RFP No. BSCDCL/xx

April 2017

SMART CITY BHOPAL

BHOPAL SMART CITY
DEVELOPMENT CORPORATION LIMITED

REQUEST FOR PROPOSAL

Selection of Master System Integrator for providing a Cloud based Common Integrated Data Centre & Disaster Recovery Centre and establish City Integrated Command and Control Centers for the Smart Cities of Madhya Pradesh

Important Dates

S. No.	Activity	Deadline
1	Release of RFP	18 Apr 2017
2	Last date of receipt of queries on RFP	28 Apr 2017
3	Pre-bid Meeting date	05 May 2017
4	Posting of response to queries	12 May 2017
5	Last date for submission of Bids	30 May 2017 (online) 31 May 2017 (hardcopy)
6	Date of opening of technical bids	01 Jun 2017
7	Date of Presentation of Solution and Approach and Methodology	To be intimated later to successful bidder
8	Date of opening of Commercial bids	To be intimated later to successful bidder

Table of Contents

Definitions/Acronyms

Sr. No.	Abbreviation	Description
1.	**ACD**	Automatic Call Distributor
2.	**AHU**	Air Handling Unit
3.	**BAS**	Building Automation System
4.	**BOM**	Bills of Material
5.	**BoQ**	Bills of Quantity
6.	**BCLL**	Bhopal Link Limited
7.	**BSCDCL**	Bhopal Smart City Development Corporation Limited
8.	**BMC**	Bhopal Municipal Corporation
9.	**CCC**	Command and Control Centre
10.	**CCA**	Command and Control Application
11.	**ICCC**	Integrated Control and Command Center
12.	**CCTV**	Close Circuit Television
13.	**CCDCSC**	Common Cloud Based Data Center for Smart Cities
14.	**CERTIN**	Indian Computer Emergency Response Team
15.	**BEB**	Bhopal Electricity Board
16.	**DFMD**	Door Frame Metal Detector
17.	**DHCP**	Dynamic Host Configuration Protocol
18.	**DMS**	Distribution Management System
19.	**DNS**	Domain Name Server
20.	**EMS**	Employee Monitoring System
21.	**ERP**	Enterprise Resource Planning
22.	**ESS**	Employee Self Service
23.	**FMS**	Facility Management Service
24.	**FRS**	Functional Requirement Specification
25.	**GIS**	Geographical Information System
26.	**GOI**	Government of India
27.	**GoMP**	Government of Madhya Pradesh
28.	**HVAC**	Heating, ventilation and air conditioning
29.	**IBMS**	Integrated Building Management System
30.	**ICT**	Information and Communication Technology
31.	**IED**	Intelligent Electronic Device
32.	**IEEE**	Institute of Electrical and Electronics Engineers
33.	**IT**	Information Technology
34.	**ITMS**	Intelligent Transport Management System
35.	**KPI**	Key Performance indicators
36.	**LDAP**	Lightweight Directory Access Protocol
37.	**LUN**	Logical Unit Number
38.	**MPLS**	Multiprotocol Label Switching
39.	**MPUADD**	Madhya Pradesh Urban Administration and Development Department
40.	**MSA**	Master Service Agreement

41.	**MSI**	Master System Integrator
42.	**MSI**	Master Service Integrator
43.	**MTBF**	Mean Time Between Failures
44.	**MW**	Mega Watt
45.	**NOC**	Network Operation Centre
46.	**OEM**	Original Equipment Manufacturer
47.	**OFC**	Optical Fiber Cable
48.	**OWASP**	Open Web Application Security Project
49.	**PABX**	private automatic branch exchange
50.	**RAID**	Redundant Array of Inexpensive Disks
51.	**RTU**	Remote Terminal Unit
52.	**SAN**	Storage Area Network
53.	**SCADA**	Supervisory Control and Data Acquisition
54.	**SDC**	State Data Centre
55.	**SITC**	Supply Installation Testing and Commissioning
56.	**SLA**	Service Level Agreement
57.	**SNMP**	Simple Network Management Protocol
58.	**SPV**	Special Purpose Vehicle
59.	**SRS**	Software Require Specification
60.	**SSL**	Secure Sockets Layer
61.	**STQC**	Standard, Testing and Quality Certification
62.	**UAT**	User Acceptance Testing
63.	**UADD**	Urban Administration and Development Department
64.	**VLAN**	Virtual Local Area Network
65.	**VM**	Virtual Machine
66.	**DMZ**	De- Militarized Zone

1. Introduction

1.1 Bidding Data Sheet

Particulars	Details
Name of Purchaser	Bhopal Smart City Development Corporation Limited (BSCDCL) (on Behalf of Smart Cities of the State of MP)
Name of the Engagement	Selection of Master System Integrator for providing a Cloud based Common Integrated Data Centre & Disaster Recovery Centre and establish City Integrated Command and Control Centers for the Smart Cities of Madhya Pradesh
Release Date of RFP by BSCDCL	18/04/2017
Last date & time for purchase of RFP Documents	30/05/2017 by 05:00 pm
Last date & time for submission of Pre-Bid Queries	28/04/2017 by 5:30 pm
Pre-Bid Meeting	05/05/2017 at 11.00am Parishad Bhawan, ISBT, Bhopal Madhya Pradesh- 462023
Publish response to pre-bid queries	12/05/2017
Last date (deadline) for submission of the bid (online as well as hardcopy submission)	30/05/2017 05:30 pm (online) 31/05/2017 05:30 pm (hardcopy)
Opening of the Bid responses	01/06/2017 02:00 pm
Opening of Technical Bids	Will be intimated to successful bidders later
Presentation by Bidders	Will be intimated to successful bidders later
Opening of Commercial Bids	Will be intimated to successful bidders later
Validity of Proposal	Proposals must remain valid 180 days after the Submission date.
Method of Selection	The method of selection is Quality and Cost Based Selection Method (QCBS). The weights given to Technical and Financial proposals are: Technical = 80% and Financial = 20%

Particulars	Details
	The Contract will be awarded to the bidder evaluated with the highest overall score (combined Technical and Financial).
Address of Communication	To, The Chief Executive Officer Bhopal Smart City Development Corporation Limited (BSCDCL), Zone-14, Bhopal Municipal Corporation, BHEL, Govindpura, Bhopal -462023 Phone-0755- 2477770 Email - smartcitycell@bmconline.gov.in
Bidding in Consortium	Consortium of up to 3 members including Lead Bidder is allowed (Lead Bidder and 2 Consortium Partner) The lead bidder shall be jointly & severally responsible for complete scope, whereas partner/s shall be severally responsible only for its/their respective scope. The bid should contain details of all the members of the consortium including their legal status and specify their roles and responsibilities in the project. The members of the consortium shall enter into an Agreement for the purpose of submitting the proposal and the same shall be submitted with the proposal, failing which bid will be summarily rejected. The MSI or a member of a consortium is not allowed to participate in more than one bid. Otherwise, such bids shall stand cancelled.
Sub-Contracting	• Limited sub-contracting is allowed for outdoor activities such as fibre laying, camera installation, network provisioning, mechanical and civil work as required in the project. • Bidder needs to mention details of any sub-contracting proposed in the bid along with name of sub-contractor and activity assigned. Any change in sub-contractor at later date will be allowed only after approval of BSCDCL.
Tender Fees	INR 50, 00,000/- (Indian Rupees fifty thousand only) To be submitted online on www.mpeproc.gov.in website

Particulars	Details
Earnest Money Deposit / Bid Security	INR 5,00,00,000/- (India Rupees five Crores only) To be submitted online through www.mpeproc.gov.in website or via Bank Guarantee

Note

1. The date of opening of the commercial bids will be intimated to the qualified Bidders through email or Telephone.
2. BSCDCL reserves the right to change any schedule of bidding process.

