like .csv, .pdf, .txt, etc.		

4.8.2 Technical Requirement of SPMS

#	Description	Bidder Compliance (Yes / No)	Proposed Solution and Product Documentation Reference
1.	Parking Management and Guidance Solution ▪ Solution shall be able to monitor and configure all devices with respect to parking (sensors, displays, and signal converters). ▪ It shall control the system functionality and monitoring shall be done from other computers and remotely. ▪ It should provide capability to create full report of exact location with respect to floors, areas, levels, etc. It should be customizable and update about occupation and movements of vehicles in real time. ▪ It should provide real time monitoring of all system status. ▪ It should report alarms when devices are not connected or when any equipment failure so it displays on screen alarm. ▪ Shall notify alarms after a period of time if a car is abandoned.		

#	Description	Bidder Compliance (Yes / No)	Proposed Solution and Product Documentation Reference
	▪ Shall provide full graphical plan information of the car park with exact locations. ▪ Shall allow downloading the information and configuration of fields for maintenance purpose. ▪ The software application should have built in tools for third party integration to obtain real time information ▪ Should provide access at user levels with passwords. ▪ Shall have historic log for available spaces, period of time. ▪ Shall be able to handle manual overriding of available spaces, special parking requirements for reserved spaces and handicapped lots. ▪ Shall be able to manage energy saving of the car parks according to car park occupation. ▪ Shall be able to reduce brightness of light indicators manually or automatically according to occupation. ▪ Shall be able to monitor any CCTV camera with IP connection. ▪ Shall be able to monitor electricity consumption, voltage, energy, and harmonics.		
2.	Parking Sensors: ▪ Sensors should be used for detecting the real-time status of the parking space ▪ It should be able to upgrade its firmware/functionality remotely from the Emergency Operations Center ▪ It should be able to permit an optimal angle between the sensor output and target ▪ Sensor should be able to work in all weather conditions relevant to the project site		

#	Description	Bidder Compliance (Yes / No)	Proposed Solution and Product Documentation Reference
	▪ Sensors should preferably have magnetic or optic technology ▪ Conform ISO 9001 Quality Assurance Standard ▪ Protection Level: IP67		
3.	▪ The on-street parking sensor shall be based on non-intrusive technology, preferably geo-magnetic/camera based sensors ▪ Each parking sensor shall be able to monitor a minimum of 10 parking spots. ▪ Parking sensor shall be able to communicate to the parking system and shall update occupancy status in real time. ▪ It shall have operating temperature range of 0 to 70 degrees C. ▪ The sensor shall be IP65 rated for environmental protection.		
4.	Parking Management and Guidance Solution a. The solution will be implemented in the Integrated Industry Standard Open Platform to manage, monitor and control C4 initiative. Integrated Industry Standard Open Platform should have API based access to the Parking Management and Guidance System as well as the devices utilized for parking. b. Solution should be able to monitor and configure all devices with respect to parking (sensors, displays, and signal converters). c. It should control the system functionality and monitoring should be done from other computers and remotely. d. It should provide capability to create full report of exact location with respect to floors, areas, levels, etc.		

#	Description	Bidder Compliance (Yes / No)	Proposed Solution and Product Documentation Reference
	e. It should be customizable and update about occupation and movements of vehicles in real time. f. It should provide real time monitoring of all system status. g. It should report alarms when devices are not connected or when any equipment failure occurs. h. The software should notify alarms after a period of time if a car is abandoned. i. The software should provide full graphical plan information of the car park with exact locations. j. The software should allow downloading the information and configuration of fields for maintenance purpose. k. The software application should have built in tools for third party integration to obtain real time information l. Should provide access at user levels with passwords. m. The software should have historic log for available spaces, period of time. n. 13. The software should be able to handle manual overriding of available spaces, special parking requirements for reserved spaces and handicapped lots.		

4.9 Environmental Management System

4.9.1 Functional Requirement of EMS

#	Description	Bidder Compliance (Yes / No)	Product Documentation Reference
1.	Shall be ruggedized enough to be deployed in open air areas on streets and park		
2.	Environmental Sensor station shall be housed in a compact environmentally rated outdoor enclosure. It shall be an integrated module which shall monitor overall ambient air, noise quality, weather etc.		
3.	Mounting of the environmental sensor module shall be co-located on streetlight pole or shall be installed on a tripod/standalone pole.		
4.	Environmental sensor station shall monitor following parameters and include the following integrated sensors inside one station: ▪ Carbon Monoxide (CO) sensor ▪ Ozone (O3) sensor ▪ Nitrogen Dioxide (NO2) sensor ▪ Sulphur Dioxide (SO2) sensor ▪ Carbon Dioxide (CO2) sensor ▪ Particulate/SPM Profile (PM10, PM2.5, and TSP) sensor ▪ Temperature sensor ▪ Relative Humidity sensor ▪ Wind Speed sensor ▪ Wind Direction sensor ▪ Rainfall sensor ▪ Barometric Pressure sensor; and ▪ • Noise sensor.		
5.	Solution shall display trends of environmental parameters based on user specific time periods.		
6.	Data shall be collected in a software platform that allows third party software applications to read that data.		
7.	Solution shall display real time and historical data in chart and table views for dashboard view of the Client.		
8.	Alarms shall be generated for events where the environmental parameters breaches the safe or normal levels.		

#	Description	Bidder Compliance (Yes / No)	Product Documentation Reference
9.	The sensor management platform shall allow the configuration of the sensor to the network and also location details etc.		
10.	**Central Monitoring System (CMS)**		
6.1	▪ It shall comprise of an Industrial PC running latest version OS and compatible software. ▪ Data logging with central Monitoring System will be through GPRS/TCP-IP from all the AAQMS and MMS system and shall have an ability to program and log channels at different intervals and shall have a capability of averaging and displaying real time data and averaged data over a period of 1 min, 10 min, ½ hr, 1 hr, 4 hr, 8, hr, 24 hr and so on. ▪ Real time or averaged data can be viewed quickly and easily through a remote interface on the central computer. ▪ System shall be able to perform nested calculations vector averaging and rolling averages. ▪ It shall have a feature for viewing instantaneous and historical data in the form of tables and graphs either locally or from a remote client. ▪ Data retrieval from CMS via USB and DVD shall be possible. ▪ Generation of reports for pollution load, wind rose etc. ▪ Alarm annunciation of analyzer/sensor in abnormal conditions.		
7	**Other Requirement**		
7.1	▪ The environment sensors shall be integrated with the command control system to capture and display/ provide feed. The data it collects is location-marked. ▪ Various environment sensors shall sense the prevailing environment conditions and send the data to the integrated control system where real time data resides and the same shall be made available to various other departments and applications for decision making.		

#	Description	Bidder Compliance (Yes / No)	Product Documentation Reference
	▪ Information shall be relayed to signage – large, clear, digital-display screens which let citizens know regarding the prevalent environmental conditions. ▪ Further environmental sensors recorded data shall be used by Mobile application to enable user for alarm management and notification of environmental details on real time basis.		

4.9.2 Technical Requirement of Environment Management Sensors

#	Description	Bidder Compliance (Yes / No/)	Proposed Solution and Product Documentation Reference
1.	**Carbon Monoxide (CO) Sensor** ▪ CO sensor shall measure the carbon monoxide in ambient air ▪ Range of CO sensor shall be between 0 to 1000 PPM ▪ Resolution of CO sensor shall be 0.001 PPM or better ▪ Lower detectable limit of CO sensor shall be 0.040 PPM or better ▪ Precision of CO sensor shall be less than 3% of reading or better ▪ Linearity of CO sensor shall be less than 1% of full scale or better ▪ Response time of CO sensor shall be less than 60 seconds ▪ Operating temperature of CO sensor shall be 0°C to 60°C ▪ Operating pressure of CO sensor shall be ±10%.		
2.	**Ozone (O3) Sensor** ▪ O3 Sensor shall measure the ozone in ambient air ▪ O3 Sensor shall have a range of at least 0-1000 PPB ▪ Resolution of O3 sensor shall be 0.001 PPM or better ▪ Lower detectable limit of O3 sensor shall be 0.001 PPM or better		

#	Description	Bidder Compliance (Yes / No/)	Proposed Solution and Product Documentation Reference
	- Precision of O3 sensor shall be less than 2% of reading or better - Linearity of O3 sensor shall be less than 1% of full scale - Response time of O3 sensor shall be less than 60 seconds - Operating temperature of O3 sensor shall be 0°C to 60°C - Operating pressure of O3 sensor shall be ±10%		
3.	**Nitrogen Dioxide (NO2) Sensor** - NO2 Sensor shall measure the Nitrogen dioxide in ambient air - NO2 Sensor shall have a range of at least 0-10 PPM - Resolution of NO2 sensor shall be 0.001 PPM or better - Lower detectable limit of NO2 sensor shall be 0.001 PPM or better - Precision of NO2 sensor shall be less than 3% of reading or better - Linearity of NO2 sensor shall be less than 1% of full scale - Response time of NO2 sensor shall be less than 60 seconds - Operating temperature of NO2 sensor shall be 0°C to 60°C - Operating pressure of NO2 sensor shall be ±10%		
4.	**Sulfur Dioxide (SO2) Sensor** - SO2 Sensor shall measure the Sulfur dioxide in ambient air - SO2 Sensor shall have a range of at least 0-20 PPM - Resolution of SO2 sensor shall be 0.001 PPM or better - Lower detectable limit of SO2 sensor shall be 0.009 PPM or better - Precision of SO2 sensor shall be less than 3% of reading or better - Linearity of SO2 sensor shall be less than 1% of full scale - Response time of SO2 sensor shall be less than 60 seconds		