1.2 Objective of the RFP

Government of Madhya Pradesh has embarked on an ambitious journey of developing various cities of the state as Smart Cities. This initiative includes 07 cities identified as part of the Smart City Mission of Government of India and state identified cities over and above these 07 cities. The 07 cities selected/planned to be selected as part of Smart City Mission and as part of this RFP are –

- Already Selected – Indore, Bhopal, Jabalpur, Ujjain and Gwalior
- Planned – Sagar and Satna

Through this RFP, BSCDCL intends to select a Master System Integrator (MSI) by following competitive bidding process to design, develop, implement, operate and maintain:

- A Cloud based Data Centre for all 07 smart cities of the state
- A Cloud based Disaster Recovery Centre for all 07 smart cities of the state
- the Integrated Control and Command Centre (ICCC) at each of the 07 cities with city based controls and analytics

It is planned that the selected MSI shall achieve a stage of Go-Live for Cloud based DC and DR within 60 days of start of the project and city ICCC for 05 identified cities as Phase I within 240 days.

The MSI is proposed to be selected for a period of 05 years (after Go-Live on a turnkey basis. Contract may be further extended after completion of 5 years of O&M period on yearly basis for next 3 years. This extension will depend on the past performance of MSI and approval of BSCDCL. Extensions may be granted with escalation of 10% on the average prices quoted for O&M of 5 years for 6th Year. 7th year onwards price will be escalated by 10% each previous year.

The scope may be expanded to include more cities by the state in future or during the project period.

A MoU has been signed between Smart Cities by the CEOs of the respective smart cities to give authority to BSCDCL to get this project developed and implemented. BSCDCL will be responsible to float RFP for this project, do the bid process management, get the MSI on-board and manage operations of this project

As per the MoU and on behalf of other Smart Cities, BSCDCL is publishing this RFP.
Bidders are expected to carefully read the contents of RFP. For reference purposes, wherever BSCDCL name appears, it shall be read as “on behalf of all Smart Cities of the State of MP” except, where specific examples from Bhopal Smart City are mentioned.

This document contains the following details:

a. Schedule 1 – Instruction to Bidders
b. Schedule 2 – Detailed Scope of Work
c. Schedule 3 – General Conditions of the Contract & Service Level Agreements
d. Schedule 4 – Annexures

This RFP document provides a high-level overview of the technology approach for setting up a Cloud based common DC/DR for the state and a City based ICCC and includes in-depth details of the functional roles of system components, and the interactions between roles, to achieve an end-to-end system design.

The Common Cloud based Data Centre for Smart Cities (CCDCSC) shall be a common cloud based data centre for management of operation of the currently identified 07 smart city of the state. The city specific

ICCC will be helpful in managing the Smart City Operations and emergency response in respective cities. The hosting of all applications and database will be done at cloud and DR will also be cloud based.

1.3 Project Vision

The Madhya Pradesh Urban Administration and Development Department (MPUADD) has envisaged to establish Common Cloud based Data Centre for Smart Cities (CCDCSC) and Integrated City Command and Control Centre (ICCC) for each city to run city operations for 7 cities. This will be used for making cities smarter in terms of managing operations of the smart components deployed across the cities. This will finally benefit citizens of smart cities within the state of Madhya Pradesh using ICT as backbone and seamless integration with all the required & existing ICT systems / Smart components. The common CCDCSC is planned considering the optimal usage of resources of all the 7 cities.

CCDCSC will be a common platform where all the information from various sources like city operation centers and applications will be stored. All the information collected here, will be analyzed for better planning of the smart cities using integrated analytical layer / BI engine. These insights / trends will be helpful in managing incidents across the state and individual city and do a better planning for the development and delivery of smart city projects.

CCDCSC will be cloud based Data Center based out of any location within India. It will host common command center application platform for all 7 cities. It will also host other common applications like integrated analytical layer / BI engine. Eventually all the smart components / applications deployed in the cities will be integrated with the common platform layer for managing smart city operations.

CCDCSC will eventually become single source of truth for all the 7 cities and its operations. It will help ICCC of each smart city to make it happy and livable place for its citizens.

CCDCSC is required to be scalable for hosting more applications and services in future for managing smart cities more effectively.

CCDCSC will help in managing the utilities for ABD areas of smart cities and in future capable of managing utilities of the entire cities through city ICCC.

For seamless operations of CCDCSC, it will also have cloud based DR. This DR is also required to be located in India and better seismic zone than Data Center.

The Common Cloud based Data Center for Smart Cities (CCDCSC) and DR Facility for running the desired operations should be currently operational and have a minimum capacity of 100 Racks owned or contracted.

The Cloud based Data Center Facility to be used for making CCDCSC and DR for high quality shall at a minimum have:

- Conform to at least Tier III standard, certified under TIA 942 or Uptime Institute certifications by a 3rd party
- Cloud platform should be certified for the latest version of ISO 27001 (year 2013) including ISO 27018, by a competent auditing authority
- Cloud platform should be certified for Payment Card Industry Data Security Standards
- Reports of periodic third party inspections/audits and the certifications should be available online or shared on demand for scrutiny.
- Compliant with IT Act 2000 (including 43A) and amendments thereof

Each ICCC for the smart cities will have 70" inches diagonal cubes for Video wall with native resolution of each Visual Display Unit / Rear Projection Module should be 1920 X 1080 pixels (Full HD) and should offer min 16.7 million colors and controller system.

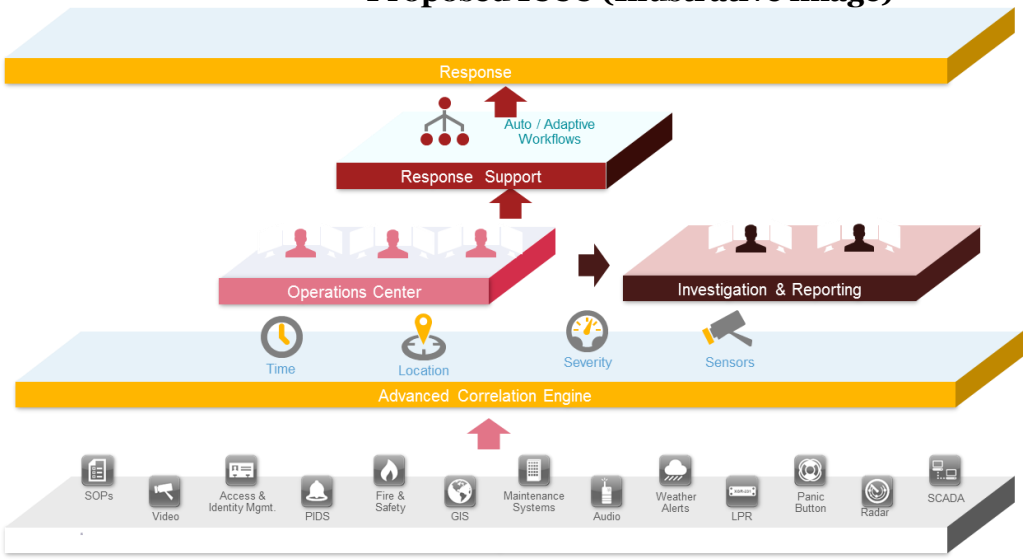
Each ICCC for the smart cities will have technical and non-technical support teams along with dedicated operators and helpdesk for cities to manage operations of the city command center and integration with CCDCSC.

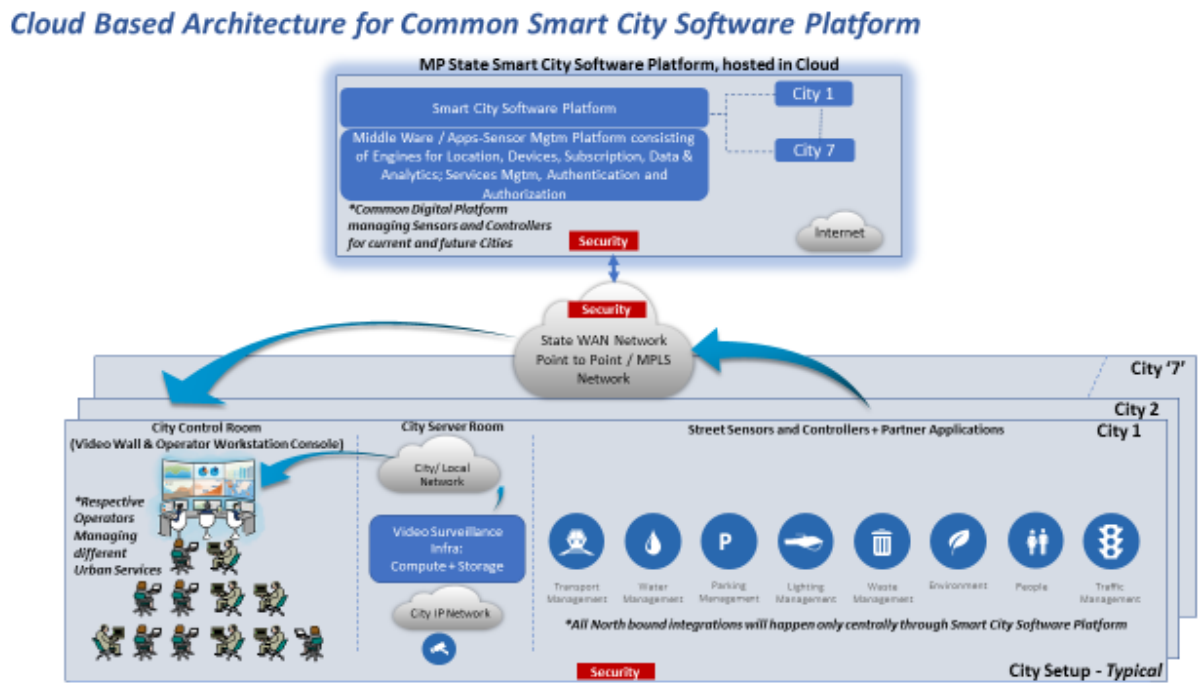
Each ICCC for the smart cities will have, on basis of city SPV requirements, a local server room for storing specific data at local level like video feeds, with minimum required infrastructure. Video feeds received from various sources will not be hosted on CCDCSC. Hosting video feeds on common cloud would require very heavy bandwidth and storage requirement, which becomes very expensive. Hence it is recommended to store such feeds locally in each ICCC.

The ICCCs for smart cities will have a situation room, to manage incidents very effectively.

Each ICCC in the State for smart cities will have physical capacity for future activities like expansion of services and its infrastructure based on the agreed plans between city SPV and implementing agency.

Proposed ICCC (Illustrative image)





1.4 Project Objectives

The primary objective of the establishing a cloud based state level integrated data centre, disaster recovery centre and integrated command and control centre for all the seven smart cities to provide better services to citizens with a view to improve the quality of life. The objective of establishing CCDCSC and ICCC is to implement holistic and integrated solution for multiple (existing and future) IT initiative for Smart Cities in MP. The IT initiative may of any department like eNagarpalika system, Safe city (CCTV surveillance) and DIAL 100 of police department, DIAL 108 of health department or network of Municipal Corporations. The end objective of establishing CCDCSC and ICCC is to drive the actions by each city authorities for their respective cities.

State plans to select an agency to be the Master System Integrator for providing a Cloud based Common Integrated Data Centre & Disaster Recovery Centre and establish & operate/maintain City Integrated Command and Control Centers for the Smart Cities of Madhya Pradesh. It will have following components:

- Common Cloud based DC and DR for the State
    - Availability of "IT infrastructure on demand" for hosting Smart City Applications
    - Aggregation of IT infrastructure (Hardware, Storage and Networking) and management resources
    - Optimal utilization by sharing of IT infrastructure resources to meet individual peak loads
    - Standardization of systems: Auto-scalability, Faster implementation cycle time and Stable and predictable physical and technical environment
    - Reduced administrative burden for each city SPV of smart city and urban Development Department by avoiding necessity of procurement, vendor management, addressing the technical issues etc.

    - Reduced cost of infrastructure creation, monitoring, management for each city SPV.
    - Enhanced reliability and security of information system through centralized management of IT infrastructure by adopting the necessary measures and practices, such as
        - Dynamic Scalability
        - Centralized and simplified management
        - Improved quality of data management
        - Lower risk of data loss
        - Higher availability of system and data – 24x7x365
        - Better management of security and access control
        - Guaranteed service levels
    - Efficient and effective management of information security issues across cloud environment
- A State level common integrated platform on Cloud for city ICCC
- State level Analytical Platform on Cloud for city ICCC
- City level ICCC for each Smart City
    - Video Wall
    - Operators
    - Technical Support Team
    - Local Server room for video storage at ICCC connected with cloud based DC and DR

State envisions the planned CCDCSC and ICCC to fulfil following objectives:

- "Single source of truth" for the city's civic functions
- Platform with the ability to receive, intelligently correlate & share information to better predict outcomes
- Act as City's emergency and disaster management platform
- Ability to integrate multiple text, voice, data, video and smart sensors communication interfaces
- Ability to integrate and correlate online and offline interactions
- Capabilities to support GIS based incidents visualization
- Future proof - based on Modular, Open, Configurable architecture with capabilities to integrate innovative new applications
- Intelligent and Intuitive work-flow management
- Advanced historical records management and archiving capabilities
- Advanced industrial grade cybersecurity features

Integration of various IT systems of different stakeholders with the objective of enhancing safety, security and providing better public services in the cities will help in following:

- To provide assistance to citizen at the time of emergencies
- To provide facilities of Ambulance, Police Van, Fire Brigade to the citizens
- To effectively manage Traffic and Roads and support police to maintain Law and Order
- Disaster Management
- Environmental Control/ Pollution Control
- Efficient user of public resources like electricity and water
- Efficient and timely delivery of public services
- Better health and education services

1.5 Phase wise envisaged activities of CCDCSC and city ICCC

The overall implementation of the project is divided in three main phases:

- Pre-Implementation Phase
- Implementation Phase
    - Phase I – Implementation of Common Cloud based DC and DR for all 07 cities and ICCC for 05 cities – Indore, Bhopal, Jabalpur, Ujjain and Gwalior
    - Phase II – Implementation of ICCC for 02 cities (Sagar and Satna) and their integration with DC and DR
- Post Implementation Phase

Pre –Implementation Phase:

Common Cloud based Data Center for Smart Cities (CCDCSC) and common DR

- Conduct the minimum level of sizing for CCDCSC and its DR required for hosting of common smart city command center application, common integrated analytical layer, and other common applications like Enterprise Management System (EMS), Backup / Archival / Replication Software, Deduplication system, Firewall, Anti-virus, Information security layer, Virtualization layer, etc.
- Develop and submit SRS and FRS for the CCDCSC and common DR to BSCDCL for review and approval.
- Develop SOPs of integration of city applications with CCDCSC and common DR

City ICCC

- Conducting site survey, obtaining necessary permissions, developing system requirements, standard operating procedures etc.
- Providing physical layout of the each city ICCC (with 3D simulation) with approximately minimum area of 10,000 square feet* of floor area. The floor area may be increased if required, but all the facilities and components of ICCC will remain as mentioned below. There will be no additional cost for layout design for more than 10,000 square feet floor area. This layout must contain the following:
    - Control and Command Setup Room
        - 2 Video walls of 6*3 (70 inches each)
        - Seating capacity of 30 operators
    - Local Server Room
    - Situation Room
    - Office Setup for City SPV, Municipal Corporation and MSI
        - At least 5 cabins for City SPV, Municipal Corporation (with seating capacity of 4 – 5 personal)
        - At least 3 meeting rooms (with furniture and fixtures)

        - One Conference Room with seating capacity of 20-30 personals (with video conferencing facility, furniture and fixtures)
    - Pantry / Common Area (with adequate capacity)
    - Restroom facilities (separate for Male & Female) with adequate capacity
    - Fire Escape & Evacuation Facilities (ISO 23601)
    - Other facilities which will be required for specially abled people as per guidelines defined by Govt. of India
- Assessment of physical security, housekeeping, waste management requirements for each ICCC premises.
- Assessment of IT Infrastructure and Non IT Infrastructure requirements, assessment of business processes, assessment of software requirements, assessment of integration requirement, assessment of connectivity requirement all locations (including buildings).
- Assessment of local server room sizing in terms of required storage, and related systems.
- Formulation of solution architecture, detailed design of smart city solutions, development of test cases (Unit, System Integration and User Acceptance), SoP documentation.
- Standard Operating Procedures (SoPs) must adhere with the Governance structure of City SPV and different Municipal Corporations of the 07 smart cities, as in case of any incident or disaster decision making ability lies with the Authority.
- Submit Monthly Progress reports as per the defined format to City SPV along with invoices.
- Submit Joint Monthly Progress reports of all cities after approval as per the format defined to BSCDCL along monthly progress report on common cloud based DC and DR along with total invoices.