#	Description	Bidder Compliance (Yes / No/)	Proposed Solution and Product Documentation Reference
	▪ Operating temperature of SO2 sensor shall be 0°C to 60°C ▪ Operating pressure of SO2 sensor shall be ±10%		
5.	**Carbon Dioxide (CO2) Sensor** ▪ CO2 Sensor shall measure the carbon dioxide in ambient air ▪ CO2 Sensor shall have a range of at least 0-5000 PPM ▪ Resolution of CO2 sensor shall be 1 PPM or better ▪ Lower detectable limit of CO2 sensor shall be 10 PPM or better ▪ Precision of CO2 sensor shall be less than 3% of reading or better ▪ Linearity of CO2 sensor shall be less than 2% of full scale ▪ Response time of CO2 sensor shall be less than 60 seconds ▪ Operating temperature of CO2sensor shall be 0°C to 60°C ▪ Operating pressure of CO2 sensor shall be ±10%		
6.	**Particulate Profile Sensor** ▪ Particulate profile sensor shall provide simultaneous and continuous measurement of PM10, PM2.5, SPM and TSP (measurement of nuisance dust) in ambient air ▪ Range of PM2.5 shall be 0 to 230 micro gms / cu.m or better ▪ Range of PM10 shall be 0 to 450 micro gms / cu.m or better ▪ Lower detectable limit of particulate profile sensor shall be less than 1 µg/m3 ▪ Accuracy of particulate profile sensor shall be <± (5 µg/m3 + 15% of reading) ▪ Flow rate shall be 1.0 LPM or better ▪ Operating temperature of the sensor shall be 0°C to 60°C		

#	Description	Bidder Compliance (Yes / No/)	Proposed Solution and Product Documentation Reference
	▪ Operating pressure of the sensor shall be ±10%		
7.	**Temperature Sensor** ▪ Temperature sensor shall have the capability to display temperature in °Celsius ▪ Temperature range shall be -10° to +80°C ▪ Sensor accuracy shall be ±0.3°C (±0.5°F) or better ▪ Update interval shall be 10 to 12 seconds		
8.	**Relative Humidity Sensor** ▪ Range of relative humidity sensor shall be 1 to 100% RH ▪ Resolution and units of relative humidity sensor shall be 1% or better ▪ Accuracy of the sensor shall be ±2% or better ▪ Update interval shall be less than 60 seconds ▪ Drift shall be less than 0.25% per year		
9.	**Wind Speed Sensor** ▪ Wind speed sensor shall have the capability of displaying wind speed in km/h or knots ▪ Range of sensor shall be 0-60 m/s ▪ Accuracy of wind speed sensor shall be ±5% or better ▪ Update interval shall be less than 60 seconds		
10.	**Wind Direction Sensor** ▪ Range of the wind direction sensor shall be 0° to 360° ▪ Display resolution shall be 16 points (22.5°) on compass rose, 1° in numeric display ▪ Accuracy shall be ±3% or better ▪ TR 6.70 Update interval shall be 2.5 to 3 seconds		
11.	**Rainfall Sensor**		

#	Description	Bidder Compliance (Yes / No/)	Proposed Solution and Product Documentation Reference
	▪ Rainfall sensor shall the capability of displaying level of rainfall in inches and millimeter ▪ Daily Rainfall range shall be 0 to 99.99" (0 to 999.8 mm) ▪ Monthly/yearly/total rainfall range shall be 0 to 199" (0 to 6553 mm) ▪ Accuracy for rain rates shall be up to 4"/hr (100 mm/hr) or ±4% of total ▪ Update interval shall be less than 60 seconds ▪ 0.02" or (0.5mm) of rainfall shall be considered as a storm event with 24 hours without further accumulation shall end the storm event		
12.	**Barometric Pressure Sensor** ▪ Barometric pressure sensor shall have the capability of displaying barometric pressure in Hg, mm Hg and hPa/mb ▪ Range of barometric pressure sensor shall be 540 hPa/mb to 1100 hPa/mb ▪ Elevation range of the barometric pressure sensor shall be -600 m to 4570 m ▪ Uncorrected reading accuracy shall be ±1.0 hPa/mb at room temperature or better ▪ Equation source of the sensor shall be Smithsonian Meteorological tables ▪ Equation accuracy shall be ±0.01" Hg (±0.3 mm Hg, ±0.3 hPa/mb) or better ▪ Elevation accuracy shall be ±10' (3m) to meet equation accuracy specification or better. ▪ Overall accuracy shall be ±0.03" Hg (±0.8 mm Hg, ±1.0 hPa/mb) or better.		

#	Description	Bidder Compliance (Yes / No/)	Proposed Solution and Product Documentation Reference
	▪ TR 6.85 Update interval shall be less than 60 seconds		
13.	**Noise Sensors** ▪ Noise sensor shall detect the intensity of the ambient sound in a particular area ▪ Nosie Sensors shall be installed for the outdoor applications ▪ Noise sensor shall be able to identify the areas of high sound intensity ranging from 30 dBA to 120 dBA ▪ Noise sensor shall have resolution of 0.1 dBA		
14.	Integration with CCCC solution, VMSB, Portal and Mobile applications		
15.	Conditions-Ruggedized enough to be deployed in open air areas on streets and park		

4.10 Web Portal and Mobile Application

4.10.1 Web Portal

4.10.1.1 Functional and Technical Requirements of Web Portal

Ranchi has approx. 1 Million of total population and number of visitors for portal may be taken as 2% of the total population.

#	Description	Bidder Compliance (Yes / No)
1.	**Home Page** A clean, visually compelling home page that quickly conveys to the visitor, the RSCCL's mission and what RSCCL does. It will include (but not limited to) the following information either directly or linked through other pages: ▪ About RSCCL; Corporation, Message from the CMD, Board of Directors, Shareholding pattern, Organogram & Key Personnel ▪ City Profile ▪ Master Plan ▪ Investment opportunities ▪ Key statistics	

#	Description	Bidder Compliance (Yes / No)
	▪ 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	

#	Description	Bidder Compliance (Yes / No)
	RSCCL and access to the portal as well the respective departments/agencies/corporations/ministries.	
10.	**Easy access to Key performance indicators (Infographics):** Seamless presentation of dashboard data to provide continuously updated graphs and charts.	
11.	**News/Update feed:** Constant and dynamic update feed on portal home page. Displays announcements and notifications for new content additions on front page of portal.	
12.	**Calendar and bookings:** A dynamic calendar that displays events as well as filters for searching events and booking any available venues/functions.	
13.	**Contact Form:** Provides a web-based contact form with anti-spam controls and shall allow stakeholders to track the status of request at any point of time, if any.	
14.	**e-Mails**: automatically send follow-up emails to our stakeholders (subscribers) if they visited a specific web page, or completed some specific task (e.g. survey) on the website.	
15.	**Social Media Engagement Tools:** New tools to improve interaction with social media.	
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 Ranchi 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:**	

#	Description	Bidder Compliance (Yes / No)
	✓ 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 RSCCL to extract maximum benefits from the system.	
27.	**Design and Construction** ▪ Work closely with the RSCCL 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 RSCCL 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 RSCCL'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 RSCCL 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.	

#	Description	Bidder Compliance (Yes / No)
28.	Portal should support JSR 286.	

4.10.2 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.

4.10.2.1 Functional and Technical Requirements of Mobile App

#	Description	Bidder Compliance (Yes / No)
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: ▪ 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	

#	Description	Bidder Compliance (Yes / No)
	▪ 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.	

4.11 Enterprise GIS

4.11.1 Functional and Technical Requirements of Enterprise GIS

#	Description	Bidder Compliance (Yes / No)	Product Documentation Reference
1	**GIS Base map Preparation**		
1.1	RSCCL shall provide available GIS administrative data along with property layer to the selected MSI		
1.2	MSI shall asses the quality of available GIS data and accordingly shall create the GIS data creation plan for remaining data layers in consultation with the RSCCL.		
1.3	GIS base map shall be a common platform across all the solutions including City Wi-Fi, Video Surveillance, Smart Lighting, Intelligent Traffic, Smart Parking, ICT based solid waste management, Intelligent transport, Disaster management, Incident Management & any other ICT component in consultation with RSCCL.		
1.4	MSI shall develop GIS based Decision Support System for public safety & law enforcement.		
1.5	MSI shall use spatial & non-spatial information from GIS database to develop real-time management of various surveillance systems like Traffic Management, VTMS, Smart Parking and incident management, etc.		
1.6	GIS database shall be in any OGC format;		

#	Description	Bidder Compliance (Yes / No)	Product Documentation Reference
1.7	GIS base map shall include following, but not limited these data with attributes with necessary attributes which shall be finalized during study phase; a) Road Network b) Railway Network c) Administrative boundaries (RSCCL Boundary, Ward Boundary etc.) d) Building footprints and names e) Points of Interest data includes: ✓ Health Services (Hospitals, Blood Banks, and Diagnostics Centre, Ambulance Services, Other Medical Services etc.) ✓ Community services (Fire stations, Police stations, Banks, ATMs, Post offices, Educational facilities, Govt. Buildings etc.) ✓ Business Centres (Shopping malls, Markets, Commercial complexes etc.) ✓ Residential areas (Apartments, Housing societies etc.) ✓ Transportation (Bus stops/Terminus, Parking areas, Petrol Pumps, Airports etc.) ✓ Recreation facilities (Restaurants, Theatres, Auditoriums etc.) ✓ Other utilities such as travel and tourism facilities, religious places, burial grounds, solid waste locations etc. ✓ Local landmarks with locally known names. f) Land-Cover (Green areas, Open Areas, Water bodies) g) Address layers (Pin code, Locality, Sub-locality etc.) h) Utility Networks (OFC, Water, Sewer, Drainage etc. i) Locations of other Municipal Assets j) Education (Primary/Secondary/High School/Colleges) k) Religious structures l) Community centres		
2	**Web GIS Decision Support System**		
2.1	User Creation and Security Management		

#	Description	Bidder Compliance (Yes / No)	Product Documentation Reference
2.2	Map Browsing Module		
2.3	Data Editing & Search Module ▪ Point ▪ Line ▪ Polygon		
2.4	Data Analysis Module ▪ Buffer ▪ Spatial Overlay ▪ Application Interface ▪ Big Data support		
2.5	Citizen Location Services		
2.6	Generating Reports		
2.7	Help File Creation		
2.8	Thematic Mapping (On the fly)		
3	**User Creation and Security Management**		
3.1	Shall facilitate to create, delete & modify different Enterprise GIS Users within RSSCL.		
3.2	▪ Shall be accessible only to System Administrator while all other modules/sub modules shall be accessible to individual users based on the access rights provided to them by System Admin ▪ Create Application Interface ▪ Create admin right and grant suitable viewing/data editing rights ▪ Monitor access rights to user departments ▪ Maintains Application Security ▪ Maintain Interface with RSCCL Internal Departments to resolve technical issues ▪ Shall allow Active Directory, LDAP, or other security source ▪ Shall allow administrator to configure security to map service, layer and attribute levels ▪ Shall allow group-based security policies ▪ Shall not require opening of any special protocols for connecting the user client to the web/application server used by the package. All communication shall be on HTTP or HTTPs. ▪ MSI shall suggest firewalls that natively support all protocols required between the various servers (database, application and web) in the package. No		

#	Description	Bidder Compliance (Yes / No)	Product Documentation Reference

	special configuration shall be required to configure the firewall.
	▪ Application users shall not have direct access to the database.
	▪ Any changes to data should be recorded in a separate table and should be stamped with the identity of the user/program and the date / time of the creation/change.
	▪ Shall be possible to audit users at the form level, user level, application module level and at the organizational role level.
	▪ Shall provide reports on user activity based on the role and the application that was used.
	▪ Shall support configurable password policies including;
	  ✓ Password expiry
	  ✓ Password complexity
	  ✓ Password history and reuse policy
	  ✓ Forced password change on first log on
	  ✓ Capability of self-service reset of passwords in case of forgotten passwords or locked accounts.
	  ✓ Shall support security system with a full-fledged Role Based Access Control (RBAC) model		

4	**Map Browsing**		
4.1	This module shall mainly comprise of the basic map navigation tools and the most essential tools for identification of features and attributes. Following are some of the map browsing functionalities : ✓ Zoom in: The user shall be able to select a particular portion of the map by drawing a rectangle on the map specifying the extent into which the map shall be zoomed in to see the features more closely and in more detail. ✓ Zoom out: The user shall be able to select a particular portion of the map by drawing a rectangle or just clicking on the map to see the map at a smaller scale.		

#	Description	Bidder Compliance (Yes / No)	Product Documentation Reference
	✓ Full view (Full Extent): The user can view the map in full extent after zooming in or zooming out at different scales ✓ Pan: The user shall be given an option to pan the map, which shall be possible if the entire map is not fitting into the screen, i.e., after the user has zoomed in to the map at a certain extent. ✓ Identify: The user shall be able to view attribute information of the feature of interest. ✓ Find: User can key in the desired area and the application shall highlight the area on the map. ✓ Measure distance/area: Two options shall be provided to the user. The user shall be able to measure the area and to measure the distance ✓ Refresh Map: All the selected features of the active map layer shall be cleared of the selection, by using this tool. ✓ Select Feature: User shall be able to select the features of active map layer ✓ Clear selection: User shall be able to clear selection that is there on map ✓ Activity indicator: Display notification while map/ data is being processed ✓ Scale input box: allow user to enter representative fraction scale for dynamic services - For cached services, scale box should contain dropdown menu of available cache scales (levels of detail) ✓ Show/hide co-ordinates: Show/hide mouse coordinates ✓ Print: The map can be printed in its current extent as viewed in the map window. The user would be presented with a layout for printing ✓ Descriptive Map Information Tool: When the mouse cursor hovers over each map feature, information should be shown based on the feature's attributes. Functionality should be available for all feature classes; should be able to display a combination of attributes and should		

#	Description	Bidder Compliance (Yes / No)	Product Documentation Reference
	not limit the number of features that can be included with the map tool. It should allow user to turn on and off as needed.		
5	**Data Editing & Search**		
5.1	▪ Shall provide the data editing capabilities including new data addition and existing data updation for geographical features and its attributes. ▪ Shall provide user to edit GIS Features. However, for a bulk data editing, RSCCL shall use Desktop GIS facility, since web based data editing of large database may cause data corruption. Following are the steps for editing any features through Web GIS- ✓ Add Features ✓ Delete Features ✓ Move Features ✓ Modify Features ✓ Select Feature to Edit ✓ Feature Locate by Manual Browsing ✓ Feature Locate by Entering Lat and Long ✓ Feature Location by search criteria. ✓ Identify Feature to Edit ▪ Shall allow users to search features by both pre-configured and dynamic based on unique values as follows; ✓ Search by Ward, ✓ Search by area, ✓ Search by Plot/ CTS Number, ✓ Search by Building Number, ✓ Search by Sector, ✓ Search by UPID, Aaadhar etc. ✓ Search by area, ✓ Search by Plot/ CTS Number, ✓ Search by Building Number, ✓ Search by Sector ✓ Search by Parcel ID etc. ▪ Shall allow user to run the custom queries on-the-fly and save those queries for shared future use ▪ Shall allow user to run spatial query on multiple layers with spatial operators ▪ Shall also allow for a buffer to be applied to the search criteria allowing for		

#	Description	Bidder Compliance (Yes / No)	Product Documentation Reference
	features within a certain distance of the query feature to be selected. ▪ Shall have facility to run combination of attribute & spatial query ▪ Shall have facility to auto-complete text boxes based on either feature attributes or linked records		
6	**Date Analysis Module**		
6.1	Shall comprise of analytical tools such as spatial overlay, buffer analysis to generate results, and shall also provide geo-processing functions that will be finalized at the time of study stage.		
7	**Visualization of Temporal Data**		
7.1	Shall have facility to visualize time aware layers		
7.2	Shall allow user to add temporal data layer on-the-fly		
8	**Printing**		
8.1	▪ Shall have ability to print maps to a printer/plotter with the selection of paper size (A2, A1, A0, Letter, Tabloid etc.) and page orientation (landscape or portrait) ▪ Shall have print preview option ▪ Shall be able to handle and process any redlining / markups of the map. ▪ Shall have ability to export the map to a standard image format (BMP, TIF, JPEG and PDF file) ▪ Shall have a variety of templates must be available which allow the user to add a custom map title and to decide which map elements (north arrow, scale bar, overview map, legend, etc.) will be visible. ▪ Print date and time shall be automatically added to output at application runtime ▪ Legend shall be automatically adjusted based layers displayed in print area		
9	**Redlining Capabilities**		
9.1	▪ Shall allow users to draw simple shapes (point, line, rectangle, polygon and circle) and add text to make annotations and markups to the map that must be		

#	Description	Bidder Compliance (Yes / No)	Product Documentation Reference
	printable. It shall allow the user to provide supplemental information on the map. ■ Shall allow user to set the redlining display style based on the following specification: Line: color, style, transparency and width. Rectangle, circle, and polygon: fill color, fill opacity, outline style, outline color and outline width.		
10	**Add Map Layers**		
10.1	Shall allow user to add GIS map layers Added new map layer shall be overlaid on the existing map		
11	**Hyperlinks**		
11.1	Shall have ability to hyperlink to document, images, avi files and PDF files with the feature's attribute		
12	**Emailing**		
12.1	Shall allow user to Email map as an attachment		
13	**Reporting**		
13.1	■ Shall provide predefined report templates ■ Shall allow user to create custom reports using SQL query interface and save those reports for shared future use ■ Shall allow user to generate reports on selected features ■ Shall be able track the history of reports a user has performed. ■ Shall be able to export reports into PDF and MS Excel ■ Shall allow use to select different date ranges to view report information ■ Shall allow user to print reports		
14	**Web-Editing**		
14.1	■ Support role based multi-user editing access and editing work flows. ■ Shall allow authenticated user to validate spatial feature create/delete/edit/upload through Web-GIS application ■ Shall allow administrator to Accept/Reject the changes made and a log shall be created for the same.		

#	Description	Bidder Compliance (Yes / No)	Product Documentation Reference
	▪ Shall have easy-to-use map editing tools ▪ Shall allow user to divide the polygon or polyline ▪ Shall allow user to amalgamate the two or multiple polygons or polylines ▪ Shall allow administrator to configure the edit/view security at the level of feature attribute		
15	**Select Feature**		
15.1	▪ Should be able to select features by clicking on or by drawing a polygon around the feature ▪ Should allow user to generate URL for current view extents, visible layers, and active selection ▪ Should allow user to email the generated URL ▪ Should allow user to export data into KML/KMZ and Shapefile		
16	**Bookmarks:** ▪ User should be able to save a map view and be able to return to that exact view at a later date ▪ User should have ability to email the current view extents, visible layers, and active selection in the form of image		
17	**Application Error Reporting:** Should allow user to report errors, with a screen capture, back to the RSCCL GIS Coordinator		
	Technical Specifications		
18	Layer and data security – it shall have a provision to configure user level access to data and layers.		
19	Shall be compatible for accessibility from any device (i.e. Mobile, Tablet and Laptop), Standard Operating Systems and Internet Browsers.		
20	Shall support One-Web functionality		
21	Shall have provision for flow of information and/or integration with existing and future applications (indicative) such as: ▪ Smart Lighting, ▪ Vehicle Tracking System ▪ ICT based solid waste management ▪ Intelligent Traffic Management System		

#	Description	Bidder Compliance (Yes / No)	Product Documentation Reference
	▪ Intelligent Transport Management System ▪ Smart Parking Management System ▪ Environmental Sensors ▪ Wi-Fi Hotspots ▪ Smart Water Supply Management ▪ Property Tax management system ▪ Building Plan Approval System ▪ Enterprise Project Management ▪ Any other Municipal e-Governance Application		
22	It shall be a single window application to visualize MIS and GIS data on the same platform.		
23	It shall be have User Management component for defining user roles to control the access of tools and database as per RSCCL's requirement.		
24	It shall have a provision to perform Quality Control activity on the data collected from the field before storing on the parent database server.		
25	It shall have provision to generate custom reports.		
26	It shall have provision to generate thematic maps on-the-fly based on attributes details available in the GIS layers		
27	It shall have a provision to store audit trail of user activities performed on the application.		
28	MSI shall be sole responsible for creating an integration approach through integration service bus for message delivery, services based on standards such as SOAP, HTTP and WCS.		
29	The integration service bus shall be designed to promote high throughput, compatibility, flexibility and scalability. Specific functionalities need to be configured for data retrieval from Web-GIS.		
30	Shall provide a simple and easy to manage integration architecture for all external applications and should have functionalities to check for integrity and validity of data during import & export.		