**** These requirement may undergo certain changes to suit local requirements at city level. City SPV shall be the deciding authority for specific city based design and implementation plan for its ICCC, based on the overall requirements laid down in this RFP document. For reference - In case of Indore it will be over an area of approximately 5000 square feet and accordingly requirement of ICCC layout, Video walls and operators seating/numbers may also change.***

Implementation Phase:

Phase I - Implementation of Common Cloud based DC and DR for all 07 cities and ICCC for 05 cities – Indore, Bhopal, Jabalpur, Ujjain and Gwalior

Common Cloud based Data Center for Smart Cities (CCDCSC) and common DR

- Implementation of common applications on CCDCSC and integration with common DR as per the agreed FRS, SRS and SOPs.
- Creation of city specific interface for accessing the common applications.
- Integration of city specific applications with common command center platform.
- Facilitating user acceptance testing and conducting the pre-launch security audit of applications
- Develop provisions for a scalable system which can integrate with more devices of the same kind (as those deployed today) and can integrate with future applications and sensors through open standards and data exchange mechanisms.

City ICCC

- Physical Setup of ICCC in the respective smart cities as per the layout agreed with the City SPV. This includes activities like false flooring, false ceiling, partitions, network cabling, electric fitting, establishment of office spaces (as required), meeting rooms, conference rooms (with video conferencing facility), local server room, Inline UPS, DG Set, Auto on-off lighting system and other facilities as mentioned above along with required furnishing of the complete CCDCSC facility.
- Local Helpdesk setup, procurement of equipment, edge devices, COTS software (if any), licenses.
- IT and Non IT Infrastructure installation, development, testing and production environment setup
- Safety and security of IT and Non IT Infrastructure is responsibility of MSI
- Housekeeping facility for ICCCs.
- Software Application customization (if any), data migration, integration with third party services/application (if any)
- Preparation of User Manuals , training curriculum and training materials
- Role based training(s) on the Smart City Solutions
- SoP implementation, Integration with City GIS Platform, Integration of solutions with Command and Control Centre
- Network connectivity establishment and configuration between CCDCSC, City ICCC and various other city command centers / applications (which are to be integrated with CCDCSC and City ICCC).
- User training and roll-out of solution
- Integration of the various services & solution with CCDCSC and ICCC platform
- Submit Monthly Progress reports as per the defined format to City SPV along with invoices.
- Submit Joint Monthly Progress reports of all cities after approval as per the format defined to BSCDCL along monthly progress report on common cloud based DC and DR along with total invoices.

Phase II - Implementation of ICCC for 02 cities (Sagar and Satna) and their integration with DC and DR

Common Cloud based Data Center for Smart Cities (CCDCSC) and common DR

- Integration of city specific applications with common command center platform.
- Facilitating user acceptance testing and conducting the pre-launch security audit of applications
- Develop provisions for a scalable system which can integrate with more devices of the same kind (as those deployed today) and can integrate with future applications and sensors through open standards and data exchange mechanisms

City ICCC

- Similar steps which were taken in case of Phase I as mentioned above.

Post Implementation Scope for the Operation and Maintenance Phase:

Common Cloud based Data Center for Smart Cities (CCDCSC) and common DR

- Operations and maintenance of Common Cloud based Data Center for Smart Cities (CCDCSC) and common DR facility.
- Annual technical support for all hardware and software components for the O & M period.
- Conducting disaster recovery site testing through regular mock drills
- Overall maintenance of the CCDCSC facility and continuity of operations as per SLAs.

City ICCC

- Deploying manpower at city level for solution maintenance and monitoring support which includes change request management, bug tracking and resolution, production support, performing version and patch updates
- Annual technical support for all hardware and software components for the O & M period.
- Preventive, repair maintenance and replacement of hardware and software components as applicable under the warranty and AMC services during the contract period
- Provide a Helpdesk and Incident Management Support at city level till the end of contractual period
- Recurring refresher trainings for the users and Change Management activities
- Provide facility, information and required access to BSCDCL / Municipal Corporation / Smart City SPV or its authorized agency for doing various kinds of Audits as and when required.
- Preventive, repair maintenance and replacement of non ICT components as applicable under the warranty and AMC services during the contract period.
- Network connectivity maintenance between CCDCSC and various other command centers / applications (which are to be integrated with CCDCSC).
- Overall maintenance of the ICCC facility and continuity of operations as per SLAs.
- For continuity of operations all cost (Bills) pertaining to power, water, and telephone and internet connectivity for ICCC will be paid by the MSI.
- Overall maintenance of housekeeping and physical security at CCDCSC.
- Provide necessary security to the ICCC premises and its setup during the period of contract.
- Submit Monthly Progress reports as per the defined format to City SPV along with invoices.
- Submit Joint Monthly Progress reports of all cities after approval as per the format defined to BSCDCL along monthly progress report on common cloud based DC and DR along with total invoices.

Exclusions

- Development of basic civil infrastructure of the building for the City ICCC
- Provisioning of power and water connection at ICCC location.

1.6 Roles and Responsibilities of various stakeholders under this RFP

BSCDCL will act as a facilitator, contracting agency and payment agency
MPUDC/MPUADD as overall governing body
CEOs of smart cities as part of steering committee

Other Roles and Responsibilities during execution of Project

Phase	City SPV	BSCDCL	Other Departments
Pre – Implementation	• Provide necessary information to MSI for doing surveys • Facilitate Interaction with other Departments for getting the required integration • Help MSI get necessary approvals for implementing ICCC at City level • Help MSI finalize the protocols for data exchange between ICCC and various other systems. • Review the documents submitted by MSI and provide feedback • Review and approve/reject monthly invoice along with progress report	• Facilitate in getting necessary information to MSI for doing surveys for implementing common cloud based DC and DR • Help MSI get necessary approvals for implementing common cloud based DC and DR • Help MSI finalize the protocols for data exchange between various systems. • Process the approved joint monthly invoice submitted along with progress report for all city ICCC	• Provide necessary information to MSI for doing future integrations. • Provide necessary information to MSI for finalizing the data exchange between the systems.
Implementation	• Provide building structure for setting up ICCC (based on agreed plan) • Help MSI get necessary electricity and water connections at ICCC premises • Help MSI get necessary network connections established between ICCC, common cloud based DC and DR with all	• Process the approved joint monthly invoice along with progress report for all city ICCC	• Provide necessary access to the current ICT setup for integration with ICCC.

	the applications to be integrated with common control and command center application • Review and approve/reject monthly invoice along with progress report		
Post – Implementation	• Facilitate Interactions with other Departments for getting the required integration. • Help MSI get necessary feeds for ICCC and get it integrated with command center and other common applications hosted on common cloud based DC and DR • Help MSI get necessary approvals (if any). • Approve / Reject Change request • Review the documents submitted by MSI and provide feedback • In case of any incident or disaster facilitate communication from ICCC to field agents (in case of absence of ICT setup with field agents)	• Help MSI get necessary feeds for common applications hosted on common cloud based DC and DR. • Help MSI get necessary approvals (if any). • Review the documents submitted by MSI and provide feedback • Process the approved joint monthly invoice submitted along with progress report for all city ICCC	• Provide and receive (if applicable) data feeds to/ from ICCC to their current ICT setup in the predefined formats. • Perform needful action in case of any incident or disaster

Schedule 1 – Instruction to Bidders

1. Instruction to Bidders

1.1 General

a. While every effort has been made to provide comprehensive and accurate background information, requirements and envisaged solution(s) specifications, Bidders must form their own conclusions about the solution(s) needed to meet the BSCDCL's requirements. Bidders and recipients of this RFP may wish to consult their own legal advisers in relation to this RFP.
b. All information supplied by Bidders as part of their bids in response to this RFP, may be treated as contractually binding on the Bidders, on successful award of the assignment by BSCDCL on the basis of this RFP.
c. No commitment of any kind, contractual or otherwise shall exist unless and until a formal written contract has been executed by or on behalf of BSCDCL. Any notification of preferred bidder status by BSCDCL shall not give rise to any enforceable rights by the Bidder. BSCDCL may cancel this public procurement at any time prior to a formal written contract being executed by or on behalf of BSCDCL.
d. Sealed bids shall be received by the BSCDCL on the e-Procurement portal of Madhya Pradesh (mpeproc.gov.in) before the time and date specified in the schedule of the tender notice. In the event of the specified date for the submission of tender offers being declared a public holiday by the Government of Madhya Pradesh, the offers will be received up to the appointed time on the next working day. The BSCDCL may, at its discretion, extend this deadline for submission of offers by issuing corrigendum and uploading the same on e-Procurement portal.
e. Telex, cable or facsimile offers will be rejected.

2.2 Eligible Bidders

Bids may be submitted by either of the following categories of bidders only:

The Bidder can be either a Single Master System Integrator (MSI) or a Consortium of companies/ corporations as described below.

a. Sole Bidder

The Sole Bidder must be a System Integrator company which has the capabilities to deliver the entire scope as mentioned in the RFP- under- Scope or Work. The Sole Bidder cannot bid as a part of any other consortium bid under this RFP.

b. Consortium of Firms

Bids can be submitted by a consortium of firms. A consortium should not consist of more than three parties (including the Lead Bidder). One of the Firms would be designated as a "Lead Bidder". The Lead Bidder would have the sole responsibility of ensuring the delivery of products and services mentioned in this RFP. The Lead Bidder would also be responsible for ensuring the

successful execution of integrated solution including meeting the SLAs. The list of Consortium Members needs to be declared in the bid which cannot be changed by the bidder later on. Any change in the consortium partner will need to be approved by BSCDCL.

The Lead Bidder will be responsible for:

i. The management of all consortium members who are part of bid and
ii. The supply, delivery and installation of all products and services submitted in their bid as part of the contract.

Bids submitted by consortium should comply with the following requirements also:

i. The Lead Bidder shall be authorized to incur liabilities and receive instructions for and on behalf of any and all consortium members. Entire execution of the Contract, including payment, shall be done exclusively by/with the Lead Bidder
ii. Any of the Lead Bidders cannot be a Consortium Member with another bidder in a separate bid
iii. Internal arrangement between the Consortium Members is left to the bidders. It is the responsibility of the lead Bidder to ensure that all the other Consortium Members in the bid are compliant to all the clauses as mentioned in the bid, failing which bid can be disqualified.

The Consortium Members will be responsible for:

i. Responsible for the delivery of project components as per agreed roles & responsibility as defined in Consortium Agreement (as per Annexure 9 of this RFP).

2.3 Compliant Bids/Completeness of Response

a. Bidders are advised to study all instructions, forms, terms, requirements and other information in the RFP documents carefully. Submission of the bid shall be deemed to have been done after careful study and examination of the RFP document with full understanding of its implications.

b. Failure to comply with the requirements of this paragraph may render the bid non-compliant and the Bid may be rejected. Bidders must:
   i. Include all documentation specified in this RFP, in the bid
   ii. Follow the format of this RFP while developing the bid and respond to each element in the order as set out in this RFP
   iii. Comply with all requirements as set out within this RFP

2.4 Bidder to Inform

The Bidder shall be deemed to have carefully examined the Terms & Conditions, Scope, Service Levels, Specifications, and Schedules of this RFP. If bidder has any doubts/clarifications as to the meaning of

any portion of the Conditions or the specifications he shall, before the last date for Submission of Pre-Bid Queries, set forth the particulars thereof and submit them to BSCDCL in writing in order that such doubt may be removed or clarifications are provided.

2.5 Bid Preparation costs

The Bidder shall bear all costs associated with the preparation and submission of its bid, including cost of presentations etc. for the purposes of clarification of the bid, if so desired by the BSCDCL.

2.6 Pre-bid meeting & Clarification

2.6.1 Bidders Queries

Any clarification regarding the RFP document and any other item related to this project can be submitted to BSCDCL as per the submission mode and timelines mentioned in the Fact Sheet. The pre-bid queries should be submitted in excel sheet format, along with name and details of the organization submitting the queries.

BSCDCL shall not be responsible for ensuring that the bidders' queries have been received by them. Any requests for clarifications post the indicated date and time shall not be entertained by BSCDCL.

Bidders must submit their queries as per the format mentioned in Annexure 3.

2.6.2 Responses to Pre-Bid Queries and Issue of Corrigendum

BSCDCL will organize a pre-bid conference and will respond to any request for clarification or modification of the bidding documents. BSCDCL shall formally respond to the pre-bid queries after the pre-bid conference. No further clarifications shall be entertained after the date and time of submission of queries.

BSCDCL shall endeavor to provide timely response to all queries. However, BSCDCL makes no representation or warranty as to the completeness or accuracy of any response made in good faith. BSCDCL does not undertake to answer all the queries that have been posed by the bidders.

Any modifications of the RFP Documents, which may become necessary as a result of the Pre-Bid Conference, shall be made by BSCDCL exclusively through a corrigendum. Any such corrigendum shall be deemed to be incorporated into this RFP. However, in case of any such amendment, the bid submission date may be extended at the discretion of BSCDCL.

Any corrigendum/notification issued by BSCDCL, subsequent to issue of RFP, shall only be available/hosted on the website URL mentioned in the fact sheet. Any such corrigendum shall be deemed to be incorporated into this RFP.

2.7 RFP Document Fee

RFP can be downloaded from the website https://www.mpeproc.gov.in/. .

Tender Fee of Rs. 50, 000/- (Rupees Fifty Thousand Only) shall be paid online through e-Procurement portal https://www.mpeproc.gov.in/. The tender fee shall be non-refundable.

Without the payment of tender fee the bids will be taken as incomplete and non-responsive and shall not be considered.

2.8 Earnest Money Deposit (EMD)

EMD of Rs. 5,00,00,000/- (Rupees Five Crores Only) shall be paid either online to BSCDCL account, or through a Bank Guarantee. EMD should be valid for six months from the date of submission of tender. Scanned copy of EMD should be submitted on e-procurement system and physical copy should be submitted to BSCDCL before submission of tender. No exemption for submitting the EMD will be given to any agency. Bid security in any other form will not be entertained. Scheduled bank payable at Bhopal.

***For Unsuccessful bidders*:** The bid security of all unsuccessful bidders would be refunded without interest by BSCDCL on finalization of the bid in all respects by the successful bidder.

For Successful bidders: The bid security, for the amount mentioned above, of successful bidder would be returned without interest upon submission of Performance Bank Guarantee by the successful bidder.
The above mentioned refund would be completed within 1 month of the selected of the MSI.

In case bid is submitted without the bid security then BSCDCL reserves the right to reject the bid without providing opportunity for any further correspondence to the bidder concerned.