#	Description	Bidder Compliance (Yes / No)	Product Documentation Reference
31	Shall be able to toggle between Web-GIS and external applications.		
32	Shall allow user to view the maps and attribute data (in limited form) from external applications as well as from the Web GIS window and perform basic functionalities of external applications through the web-GIS window and vice-versa.		
33	Shall be supported with Internet Explorer 9 and above, Latest version of Chrome, Mozilla & Safari browser.		
34	System is expected to realign and fit to the smart mobile devices (iOS, Android etc.).		
35	Solution should be compatible with various open standards and technologies and should not restrict RSCCL in using the solution data for any other applications, and should compliance National Data Sharing and Accessibility Policy (NDSAP) dated 17 March 2012, India's open Government data guidelines.		
36	Standardization and Interoperability – the proposed Web GIS Map engine shall be OGC (Open Geospatial Consortium) and SWE (Sensor Web Enablement) compliant.		
37	**Distance and Area Measurement**		
37.1	Should have distance measurements tool to allow user to measure the length of irregular shaped lines		
37.2	Should have area measurements tool to allow user to measure irregular shaped polygons		
37.3	Measurements should be shown using the metric and the imperial system. The ability to snap to the edge or nodes of the feature being measured is desirable		
38	**Event based trigger**		
38.1	Ability to connect to Data Stream: Connectors for common data streams including in-vehicle GPS devices, mobile devices, and social media providers		
38.2	Process and Filter Real-Time Data: Detect and focus on the most important events, locations, and thresholds of operations without interruption. (data transmission		

#	Description	Bidder Compliance (Yes / No)	Product Documentation Reference
	without latency) Should be able to accommodate multiple streams of data flowing continuously through filters and processing steps that you define. (live event route mapping)		
38.3	Monitor Assets: Track most valuable assets on a map. Should be able to track dynamic assets that are constantly changing location (such as vehicles), or stationary assets, such as weather and environmental monitoring sensors.		
38.4	Respond to Events in Real Time: When locations change or specified criteria are met, automatically and simultaneously send alerts to key personnel, update the map, append the database, and interact with other enterprise systems. Alerts can be sent across multiple channels, such as e-mails, texts, and instant messages.		
39	**Hyperlink**		
39.1	Should have ability to hyperlink to document, images, avi files and PDF files with the feature's attribute		
40	**Dashboard**		
40.1	Should provide easy-to-understand, easy-to-use reports that use appropriate infographics (Charts) to present key indicators from the GIS database, to provide overall information to the key officials		
40.2	Should have a GIS-enabled real-time dashboard to display dynamic charts & graphs		
41	Video / CCTV Surveillance Interface		
41.1	User should be able to see the location of CCTV cameras installed and mapped on to the GIS map		
41.2	System should have provision to integrate with video feeds available from CCTV camera		

Functional & Technical Requirement: WebGIS Software

#	Description	Bidder Compliance (Yes / No)	Product Documentation Reference
1.	Facility for display of spatial layers, query management like have various query tools for queries based on attributes, location, etc.		
2.	Facility for basic Navigation tools like the software should have tools to Pan, Zoom, and Rotate the Map according to user requirements		
3.	Facility for spatial data classification based on specific attribute value and report generation		
4.	Ability to search and to zoom into the user specified x, y coordinates		
5.	Provision for definition of map projection system and geodetic datum to set all the maps in a common projection and scale.		
6.	Facility to click on any feature of the map and return a select set of attributes for feature.		
7.	Facility to perform the spatial intersection analysis like plot area with buffer zone to calculate road widening impact on adjacent land.		
8.	Allow user to open raster images, or satellite images of various standard format.		
9.	Ability to import / export data from / to various formats like shape, MIF, dxf etc.		
10.	Allow users to export query results to various file formats like bmp, Tiff, Jpeg, pdf, etc.		
11.	Support printing spatial data at different scales and at adjustable print quality.		
12.	WebGIS Software should use RDBMS for geometrical and geographical data		
13.	ODBC compliance enabling interface with leading industry RDBMS should be there.		

#	Description	Bidder Compliance (Yes / No)	Product Documentation Reference
14.	Allow user to create layers or shortcuts to geographic data that store symbology for displaying features.		
15.	Provision of hyper linking the GIS feature as well as its attribute fields with existing documents, drawing files or scanned maps related to that feature.		
16.	Facility to create and organize user desired number of Spatial Bookmarks and should be able to share the same.		
17.	To have Control environment, feature functions, spatial relationship and geometric functions including math's and transformation functions		
18.	The software should support Map Services, Open Geospatial Consortium, Inc. (OGC) services like WMS, WFS etc.		
19.	The Application shall be able to serve multiple maps/layer with single/fewer configurations or shall have support for SQL Views		
20.	The application Shall have support for CQL Filters to obtain better Analytical capabilities		
21.	The WebGIS Application shall be highly scalable to serve increasing number of user with no extra cost		

Selection of Master System Integrator (MSI) for Implementation of Command Control and Communication Centre (C4) under Smart City Mission in Ranchi

Technical Requirement

#.	Description	Bidder Compliance (Yes / No)	Product Documentation Reference
1.	The application shall support all leading browsers		
2.	The application shall be OS independent		
3.	The application shall offer User rights (ensuring security)		
4.	The application shall run on Web browser and be capable to display as base Map, Google Maps, ESRI Street map as well as the Project Base Map		
5.	It shall offer an overview or inset		
6.	Collapsible Map Content (with layer switch on off)		
7.	Normal view & grid view (DD/DMS)		
8.	Supporting publishing of various Imageries, Raster & vector data formats		
9.	Online Dynamic legend creation for raster & vectors with proper labelling		
10.	Online Chart creation on attribute data & Analysis data generated Report Generation		
11.	Export to excel, pdf, doc formats		
12.	Geopdf creation		
13.	Map layout & printing (cartographic output)		
14.	provision of administrative data ingestion		
15.	GIS data download provision based on rights of user		

4.12 City Wi-Fi

4.12.1 Technical Specifications - Wireless Intrusion Prevention System

#	Minimum specification	Bidder compliance (Y/N)	Product Documentation Reference
1.	The WIPS system needs to have dedicated wireless security devices for monitoring the air space, detecting unauthorized connections and a centralized server that analyses the data received from Sensor		
2.	The sensor should be capable of handling wireless devices that are typically visible at a location in a large deployment (e.g., 200 to 500 APs, 200 to 500 clients)		
3.	The sensor should completely support the IEEE 802.11a/b/g/n technology and support both the 2.4 & 5.0 GHz bands		
4.	The communication between the sensor and WIPS server should be secure		
5.	The WIPS system should support centralized policy management		
6.	The WIPS system should support wireless LAN security policy definition		
7.	WIPS Server & Sensors should not require frequent signature updates		
8.	WIPS System should have zero-day attack detection and prevention capabilities		
9.	The WIPS system should be based on industry standards		
10.	The WIPS system should automatically detect & classify authorized NMC APs without any manual intervention		
11.	The WIPS system should support AP restriction by SSID, vendor type, protocol, encryption, authentication and the type of radio		
12.	The WIPS system server should be accessible from anywhere using a web browser and provide access restriction to particular computers [IP pools etc.]		
13.	The WIPS system should auto-classify APs as managed, external and rogue APs		
14.	The WIPS system should have the capability of auto-classifying Wi-Fi clients as authorized, guest, rogue or external in addition to manual classification w.r.t. NMC network		

#	Minimum specification	Bidder compliance (Y/N)	Product Documentation Reference
15.	The WIPS system should correctly detect Smart-devices connecting to NMC network and classify them as approved or unapproved.		
16.	The WIPS system should support automatic detection of whether an AP is ON or OFF the NMC wired network		
17.	Layer-2 unencrypted and Layer-2 encrypted (WEP, WPA and WPAv2)		
18.	Smartphones and other Wi-Fi enabled devices tethering when connected to NMC Backbone network		
19.	The WIPS system should detect miss configured authorized NMC APs		
20.	The WIPS system should detect NMC's wireless client connecting to an outside AP		
21.	The WIPS system should detect an outside client trying to connect to the NMC's WLAN		
22.	The WIPS system should detect an Ad hoc connection involving NMC authorized Wi-Fi devices		
23.	The WIPS system should detect masquerading attacks on both APs and clients(MAC spoofing attacks)		
24.	The WIPS system should detect Honey Pot (aka "Evil-Twin") attacks		
25.	The WIPS system should detect AP MAC spoofing attacks across multiple locations and VLANs		
26.	The WIPS system should detect Layer-2 based wireless Denial of Service (DoS) attacks on NMC WLAN		
27.	The WIPS system should have configurable intrusion alert severity levels		
28.	The WIPS system should support location tracking of a DoS attacker		
29.	The WIPS system should detect APs configured for multiple SSIDs		
30.	The WIPS system should be able to detect a NMC Client bridging its Wired and Wireless interfaces or participating in ICS		
31.	The WIPS system should be capable of automatic prevention		
32.	The WIPS system should prevent any Layer-2 based wireless Denial of Service (DoS) attacks		