The EMD may be forfeited in any of the following circumstances:

a. If a bidder withdraws its bid during the period of bid validity.
b. In case of a successful bidder, if the bidder fails to submit the performance bank guarantee and/or sign the contract in accordance with this RFP.

2.9 Bid Validity Period

Bid shall remain valid for the time period mentioned in the Bidding Data Sheet.

On completion of the validity period, unless the Bidder withdraws his bid in writing, it will be deemed to be valid until such time that the Bidder formally (in writing) withdraws his bid. – not to be deemed

2.10 Contents of Bid

The two bids system shall be followed. Technical and Commercial Offers shall be uploaded separately through the e - Procurement portal https://www.mpeproc.gov.in/.

Document Set	Name of Document	Content
One	RFP Document fee & Bid Security/Earnest Money Deposit (EMD)	a. RFP Document Fee receipt b. Bid Security/Earnest Money Deposit (EMD) receipt
Two	Pre-Qualification Bid	a. Pre-Qualification bid as per this RFP along with the required supporting documents. b. Total Responsibility declaration as per Section 6.6
Three	Technical bid	a. Technical bid
Four	Commercial Bid	a. Commercial bid

a. Please note that Prices should NOT be indicated in the Technical Bid but should only be indicated in the Commercial Bid.

b. All the pages of the bid must be sequentially numbered. The bid documents must contain in the beginning of the document, a list of contents with page numbers. Any deficiency in the documentation may result in the rejection of the Bid.

c. The original bid shall be prepared in indelible ink. It shall contain no interlineations or overwriting, except as necessary to correct errors made by the Bidder itself. Any such corrections must be initialed by the person (or persons) who sign(s) the bids.

d. All pages of the bid shall be initialed and stamped by the person (or persons) who sign the bid.

e. Failure to submit the bid before the submission deadline specified in the Fact Sheet would cause a bid to be rejected.

g. BSCDCL will not accept delivery of bid by fax, or e-mail.

2.11 Bid Formats

2.11.1 Pre-Qualification Bid Format

Section #	Section Heading	Details
1.	Pre-qualification checklist	As per format provided in Annexures
2.	Pre-Qualification Bid Covering Letter	As per format provided in Annexures
3.	Consortium Agreement	As per format provided in Annexure
4.	About Bidder	As per format provided in Annexures
5.	Legal	1. Copy of Certification of Incorporation/Registration Certificate 2. PAN card 3. VAT registration *As per Pre-qualification criteria – Sl # 1*
6.	Annual Turnover	Details of annual turnover with documentary evidence. *As per Pre-qualification criteria – Sl # 2*
7.	Net worth	Details of net worth with documentary evidence. *As per Pre-qualification criteria – Sl # 3*
8.	Certification	Relevant ISO certification *As per Pre-qualification criteria – Sl # 5*
9.	Self-certificate for non-blacklisting clause	As per format provided in Annexures *As per Pre-qualification criteria – Sl # 6*
10.	Power of Attorney	Documentary evidence as per format provided in Annexure 10

Section #	Section Heading	Details
11.	Project Experience	Citation details of projects as per format in Annexures
12.	Total responsibility certificate	As per format in Annexures

2.11.2 Technical Bid Format

Section #	Section Heading	Details
1.	Technical Bid Checklist	As per format provided in Annexure 5
2.	Technical Bid Covering Letter	As per format provided in Annexure 5
3.	About Bidder	· Details about bidder (whether sole bidder or consortium) · Bidder's General Information as required in Technical Criteria 3.6.1
4.	Understanding	Details as required in Technical Criteria 3.6.1.
5.	Solution proposed	Details as required in Technical Criteria 3.6.1. Please refer to Annexure 5
6.	Project/credential summary	As per format provided in Annexure 5
7.	Bidder's Experience	Project citation as per format provided in section Annexure 5 and supporting documentary evidences and Self-certifications as per format in Annexure 4 as Applicable
8.	Project Plan and Resources	· Project plan as per format provided in · Manpower Plan as per format provided in · Summary of resources as per format Annexure 5 · CV of resources as per format provided Annexure 5
9.	Manufacturers'/Producers' Authorization Form	As per format provided in Annexure 5
10.	Proposed Bill of Material (BoM)	As per format provided in Financial Bid, without any price / quote (masked price bid)

11.	Anti-Collusion Certificate	As per format provided in Annexure 5
12.	Non-disclosure agreement	As per format provided in the RFP

2.11.3 Commercial Bid Format

The Bidder must submit the Commercial Bid is the formats specified in Annexure of this RFP.

2.12 Language

The bid should be prepared and submitted by the bidders in English language only. If any submitted supporting documents are in any language other than English, translation of the same in English language is to be provided (duly attested) by the Bidders. For purposes of interpretation of the documents, the English translation shall govern.

2.13 Authentication of Bids

An authorized representative (or representatives) of the Bidder shall initial all pages of the Pre-Qualification, Technical and Commercial Bids.

Bid should be accompanied by an authorization in the name of the signatory (or signatories) of the Bid. The authorization shall be in the form of a written power of attorney accompanying the Bid or in any other form demonstrating that the representative has been duly authorized to sign.

2.14 Amendment of Request for Proposal

At any time prior to the due date for submission of bid, BSCDCL may, for any reason, whether at its own initiative or in response to a clarification requested by prospective bidder(s), modify the RFP document by amendments. Such amendments shall be uploaded on the e-procurement portal website https://www.mpeproc.gov.in/, through corrigendum and shall form an integral part of RFP document. The relevant clauses of the RFP document shall be treated as amended accordingly.

It shall be the responsibility of the prospective bidder(s) to check the procurement portal https://www.mpeproc.gov.in/ from time to time for any amendment in the RFP document. In case of failure to get the amendments, if any, BSCDCL shall not be responsible.

In order to allow prospective bidders a reasonable time to take the amendment into account in preparing their bids, BSCDCL, at its discretion, may extend the deadline for submission of bids. Such extensions shall be uploaded on procurement portal https://www.mpeproc.gov.in.

2.15 Bid Price

Commercial Bid shall be as per the format provided in Section 8. Bidders shall give the required details of all applicable taxes, duties, other levies and charges etc. in respect of direct transaction between BSCDCL and the Bidder.

Bidders shall quote for the entire scope of contract on a "overall responsibility" basis such that the total bid price covers Bidder's all obligations mentioned in or to be reasonably inferred from the bidding documents in respect of providing the product/services.

Prices quoted by the Bidder shall remain firm during the entire contract period and not subject to variation on any account. A bid submitted with an adjustable price quotation shall be treated as non-responsive and rejected.

2.16 Deviations and Exclusions

Bids shall be submitted strictly in accordance with the requirements and terms & conditions of the RFP.

2.17 Total Responsibility

Bidder should issue a statement undertaking total responsibility for the defect free operation of the proposed solution as per the format mentioned in Section 6.6.

2.18 Late Bids

Late submission will not be entertained and will not be permitted by the e-Procurement Portal.

The bids submitted by telex/telegram/fax/e-mail etc. shall not be considered. No correspondence will be entertained on this matter.

BSCDCL shall not be responsible for any non-receipt/non-delivery of the documents due to technical snag whatsoever at Bidder's end. No further correspondence on the subject will be entertained.

BSCDCL reserves the right to modify and amend any of the above-stipulated condition/criterion.

2.19 Right to Terminate the Process

BSCDCL may terminate the RFP process at any time and without assigning any reason. BSCDCL makes no commitments, express or implied, that this process will result in a business transaction with anyone. This RFP does not constitute an offer by BSCDCL.

2.20 Non-Conforming bids

A bid may be construed as a non-conforming bids and ineligible for consideration:

a. If it does not comply with the requirements of this RFP.

b. If a bid does not follow the format requested in this RFP or does not appear to address the particular requirements of the solution.