#	Minimum specification	Bidder compliance (Y/N)	Product Documentation Reference
33.	The WIPS system should NOT affect the operation of an external (i.e. neighbours) or a managed access point while preventing a rogue AP on the same channel		
34.	The WIPS system should allow a manual override for Intrusion Prevention		
35.	A single sensor should simultaneously block any attacks and continue to scan/detect new vulnerabilities		
36.	The WIPS system should prevent aggressive client connections		
37.	A single sensor should simultaneously block multiple threats on multiple channels		
38.	The WIPS system should locate APs on live coverage maps		
39.	The WIPS system should locate clients (including ad hoc clients) on live coverage map		
40.	The WIPS system should provide notification mechanisms via email and Syslog messages for critical security breaches (i.e. a new rogue AP found)		
41.	The WIPS system should send notifications based on location and alarm type		
42.	The WIPS system should support addition of tags and notes to devices		
43.	The WIPS system support addition of acknowledgement notes to system alerts		
44.	The WIPS system should provide a device summary (for APs, sensors, and clients) report per location		
45.	The WIPS system should provide an event summary report		
46.	The WIPS system should categorize events by location (for ease of management)		
47.	The WIPS system should allow customization of existing reports and creation of new reports by end-user		
48.	Should Automatically blacklist clients based on DoS/MITM attacks		
49.	Should detect rough clients/ AP on Wired network by querying routers and switches		
50.	Should support for Off-channel rogue containment		
51.	Should support historic data retention		

#	Minimum specification	Bidder compliance (Y/N)	Product Document ation Reference
52.	Should provide Integrated PCI reports for easy auditing		
53.	Must support RFID asset tags for location tracking.		
54.	Should provide Open APIs / SDK for app development		
55.	Should be able to provide location accuracy within 3 meters without requiring any special client App.		
56.	Clients and tags should be tracked in indoor, indoor high-ceiling, and outdoor environments		
57.	The system shall offers analytic dashboard for guest access usage info		
58.	The system shall provide location Analytic service that provides real- time live analytic of demographic information		
59.	Analytics dashboard should provide real-time information on Wi-Fi client count and Client Dwell-Time		
60.	Should support creating logical zones within a venue to understand relative utilization of different areas and to identify trends such as foot traffic in different parts of a store		
61.	The WIPS system should provide a device summary (for APs, sensors, and clients) report per location		
62.	Historical data on the elements being tracked should be collected and stored for drawing up trends and faster troubleshooting		

4.12.2 Technical Specifications - Centralized Wi-Fi Management System

#	Minimum specification	Bidder compliance (Y/N)	Product Document ation Reference
1.	NMC proposes to procure a centralized authentication system for its proposed Wi-Fi network. The system shall authenticate the City WiFi users of NMC. The system shall also provide facilities like web self-care.		
2.	The system shall comply to the DoT guidelines regarding provision of Wi-Fi internet service under un-licensed frequency band		

#	Minimum specification	Bidder compliance (Y/N)	Product Documentation Reference
3.	The Solution Shall Support Captive portal having customizable GUI. This portal should be available to any client coming into the Wi-Fi zone of NMC		
4.	Captive portal shall allow local branding and content as per the location.		
5.	Solution shall be able to restrict the bandwidth as per the policies. Solution shall have configurable GUI for Policy management to differentiate location wise Bandwidth policies		
6.	The solution shall support Usage based as well as Time duration based accounting. It shall support real time disconnection on completion of allotted resources i.e. Time or Data		
7.	The solution shall support centralized server for User authentication		
8.	The application should be IPv4 and IPv6 compliant.		
9.	GUI based management console for system administration, policy / package creation, backup and restore accounting data, SMS gateway configuration etc.,		
10.	Tool for Troubleshooting and Health Diagnostic		
11.	Creation of batches in advance and activation upon first usage		
12.	Generation of report of usage and accounting, real time usage of USER as per the location.		
13.	Access Control List for different accounting and report related activities		
14.	Management of different Packages.		
15.	Centralized system shall available in Failover mode		
16.	Policy based access control for administrative activities		
17.	Login and session details, browsing history and audit trails		
18.	Creation of subscribers as per the required packages. Activation of subscribers as per the usage		
19.	Renewal / Registration of the subscriber.		
20.	Portal providing Self registration.		
21.	Creation of various packages		
22.	Real time accounting of the usage		
23.	Location wise usage and billing detail		
24.	It shall offer complete subscriber management features in Subscriber Management options which mainly focuses on creating, editing, updating,		

#	Minimum specification	Bidder compliance (Y/N)	Product Documentation Reference
	renewing, deleting, and managing of accounts for all subscribers.		
25.	It shall support multiple Login Controls		
26.	It shall support Guest Management.		
27.	It shall support bulk username and password creation		
28.	It shall support centralized Profile creation & Subscriber Provisioning		
29.	It shall support Web self-care for subscriber to track usage summary		
30.	It shall support different customer acquisition process for Public Wi-Fi users		
31.	It shall support time bound username & password generation for Wi-Fi users		
32.	It shall be able to bind the MAC of Wi-Fi users		
33.	It shall have centralized Database which enables administrator easily manage database from a single point in distributed Architecture		
34.	It shall allow administrator to define whether the subscriber has to be added to the existing customer database or added as a fresh customer. Multiple subscribers shall be added under same customer. Administrator can define the username & password by which the subscriber can login.		
35.	It shall allow administrator to lists down the complete subscriber list in the system and allows updating or modifying subscriber information as required.		
36.	Administrator can select the customer name from the list and update details.		
37.	The database for the system is to be provided by the vendor along with the required hardware, software, etc. to maintain logs as per TRAI guidelines issued time to time.		
38.	This shall work as interface between NMC and City Wi-Fi user. Any prospective user coming into NMC public hotspot shall be presented a webpage portal giving details of Wi-Fi services, tariffs and procedure to subscribe to the services.		
39.	Citizen should be able to make payment through this portal		
40.	The subscriber shall be able to check his Wi-Fi account details		
41.	Shall be able to change his password		

#	Minimum specification	Bidder compliance (Y/N)	Product Document ation Reference
42.	Shall be able to create new Wi-Fi accounts through Captive/Web portal		
43.	Shall be able to display the complete information includes IP address using which the subscriber logged in as well as the MAC address of the subscriber (if MAC binding option is selected).		
44.	For security reasons it shall suggest subscribers to regularly change or update their password.		
45.	It shall allow subscribers to update personal details and contact information		

4.12.3 Technical Specifications - WLAN Controller

#	Minimum specification	Bidder compliance (Y/N)	Product Document ation Reference
1.	Must be compliant with either IEEE CAPWAP controller-based or Autonomous based WLANs.		
2.	WLAN Controller should support minimum of 5000 Access points in a single chassis. If any OEM/Bidder can't provide WLAN controller to support 5000 AP in 2RU form factor, multiple controllers must be proposed to meet the requirement from day one. Proposed controller should support N+N redundancy from day one		
3.	Controller should be appliance based and must have at least 4 x 10Gbps of uplink interfaces.		
4.	Controller shall support 30000 concurrent sessions per chassis.		
5.	The controller shall support Cellular offload by PMIPv6/EoGRE tunneling to Mobile Core network		
6.	Solution shall support wireless IPS feature		
7.	Must have feature for stateful recovery without re-authentication of the client in the event of LAN and WLAN infrastructure disruption to deliver a non-stop client session		
8.	Controller should have hot-swappable redundant power supplies.		
9.	Must support an ability to dynamically adjust channel and power settings based on the RF environment.		
10.	Radio coverage algorithm must allow adjacent APs to operate on different channels, in order to		

#	Minimum specification	Bidder compliance (Y/N)	Product Documentation Reference
	maximize available bandwidth and avoid interference		
11.	Must have Automatic 802.11 interference detection, identification, classification, and mitigation		
12.	Must support coverage whole detection and correction that can be adjusted as per WLAN basis.		
13.	Must support RF Management with 20/40/80 MHz channels with 802.11a/b/g/n/ac		
14.	Solution should support L2 and L3 roaming of IPv6 clients		
15.	WLC should support IPv6 access control lists		
16.	WLC should support Guest-access functionality for IPv6 clients		
17.	Solution performance must remain the same if encryption is on or off for wireless SSIDs.		
18.	Should support ability to adjust Delivery Traffic Indicator Message (DTIM) or equivalent on a per WLAN basis to improve performance for latency sensitive applications		
19.	Should adhere to the strictest level of security standards, including 802.11i Wi-Fi Protected Access 2 (WPA2), WPA, Wired Equivalent Privacy (WEP), 802.1X with multiple Extensible Authentication Protocol (EAP) types, including Protected EAP (PEAP), EAP with Transport Layer Security (EAP- TLS), EAP with Tunnelled TLS (EAP-TTLS		
20.	Should support Management frame protection for the authentication of		
21.	802.11 management frames by the wireless network infrastructure and must support data plane encryption		
22.	The solution should support a capability to shun / block WLAN client in collaboration with wired IPS on detecting malicious client traffic.		
23.	Controller should have rogue AP detection, classification and automatic containment feature		
24.	Controller should be able to detect attacks like Broadcast de- authentication, NULL probe, from day one for all access points		
25.	Controller should have profiling of devices based on protocols like HTTP, DHCP and more to identify the end devices on the network		