2.21 Acceptance/Rejection of Bids

a. BSCDCL reserves the right to reject in full or part, any or all bids without assigning any reason thereof. BSCDCL reserves the right to assess the Bidder's capabilities and capacity. The decision of BSCDCL shall be final and binding.

b. Bid should be free of over writing. All erasures, correction or addition must be clearly written both in words and figures and attested.

In the event of any assumptions, presumptions, key points of discussion, recommendation or any points of similar nature submitted along with the Bid, SCDCL reserves the right to reject the Bid and forfeit the EMD.

If there is any discrepancy in the commercial bid, it will be dealt as per the following:

a. If, in the price structure quoted for the required goods/services/works, there is discrepancy between the unit price and total price (which is obtained by multiplying the unit price by the quantity), the unit price shall prevail and the total price corrected accordingly.
b. If there is an error in a total corresponding to the addition or subtraction of subtotals, the subtotals shall prevail and the total shall be corrected.
c. If there is a discrepancy between words and figures, the amount in words shall prevail.
d. If there is such discrepancy in an offer, the same shall be conveyed to the bidder with target date up to which the bidder has to send his acceptance on the above lines and if the bidder does not agree to the decision of BSCDCL, the bid is liable to be disqualified.

2.22 Confidentiality

All the material/information shared with the Bidder during the course of this procurement process as well as the subsequent resulting engagement following this process with the successful bidder, shall be treated as confidential and should not be disclosed in any manner to any unauthorized person under any circumstances. The employees of the successful Lead bidder and Consortium members who are proposed to be deployed on the project need to furnish a Non-Disclosure Agreement (NDA) as per RFP.

2.23 Disqualification

The bid is liable to be disqualified in the following cases or in case bidder fails to meet the bidding requirements as indicated in this RFP:

a. During validity of the bid, or its extended period, if any, the bidder increases its quoted prices
b. The bidder's bid is conditional and has deviations from the terms and conditions of RFP
c. Bid is received in incomplete form
d. Bid is not accompanied by all the requisite documents
e. Information submitted in technical bid is found to be misrepresented, incorrect or false, accidentally, unwittingly or otherwise, at any time during the processing of the contract (no matter at what stage) or during the tenure of the contract including the extension period if any
f. Financial bid is enclosed with the same document as technical bid.
g. Bidder tries to influence the bid evaluation process by unlawful/corrupt/fraudulent means at any point of time during the bid process
h. In case any one party submits multiple bids or if common interests are found in two or more bidders, the bidders are likely to be disqualified, unless additional bids/bidders are withdrawn upon notice immediately
i. If any of the Lead Bidder is also partner in any other bid, then all the affected bids shall be disqualified

2.24 Key Personnel

BSCDCL has identified certain key positions and minimum qualifications for each of the positions that should be part of project team of the bidder (hereby referred to as "key personnel"). Details of these key positions are provided in Section 3.6.4.

2.24.1 Initial Composition; Full Time Obligation; Continuity of Personnel

Bidder shall ensure that each member of the Key Personnel devotes substantial working time as per the staffing schedule/ manpower plan to perform the services to which that person has been assigned as per the bid.

Bidder shall not make any changes to the composition of the Key Personnel and not require or request any member of the Key Personnel to cease or reduce his or her involvement in the provision of the Services during the defined term of the engagement unless that person resigns, is terminated for cause, is long-term disabled, is on permitted mandatory leave under Applicable Law or retires.

In any such case, the BSCDCL's prior written consent would be mandatory.

2.24.2 Replacement

In case any proposed resource resigns, then the Bidder has to inform BSCDCL or the respective City nodal officer within one week of such resignation.

Bidder shall promptly initiate a search for a replacement to ensure that the role of any member of the Key Personnel is not vacant at any point in time during the contract period, subject to reasonable extensions requested by Bidder to BSCDCL or City nodal officer.

Before assigning any replacement member of the Key Personnel to the provision of the Services, Bidder shall provide BSCDCL with:

a. a resume, curriculum vitae and any other information about the candidate that is reasonably requested by BSCDCL; and
b. An opportunity to interview the candidate.

The bidder has to provide replacement resource of equal or better qualification and experience as per the requirements of this RFP.

If BSCDCL objects to the appointment, Bidder shall not assign the individual to that position and shall seek an alternative candidate in accordance with the resource requirements of this RFP.

The bidder needs to ensure at least 4 weeks of overlap period in such replacements. BSCDCL will not be responsible for any knowledge transition to the replacement resource and any impact/escalation of cost incurred by the bidder due to resource replacement.

2.24.2 High Attrition

If in the first 6 month period from the Contract Effective Date and in any rolling 12 months period during the Term of contract, 15 percent or more of the members of the Key Personnel cease or reduce their involvement in the Services for any reason other than with BSCDCL's prior written consent, Bidder shall:

a. provide BSCDCL with a reasonably detailed explanation as to the reasons for such change, including, where applicable and permitted, notes from any exit interviews conducted by Bidder with any departing member of the Key Personnel; and

b. if such change to Key Personnel has or is likely to have any material adverse impact on the provision of the Services or any substantial part thereof, undertake, at its own costs, such remediation acts as are reasonably necessary in order to improve the retention of the Key Personnel including making reasonable changes to the human resources policies and procedures applicable to the Key Personnel (including those related to compensation, benefits and other conditions so that they are competitive with the market) as may be necessary to ensure that such policies and procedures comply with Good Industry Practice.

2.25 Fraud and Corrupt Practices

a. The Bidders and their respective officers, employees, agents and advisers shall observe the highest standard of ethics during the Selection Process. Notwithstanding anything to the contrary contained in this RFP, BSCDCL shall reject a Bid without being liable in any manner whatsoever to the Bidder, if it determines that the Bidder has, directly or indirectly or through an agent, engaged in corrupt practice, fraudulent practice, coercive practice, undesirable practice or restrictive practice (collectively the "Prohibited Practices") in the Selection Process. In such an event, BSCDCL shall, without prejudice to its any other rights or remedies, forfeit and appropriate the EMD or PBG, as the case may be, as mutually agreed genuine pre-estimated compensation and damages payable to BSCDCL for, inter alia, time, cost and effort of BSCDCL, in regard to the RFP, including consideration and evaluation of such Bidder's Bid.

b. Without prejudice to the rights of BSCDCL under Clause above and the rights and remedies which BSCDCL may have under the LOI or the Agreement, if a Bidder is found by BSCDCL to have directly or indirectly or through an agent, engaged or indulged in any corrupt practice, fraudulent practice, coercive practice, undesirable practice or restrictive practice during the Selection Process, or after the issue of the LOI or the execution of the Agreement, such Bidder shall not be eligible to participate in any tender or RFP issued by BSCDCL during a period of 3 years from the date such Bidder is found by BSCDCL to have directly or through an agent, engaged or indulged in any Prohibited Practices.

c. For the purposes of this Section, the following terms shall have the meaning hereinafter respectively assigned to them:

   i. *"corrupt practice"* means (i) the offering, giving, receiving, or soliciting, directly or indirectly, of anything of value to influence the action of any person connected with the Selection Process (for avoidance of doubt, offering of employment to or employing or engaging in any manner whatsoever, directly or indirectly, any official of BSCDCL who is or has been associated in any manner, directly or indirectly with the Selection Process or the LOI or has dealt with matters concerning the Agreement or arising there from, before or after the execution thereof, at any time prior to the expiry of one year from the date such official resigns or retires from or otherwise ceases to be in the service of BSCDCL , shall be deemed to constitute influencing the actions of a person connected with the Selection Process); or (ii) save as provided herein, engaging in any manner whatsoever, whether during the Selection Process or after the issue of the LOA or after the execution of the Agreement, as the case may be, any person in respect of any matter relating to the Project or the Award or the Agreement, who at any time has been or is a legal, financial or technical consultant/adviser of BSCDCL in relation to any matter concerning the Project;

   ii. *"fraudulent practice"* means a misrepresentation or omission of facts or disclosure of incomplete facts, in order to influence the Selection Process;

iii. *"coercive practice"* means impairing or harming or threatening to impair or harm, directly or indirectly, any persons or property to influence any person's participation or action in the Selection Process;

iv. *"undesirable practice"* means (i) establishing contact with any person connected with or employed or engaged by BSCDCL with the objective of canvassing, lobbying or in any manner influencing or attempting to influence the Selection Process; or (ii) having a Conflict of Interest; and

v. *"restrictive practice"* means forming a cartel or arriving at any understanding or arrangement among Bidders with the objective of restricting or manipulating a full and fair competition in the Selection Process.