#	Minimum specification	Bidder compliance (Y/N)	Product Documentation Reference
26.	Must be able to set a maximum per-user bandwidth limit on a per-SSID basis.		
27.	Must support user load balancing across Access Points.		
28.	Controller must provide Mesh capability for Mesh supported AP.		
29.	Must be able to dedicate APs to monitor-only for Intrusion Prevention Services.		
30.	Must support client roaming across controllers separated by a layer 3 routed boundary		
31.	Solution proposed must support clients roaming across at least 500 APs.		
32.	Must support AP over-the-air packet capture for export to a tool such as Wire shark.		
33.	Shall support the ability to classify over 20 different types of interference with in 5 to 30 seconds.		
34.	Should provide a snapshot of air quality in terms of the performance and impact of interference on the wireless network identifying the problem areas.		
35.	Should provide an Air Quality rating on a per- radio basis to help gauge the impact of interference on the network		
36.	Should provide real-time charts showing interferers per access point, on a per-radio, per-channel basis.		
37.	Should support encrypted mechanism to securely upload/download software images to and from wireless controllers		
38.	Must support 802.11e (WMM)		
39.	Shall able to prioritize all traffic such as (Data ,voice and video)		
40.	Solution shall integrate with existing firewall or DPI device for deep packet inspection		
41.	Should have rate limiting per user and per SSID basis for encrypted tunnel mode		
42.	To deliver optimal bandwidth usage, reliable multicast must use single session between AP and Wireless Controller.		
43.	Should support both centralized as well as distributed traffic forwarding architecture with L3 roaming support from day 1 as well as should be IPV6 ready from day one		
44.	WLC should support AC and DC powering options		

#	Minimum specification	Bidder compliance (Y/N)	Product Documentation Reference
45.	WLC should support AP License Migration from one WLC to another		
46.	Must support stateful switchover between active and standby controller in a sub second time frame.		
47.	Solution shall be proposed with complete feature set including licensed feature.		
48.	Should support visibility and control based on the type of applications and should provide access or deny or rate-limit.		
49.	Solution should have Deep Packet Inspection for Layer 4-7 traffic for user for all traffic across the network to analyses information about applications usage and prioritization		
50.	Should support AP Plug and Play (PnP) deployment with zero- configuration capability		
51.	Should support encrypted mechanism to securely upload/download software image to and from Wireless controller.		
52.	Should support minimum 4000 VLANs		
53.	Should support Hot Spot 2.0		
54.	Should support minimum 500 WLANs		
55.	Should support dynamic VLAN assignment		
56.	Should able to do dynamic channel bonding based on interference detected on particular channel.		
57.	Must support coverage hole detection and correction that can be adjusted on a per WLAN basis.		
58.	Should provide visibility to Network airtime in order to set the airtime policy enforcement		
59.	Must support dynamic Airtime allocation on per WLAN, per AP, Per AP group basis.		
60.	Should support web-based authentication to provide a browser-based environment to authenticate clients that do not support the IEEE 802.1X supplicant.		
61.	Should support port-based and SSID-based IEEE 802.1X authentication.		
62.	Should support MAC authentication to provide simple authentication based on a user's MAC address.		
63.	Should support Rogue AP detection, classification and standard WIPS signatures.		
64.	Should be able to exclude clients based on excessive/multiple authentication failure.		

4.12.4 Technical Specifications - Wireless Access Point

#	Minimum specification	Bidder compliance (Y/N)	Product Documentation Reference
1.	Must have a robust design for durability, without visible vents		
2.	Access points shall have an integrated in-built or external antenna (IP67). Dual band Internal / External antennas to support both the 2.4GHz and 5GHz operations simultaneously from single antenna.		
3.	The Wi-Fi access point shall be supplied with MIMO sectoral (120x30 degrees) or omni-directional antennas (in-built or external) as needed to meet the design requirements of the Project. It shall support multiple unique antenna patterns. The antennas shall have antenna gain required to support the coverage requirements of the Project.		
4.	Mounting kit should be from OEM which shall be used for mounting access point		
5.	Access point shall support pole, wall, and roof mounting options.		
6.	Access Points proposed must include radios for both 2.4 GHz and 5 GHz.		
7.	Must support 2X2 multiple-input multiple-output (MIMO) with TWO spatial streams		
8.	Must support simultaneous 802.11n on both the 2.4 GHz and 5 GHz radios.		
9.	Must support data rates upto 300 Mbps		
10.	Must support 40 MHz wide channels in 5 GHz and 20 MHz wide channel in 20 GHz		
11.	Must support unto 27dbm of transmit power in both 2.4Ghz and 5Ghz radios		
12.	The Wireless AP should have the technology to improve downlink performance.		
13.	The AP shall be able to load-balance between 2.4Ghz and 5Ghz band.		
14.	Must incorporate radio resource management for power, channel, no grey areas and performance optimization		
15.	Must have -93 dB or better Receiver Sensitivity.		
16.	The Wireless Backhaul shall operate in 5Ghz		
17.	Support Encrypted and authenticated connectivity between all backhaul components		
18.	Should have two RJ-45 auto-sensing 10/100/1000 Mbps port and a console port.		

#	Minimum specification	Bidder compliance (Y/N)	Product Documentation Reference
19.	Mesh should support QoS for voice over wireless.		
20.	Must support Proactive Key Caching and/or other methods for Fast Secure Roaming.		
21.	shall support 802.11w standard for communication between AP and controller		
22.	Should support locally-significant certificates on the APs using a Public Key Infrastructure (PKI).		
23.	Provision of Wireless IPS to filter malicious traffic		
24.	Access Points must support a distributed encryption/decryption model.		
25.	Access Points must support hardware based encryption		
26.	Must support the ability to serve clients and monitor the RF environment.		
27.	Must support 16 WLANs per AP for SSID deployment flexibility.		
28.	Must support telnet or SSH or console login to APs directly for troubleshooting flexibility.		
29.	Must support locking option for Theft Protection or equivalent		
30.	Proposed access point shall support MDO (Mobile Data offload)		
31.	Must support Power over Ethernet (802.3af) / 802.3at		
32.	shall have the support of 802.11e and WMM		
33.	Must support Reliable Multicast Video to maintain video quality		
34.	Must support QoS to prioritize video ,voice and Data traffic		
35.	Geographic orientation flexibility – tilt angle for pole, wall, and roof mounting units		
36.	The equipment shall support up to 100 MPH sustained winds &140 MPH wind gusts.		
37.	The Access point shall be IP67 certified. The quoted wireless Access point should be WPC – ETA approved.		
38.	The Access point shall be rated for operation over an ambient temperature range of 0o C to + 600 C		
39.	Should be able to support LTE & WiMAX Signal Rejection		
40.	Should be able to support PoE, DC powering option		
41.	Should support both centrally controlled mode (configured and updated via wireless controller)		

#	Minimum specification	Bidder compliance (Y/N)	Product Document ation Reference
	and autonomous mode (without controller) which is software selectable		
42.	Certified for interoperability with all IEEE 802.11a/b/g/n client devices.		

4.12.5 Technical Specifications - Ruggedised L2 PoE switch

#	Specifications	Bidder Compliance (Yes/No)	Product Documentation Reference
1.	Port Density & Redundancy: The switch should have at least 8 ports 10/100/1000TX PoE / PoE+(min. 8 Port IEEE802.3af Or 4 Port 802.3at) and with 2 100/1000x Fibre SFP / RJ45 ports and PoE Power will be min 120W		
2.	System Capacity: 16K MAC addresses		
3.	Performance: The switch should have min. 20 Gbps of switching capacity & min. 17 Mpps of forwarding rate		
4.	VLAN: Support for Port-based VLANs, 500 VLANs (IEEE 802.1Q), MAC-based VLANs, Port-based Private VLANs, IP subnet-based VLANs		
5.	Quality of Service: Support for Egress rate limiting, Eight egress queues per port, Voice VLAN, DSCP for IP-based QoS, Differentiated services architecture, IEEE 802.1p Class of Service with strict and weighted round Robin scheduling.		
6.	Multicast: Support for IGMPv1 and IGMPv2 snooping, Multicast groups 255, IGMPv2 snooping querier.		
7.	Management: Support for Telnet server, should have Console management port, Web GUI, HTTP, TFTP, SNMP V3, RMON 4 groups Stats, History, Alarms and Events, Event log, Auto config, MIB, SNTP or equivalent, sFlow or equivalent.		

#	Specifications	Bidder Compliance (Yes/No)	Product Documentation Reference
8.	Security: The switch should support TACACS+, RADIUS accounting and RADIUS client, IEEE 802.1x port-based Network Access Control (NAC), IEEE 802.1x multiple supplicant mode, EAP, EAP-TLS, LEAP, PEAP, TTLS, Per port MAC address filtering, Layer 2/3/4/ Access Control Lists (ACLs), SSL for Web management, Per port MAC address limiting, MAC address security/lockdown, Guest VLANs and SSH session, Time out.		
9.	Resiliency: IEEE 802.1D Spanning-Tree Protocol, IEEE 802.1D- RapidSpanning-Tree Protocol and IEEE802.1q-Multiple Spanning-Tree Protocol, BPDU guard, Loop guard and Root guard, 802.17 Ring protection technology or equivalent		
10.	Other Essential Feature: Support for IPv6 host, ICMPv6, IPv6 ACL, Dual-stack IPv4/IPv6 management, IPv6 applications WEB/SSL, Static IPv4 routing 4K, RIPv1,v2, Proxy ARP, IEEE 802.3ad, ICMP, LLDP, DHCP snooping, DHCP option 82, DHCP relay, ICMP. The switch should have ECO Friendly design and operation.		
11.	Power Characteristics: Voltage: 100-240V AC (10% auto-ranging), Frequency 47-63Hz Operating temperature: 0C to 65C Storage temperature: -25C to 70C Operating humidity: 5% to 90% non-condensing		
12.	Safety Certifications: EMI: FCC class A, CE, UL 60950-1, EN60950-1, EN60825 Etc and Compliant with RoHS standards, NEMA – TS2		
13	Ruggedness: The Layer 2 industrial grade switch (access switch) shall at a minimum carry IP30 rating		

5   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 size the hardware and software infrastructure requirement to meet the project objectives and SLA.

5.1   Pan City Network Backbone

#	Line Item	Unit of Measurement	Indicative quantity
1.	24 Core Optical Cable and required Access router, switches for last mile connectivity	KM	As required to cover pan city area including ABD
2.	Aggregate bandwidth at DC	Gbps	5
3.	Leased Circuit Bandwidth	1 Mbps	40
4.	Leased Circuit Bandwidth	2 Mbps	50
5.	Leased Circuit Bandwidth	5 Mbps	20
6.	Leased Circuit Bandwidth	10 Mbps	20
7.	Leased Circuit Bandwidth	20 Mbps	10

5.2   Command Control and Communication Centre

#	Line Item	Unit of Measurement	Indicative quantity
1.	Video wall (70" in 5x3 configuration)	Unit	1
2.	Video Wall Controller	No.	1
3.	Video Wall Management Software	No.	1
4.	Cabling & Other Fixtures	Lot	1
5.	Keyboard Joystick to control PTZ Cameras	No.	10
6.	Network Access Switch	No.	1
7.	LED TV 55"	No.	3
8.	Public Address System	Set	1
9.	Audio Mixer and speaker system	Set	1
10.	Workstation Desktop with two monitors	No.	20
11.	Online UPS (sizing as per proposed solution)	No.	As per requirement (in n + n fashion)
12.	Multifunction Device	No.	2
13.	IP Phones	Set	10
14.	Public Address System	Set	1
15.	Video Conferencing software and solution	Set	1
16.	Network Colour Laser printer	No.	1
17.	Network B/W Laser Printer	No.	2

#	Line Item	Unit of Measurement	Indicative quantity
18.	Network B/W Laser Printer (Heavy Duty)	No.	1
19.	Biometric access control system	No.	As per bidder's solution
20.	Dome cameras for internal surveillance	No.	12
21.	Fire Alarm System	Set	1
22.	Rodent Repellent system	Set	1
23.	Split Air Conditioner 2 Ton (5 star energy efficiency rating)	No.	As per requirement
24.	Site Preparation as per the RFP	Lump sum	1
25.	Workstation Furniture and Fixtures for C4	No.	20
26.	Revolving Chairs for office staff	No.	20
27.	Office Desk Furniture and Fixtures	No.	20
28.	Ergonomic Chairs for CCCC	No.	25
29.	Conference Table (for 10 personnel) & Chairs Set	Set	1
30.	Manpower – Operators	No.	30 in three shifts (shift distribution shall be decided by RSCCL)

5.3   Helpdesk

#	Line Item	Unit of Measurement	Indicative quantity
1.	Hand Set	No.	5
2.	Head Set	No.	5
3.	Voice Logger	No.	1
4.	Soft telephone	No.	5
5.	Desktops	No.	5
6.	Officer Furniture and Revolving Chair	Lot	5

5.4   Data Centre

#	Line Item	Unit of Measurement	Indicative quantity
	Core Infrastructure		
1.	Core Router	No.	2
2.	Core Switch	No.	2
3.	Internet Router	No.	1
4.	Firewall	No.	2
5.	IPS	No.	2
6.	Data Centre Switch	No.	As per requirement
7.	42U Network Rack	No.	As per requirement
8.	KVM Switch	No.	2
9.	Blade Chassis	No.	As per requirement
10.	Video Management Server	No.	4
11.	Video Analytics Server	No.	2
12.	Network Video Recorder	Lot	As per requirement
13.	ATCS Server	No.	2
14.	ANPR Server	No.	4
15.	RLVD Server	No.	4
16.	TARS server	No.	2
17.	Variable Message Signboard server	No.	2
18.	Smart Parking Information Management Solution Server	No.	2
19.	Environment Management server	No.	1
20.	City Wi-Fi Server	No.	2
21.	Wireless Intrusion Prevention System	No.	2
22.	Wi-Fi Controller	No.	2
23.	IVRS Server	No.	1
24.	CTI Server	No.	1
25.	Automatic Call Distributor Server	No.	1
26.	Digital Voice Logger Server	No.	1
27.	GIS server	No.	2
28.	Database Server	No.	4
29.	Web Server	No.	2
30.	Server Load Balancer	No.	2
31.	SAN Switch	No.	2
32.	Storage (Primary)	TB	300
33.	Storage (Secondary)	TB	500
34.	Tape Library	Lot	As per requirement
35.	Online UPS (sizing as per proposed solution)	No.	As per requirement (in n + n fashion)

Selection of Master System Integrator (MSI) for Implementation of Command Control and Communication Centre (C4) under Smart City Mission in Ranchi

#	Line Item	Unit of Measurement	Indicative quantity
36.	Precision Air Conditioning System for the Server Farm Area	No.	As per requirement (in n+1 fashion)
37.	Split Air Conditioner for the Auxiliary Area	No.	As per requirement
38.	Site Preparation Cost	Lump Sum	1
	Software Solutions		
39.	Server OS License	No.	As per requirement
40.	Database	Lot	1
41.	Web server	Lot	1
42.	Anti-virus & Anti-Spam software	Lot	1
43.	Backup software	Lot	1
44.	EMS	Lot	1
45.	Mail & Messaging Solution	Lot	1
46.	C4 core application	Lot	1
47.	SMS Gateway with annual 200,000 SMSs	Lot	1
48.	ITMS - ACTS Software	Lot	1
49.	ITMS - Video Management Software	Lot	1
50.	ITMS - Video Analytics Software	Lot	1
51.	ITMS - ANPR Software	Lot	1
52.	ITMS - RLVD Software	Lot	1
53.	ITMS - SVD software	Lot	1
54.	ITMS - TARS	Lot	1
55.	ITMS - PA Software	Lot	1
56.	ITMS - ECB management software	Lot	1
57.	ITMS - Variable Message Software	Lot	1
58.	Environment Management	Lot	1
59.	Smart Parking Management Information System	Lot	1
60.	Centralized Wi-Fi Management Solution	No.	1
61.	City Portal	Lot	1
62.	Mobile Application	Lot	1
63.	Enterprise GIS	Unit	1
64.	Automated Call Distribution Software	Lot	1
65.	Computer Telephony Integration Software	Lot	1
66.	IVR Software	Lot	1
	Bandwidth		

#	Line Item	Unit of Measurement	Indicative quantity
67.	Aggregate bandwidth at DC	Bandwidth	5 Gbps
68.	MPLS line between DC & Cloud DR	Bandwidth	As per requirement
69.	Leased circuit/bandwidth termination at field locations	Quantity	100
	Power Backup		
70.	Diesel Genset	Unit	1
	Manpower		
71.	System Administrator	No.	1
72.	Network Administrator	No.	1
73.	Database Administrator	No.	1

5.5 Data Recovery Centre

#	Line Item	Unit of Measurement	Indicative quantity
1.	Servers	No.	As per requirement
2.	Storage	No.	As per requirement
3.	Bandwidth	Mbps	As per requirement
4.	DC-DR license	Lot	As per requirement

5.6 City Wi-Fi – Field Equipment

#	Line Item	Unit of Measurement	Indicative quantity
1.	Access Point	No.	500
2.	Network Switch Ruggedised	No.	50
3.	Junction Box	No.	As per requirement
4.	Online UPS – 1 KVA (in case bidder proposes solar power, required items should be mentioned in the technical proposal)	No.	1
5.	Site Preparation Cost	Lump-sum	1

5.7 ITMS – Field Equipment

Total no. of locations across the city identified for implementing ITMS including ATCS, RLVD, ANPR, SVD, Surveillance, PA and ECB solution is around 50. An indicative Bill of Material required for undertaking initial stage of implementation is specified below.

Selection of Master System Integrator (MSI) for Implementation of Command Control and Communication Centre (C4) under Smart City Mission in Ranchi

#	Line Item	Unit of Measurement	Indicative quantity
1.	**ATCS**		
a.	ATCS Traffic signal controller	No.	40
b.	Vehicle Detection Camera	No.	150
c.	Countdown timer	No.	150
d.	Traffic Light Aspects – Red	No.	As per requirement
e.	Traffic Light Aspects – Green	No.	As per requirement
f.	Traffic Light Aspects – Amber	No.	As per requirement
g.	Pedestrian lamp heads – Stop	No.	As per requirement
h.	Pedestrian lamp heads – Walk	No.	As per requirement
i.	Gantry Pole including site preparation cost	No.	As per requirement
j.	Mounting Structure with poles, junction boxes	Set	As per requirement
k.	Network Switch Ruggedised	No.	As per requirement
2.	**RLVD**		
a.	Red Light Violation Detection (RLVD) sensors	Per leg	120
b.	Camera with ANPR capability	No.	120
c.	Local processing unit	No.	30
d.	Mounting structure with pole, junction boxes etc.	Set	As per requirement
e.	Network Switch Ruggedised	No.	As per requirement
f.	Overview camera	No.	120
3.	**SVD**		
a.	Speed Detection System for covering 2 lanes in one direction with complete subcomponents including ANPR camera, sensors, wide angle evidence camera, IR illuminator, non-intrusive speed sensor, with cabling & mounting infrastructure as required	Locations	10
4.	**Surveillance System**		
a.	Outdoor Fixed Box Camera + IR Illuminator	No.	80
b.	Outdoor PTZ Camera + IR Illuminator	No.	30
c.	ANPR Camera	No.	30

#	Line Item	Unit of Measurement	Indicative quantity
d.	Network Video Recorder	Lot	As per requirement
5.	**Traffic Accident Reporting System (TARS)**		
a.	Camera	No.	15
b.	Video Recorder	Lot	As per requirement
6.	**Public Address System**		
a.	Public Address System – IP based PA with speakers	No.	50
b.	UPS (required capacity)	No.	As per requirement
c.	Mounting structures with pole etc.	No.	As per requirement
7.	**Variable Message Sign**		
a.	Variable Message Sign Board	No.	50
b.	UPS (required capacity)	No.	As per requirement
c.	Mounting structures with pole etc.	No.	As per requirement
8.	**Emergency Call Box**		
a.	ECB system	No.	50
b.	UPS (required capacity)	No.	As per requirement
c.	Mounting structure with pole etc.	No.	As per requirement
9.	Junction boxes for ITMS solution	No.	As per requirement
10.	Power cables	Meter	As per requirement

5.8 Smart Parking – Field Equipment

#	Line Item	Unit of Measurement	Indicative quantity
1.	Camera Based Sensors parking sensors	No.	50
2.	Parking Information Management Software for On-Street parking	Lot	1
3.	Parking Mobile Application	Lot	1
4.	Network Switch	No.	As per requirement
5.	Pole including site preparation cost	No.	As per requirement
6.	Junction box	No.	As per requirement
7.	Site Preparation	Lump sum	1

5.9 Environment Sensors – Field Equipment

#	Line Item	Unit of Measurement	Indicative quantity
1.	Environment sensors	No.	15

6 Annexure II: C4 Design Consideration

6.1 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 RSCCL 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 RSCCL)

- API Approach- RSCCL has decided to adopt Open API as the guiding paradigm to achieve the above goals. Though RSCCL system would develop a portal but that would not be the only way for interacting with the RSCCL 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 RSCCL system. These applications will connect with the RSCCL system via secure RSCCL 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 RSCCL 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.

6.1.1 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.

RSCCL system will be built on the following core principles:

6.1.1.1 *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 C4 system is envisaged as a faceless system with 100% API driven architecture at the core of it. RSCCL 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.

6.1.1.2 *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.

6.1.1.3 *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.

6.1.1.4 *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.

6.1.1.5 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.

6.1.1.6 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.

6.1.1.7 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.

6.1.1.8 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

6.1.1.9 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 RSCCL system should be prevented

- Ensure minimum data loss (expected zero data loss)

6.1.1.10 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.

6.1.1.11 Availability

The solution design and deployment architecture will ensure that the application can be deployed in a centralized environment offering system High Availability and failover.

The solution should meet the following availability requirements

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

- Deployment of multiple application instances should be possible

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

- Network, DC, DR should be available 99.99 % time.

6.1.1.12 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.

6.1.1.13 Reconstruction of truth

System should not allow database/system administrators to make any changes to data. It should ensure that the data and file (data at rest) that is kept in the systems has tamper resistance capacity and source of truth (original data of invoices and final

returns) could be used to reconstruct derived data such as ledgers and system generated returns. System should be able to detect any data tampering through matching of hash value and should be able to reconstruct the truth.

- Services/solutions should be flexible and extensible to respond to, accommodate and adapt to changing business needs and unanticipated requirements easily. Consolidate and simplify technology applications wherever possible to minimize complexity. Ongoing application, database and server consolidation may be required.

- Software should use meta-data to configure itself (using declarations rather than coding).

- Avoid proprietary solutions and technologies if possible. Consider adhering to latest industry best practices and technical standards.

- The infrastructure should support an environment that allows applications to start small, grow quickly, and operate inexpensively. An adaptable infrastructure provides the capability to add to the current infrastructure with minimum inconvenience to the user.

- The IT architecture should be designed to support the overall SLA requirements around scalability, availability and performance.

- Each application should be performance tested to identify performance issues. The potential performance bottlenecks need to be identified and cost-effective paths for performance improvements should be provided for these identified problem areas.

- The system infrastructure should be architected considering failover requirements and should ensure that a single server or network link failure does not bring down the entire system.

- The system should be reliable handling every request and yield a response. It should handle error and exception conditions effectively

6.1.1.14 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 RSCCL 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 RSCCL 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 RSCCL solution will automate complex business processes or provide unified access to information that is scattered across many systems. Process Integration will provide a clean separation between the definition of the process in the process model, the execution of the process in the process manager, and the implementation of the individual functions in the applications. This separation will allow the application functions to be reused in many different processes.

An enterprise service bus (ESB) is a software architecture model used for designing and implementing the interaction and communication between mutually interacting software applications in Service Oriented Architecture. As software architecture model for distributed computing it is a variant of the more general client server software architecture model and promotes strictly asynchronous message oriented design for communication and interaction between applications. Its primary use is in Enterprise Application Integration of heterogeneous and complex landscapes. Following are the requirement for an ESB system:

- The solution should support static/deterministic routing, content-based routing, rules-based routing, and policy-based routing, as applicable in various business cases.

- The solution should have capabilities to receive input message in heterogeneous formats from various different systems, interpret those messages, process and transform those messages to generate output and feed them to various different

clients as per formats applicable.

- 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 RSCCL, 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 antispam 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 RSCCL. 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:

- o Interface Definition
- o Interface Owner
- o Interface Type
- o Interface Format
- o Frequency
- o Source System
- o API/Service/Store Procedure
- o Entitlement Service
- o Consuming System
- o 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

6.2 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 GoJ/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.

6.2.1 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

6.2.1.1 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.

6.2.1.2 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

6.2.2 Data Security

6.2.2.1 Traditional Structured Enterprise Data

RSCCL 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 RSCCL 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 RSCCL 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.

6.2.2.2 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.

6.2.3 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.

- 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.

6.2.4 Infrastructure Security

The following focused initiatives to discover and remedy security vulnerabilities of the IT systems of RSCCL 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.

6.2.4.1 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

6.3 Software Development Lifecycle Continuous Build

The Ranchi 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.

6.4 Quality Assurance

A thorough quality check is proposed for the Ranchi 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 RSCCL. 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 RSCCL that all applications installed in the system have been tested.

6.5 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 Ranchi 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 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. MSI should ensure that only one make and model is proposed for one component in Technical Bid for example all Field cameras must belong to a single OEM and must be of the same model etc.

8. MSIs should ensure complete warranty and support for all equipment from OEMs. All the back-to-back service agreements should be submitted along with the Technical Bid.

9. **All equipment, parts should be original and new.**

10. The user interface of the system should be a user friendly Graphical User Interface (GUI).

11. Critical core components of the system should not have any requirements to have proprietary platforms and should conform to open standards.

12. For custom made modules, industry standards and norms should be adhered to for coding during application development to make debugging and maintenance easier. Object oriented programming methodology must be followed to facilitate sharing, componentizing and multiple-use of standard code. Before hosting the application, it shall be subjected to application security audit (by any of the CERTIN empaneled vendors) to ensure that the application is free from any vulnerability; and approved by the RSCCL.

13. All the Clients Machines / Servers shall support static assigned IP addresses or shall obtain IP addresses from a DNS/DHCP server.

14. The Successful MSI should also propose the specifications of any additional servers / other hardware, if required for the system.

15. The indicative architecture of the system is given in this volume. The Successful MSI must provide the architecture of the solution it is proposing.

16. The system servers and software applications will be hosted in Data Centers as specified in the Bid. It is important that the entire set of Data Centre equipment are in safe custody and have access from only the authorized personnel and should be in line with the requirements& SLAs defined in the Tender.

17. The Servers provided should meet industry standard performance parameters (such as CPU Utilisation of 60 percent or less, disk utilisation of 75 percent or less). In case any non- standard computing environment is proposed (such as cloud), detail clarification needs to be provided in form of supporting documents, to confirm (a) how the sizing has been arrived at and (b) how SLAs would be met.

18. MSI is required to ensure that there is no choking point / bottleneck anywhere in the system (end-to-end) and enforce performance and adherence to SLAs. SLA reports must be submitted as specified in the Bid without fail.

19. All the hardware and software supplied should be from the reputed Original Equipment Manufacturers (OEMs). RSCCL reserves the right to ask replacement of any hardware / software if it is not from a reputed brand and conforms to all the requirements specified in the tender documents.

20. All proposed servers, active networking components, security equipment, storage systems and COTS Application should be from OEMs who are top supplier in the market.

21. Cameras, Network Video Recorder (NVR) and the Video Management / Video Analytics Software should be ONVIF Core Specification '2.X' or 'S' compliant and provide support for ONVIF profiles such as Streaming, Storage, Recording, Playback, and Access Control.

22. MSI shall place orders on various OEMs directly and not through any sub-contractor / partner. All licenses should be in the name of the RSCCL.

8 Annexure IV- Tentative List of Locations

Tentative List of Wi-Fi Hot Spots

#	List of Locations
1	Doranda College
2	Employment Exchange
3	Hinoo Chowk
4	Indira Palace
5	Jail Chowk / JPSC
6	Kutchery Chowk
7	MECON/ Vivekanand Chowk
8	Opp RWC Hostel
9	Post Office, Doranda/ Van Bhawan
10	Ranchi Women's College
11	Ratu Rd stop (Near Rajbhavan)
12	Shree Krishna Park
13	Sai Mandir/ HDFC Bank
14	Birsa Munda bus stand, Khadgada
15	Gossner College
16	Pahari Mandir
17	Near Tagore Hill (Morhabadi area)
18	Science Centre, Chiraundi
19	Near RIMS
20	Bariatu Housing Colony
21	Harmu Housing Colony
22	Sidhu Kanhu Park
23	Near Ranchi College & surrounding Parks at Morhabadi Area
24	Nakshatra Van
25	Kanke Dam Park
26	Aqua World
27	Rock Garden
28	Near Gandhi Nagar Colony
29	Birsa Smiriti Park
30	Park near Ashok Nagar Road No. 3
31	Singh More
32	NIFFT Gate
33	Near Argora Maidan
34	Ranchi Municipal Corporation
35	XISS
36	Albert Ekka Chowk
37	Near Sadar Hospital and St. Xavier's College
38	Lalpur Chowk near BIT Lalpur

#	List of Locations
39	Chandni Chowk, Kanke Road
40	GEL Church Complex
41	Daily Market
42	Near Main Road Gurudwara
43	Ranchi Club Complex

RSSCL may modify the list of locations and make addition to or deletion from the list of locations mentioned above.

End of Document