2.26 Conflict of Interest

a. A bidder shall not have a conflict of interest that may affect the Selection Process or the Solution delivery (the "Conflict of Interest"). Any Bidder found to have a Conflict of Interest shall be disqualified. In the event of disqualification, BSCDCL shall forfeit and appropriate the EMD, if available, as mutually agreed genuine pre-estimated compensation and damages payable to BSCDCL for, inter alia, the time, cost and effort of BSCDCL including consideration of such Bidder's Bid, without prejudice to any other right or remedy that may be available to BSCDCL hereunder or otherwise.

b. BSCDCL requires that the bidder provides solutions which at all times hold BSCDCL's interests paramount, avoid conflicts with other assignments or its own interests, and act without any consideration for future work. The bidder shall not accept or engage in any assignment that would be in conflict with its prior or current obligations to other clients, or that may place it in a position of not being able to carry out the assignment in the best interests of BSCDCL.

2.27 Sub-Contracting

The bidder would not be allowed to sub-contract / outsource work, except for the following:

- Fiber optic network build, other cabling and fixtures work, and all civil work during implementation
- Facility Management Staff at Command Control Center & City Operation Center

Sub-contracting / Outsourcing shall be allowed only with prior written approval of BSCDCL. However, even if the work is sub-contracted / outsourced, the sole responsibility of the work shall lie with the lead bidder. The lead bidder 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 BSCDCL.

2.28 Eligible Goods and Services, and OEM Criteria:

a. For purposes of this Clause, the term "goods" includes commodities, raw material, machinery, equipment, and industrial plants; and "related services" includes services such as insurance, transportation, supply, installation, integration, testing, commissioning, training, and initial maintenance.
b. The Bidder shall quote only one specific make and model from only one specific OEM, for each of the goods. Providing more than one option shall not be allowed. All goods quoted by the Bidder must be associated with item code and names and with printed literature describing configuration and functionality. Any deviation from the printed specifications should be clearly mentioned in the offer document by the Bidder.
c. The OEM for each products or technology quoted should be in the business of that product or solution or technology for at least 3 years as on the date of release of the RFP.
d. All the OEMs should have authorized presence in India either directly or through channel partner(s) as on the date of release of RFP.
e. Bidder must quote products in accordance with above clause "Eligible goods and related services.

Adequate supporting documents pertaining to the above points, along with a summary compliance table, should be submitted in the technical proposal by the Bidder.

2.29 Right to vary quantity

a. At the time of award of contract, the quantity of goods, works or services originally specified in the bidding documents may be increased not more than 10%. It shall be without any change in the unit prices or other terms and conditions of the Bid and the bidding documents.
b. If the BSCDCL does not procure any subject matter of procurement or procures less than the quantity specified in the bidding documents due to change in circumstances, the bidder shall not be entitled for any claim or compensation except otherwise provided in the bidding document.
c. Repeat orders for extra items or additional quantities may be placed, if it is provided in the bidding document, on the rates and conditions given in the contract if the original order was given after inviting open competitive bids. Delivery or completion period may also be proportionally increased.

2.30 Withdrawal, Substitution, and Modification of Bids

a. A Bidder may withdraw its Bid or re-submit its Bid (technical and/ or financial) as per the instructions/ procedure mentioned at e-Procurement website
b. Bids withdrawn shall not be opened and processed further.

2.31 Site Visit

The Bidder may wish to visit and examine the site or sites and obtain for itself, at its own responsibility and risk, all information that may be necessary for preparing the bid and entering into the Contract. The costs of visiting the site or sites shall be at the Bidder's own expense.

b. The City SPV will arrange for the Bidder and any of its personnel or agents to gain access to the relevant site or sites, provided that the Bidder gives the BSCDCL adequate notice of a proposed visit of at least fourteen (14) days. Alternatively, the BSCDCL may organize a site visit or visits concurrently with the pre-bid meeting, as specified in the RFP. Failure of a Bidder to make a site visit will not be a cause for its disqualification.

c. No site visits shall be arranged or scheduled after the deadline for the submission of the Bids and prior to the award of Contract.

3. Selection Process for Bidder

3.1 Opening of Bids

The Bids shall be opened by BSCDCL in presence of those Bidders or their representatives who may be present at the time of opening.

The representatives of the bidders should be advised to carry the identity card or a letter of BSCDCL from the bidder firms to identify that they are bona fide representatives of the bidder firm, for attending the opening of bid.

There will be three bid-opening events

a. Set 1 (RFP Document fee & Bid Security/EMD) and Set 2 (Pre-Qualification bid)
b. Set 3 (Technical bid)
c. Set 4 (Commercial bid)

The venue, date and time for opening the Pre-qualification bid are mentioned in the Fact sheet.

The date and time for opening of Technical & Commercial bid would be communicated to the qualified bidders.

The Technical Bids of only those bidders will be opened who clears the Pre-qualification stage.

The Commercial Bids of only those bidders will be opened who score equal to or more than qualifying marks in Technical Bid.

3.2 Preliminary Examination of Bids

Evaluation Committee shall examine the bids to determine whether they are complete, whether the documents have been properly signed and whether the bids are generally in order. Any bids found to be nonresponsive for any reason or not meeting any criteria specified in the RFP, shall be rejected by Evaluation Committee and shall not be included for further consideration.

Initial Bid scrutiny shall be held and bids will be treated as non-responsive, if bids are:

a. Not submitted in format as specified in the RFP document
b. Received without the Letter of Authorization (Power of Attorney)
c. Found with suppression of details
d. With incomplete information, subjective, conditional offers and partial offers submitted
e. Submitted without the documents requested
f. Non-compliant to any of the clauses mentioned in the RFP
g. With lesser validity period

3.3 Clarification on Bids

During the bid evaluation, BSCDCL may, at its discretion, ask the Bidder for any clarification(s) of its bid. The request for clarification and the response shall be in writing, and no change in the price or substance of the bid shall be sought, offered, or permitted.

3.4 Evaluation Process

The Evaluation Committee shall evaluate the responses to the RFP and all supporting documents/documentary evidence. Inability to submit requisite supporting documents/documentary evidence by bidders may lead to rejection of their bids.

The decision of the Evaluation Committee in the evaluation of bids shall be final. No correspondence will be entertained outside the process of evaluation with the Committee. The Evaluation Committee may ask for meetings or presentation with the Bidders to seek clarifications or conformations on their bids.

The Evaluation Committee reserves the right to reject any or all bids. Each of the responses shall be evaluated as per the criteria and requirements specified in this RFP.
The steps for evaluation are as follows:

3.4.1 Stage 1: Pre-Qualification

a. Evaluation Committee shall validate the Set 1 "RFP Document fee & Bid Security/Earnest Money Deposit (EMD)".

b. If the contents of the Set 1 are as per requirements, BSCDCL shall open the "Pre-Qualification Bid**". Each of the Pre-Qualification condition mentioned in Section 3.5 is MANDATORY**. In case, the Bidder does not meet any one of the conditions, the bidder shall be disqualified.

Bidders would be informed of their qualification/disqualification based on the Pre-Qualification criteria through Email and Phone and subsequently, the Bid Security amount shall be returned to the respective disqualified Bidders after the submission of Performance Bank Guarantee by the successful Bidder.

c. Technical and Financial bids for those bidders who don't pre-qualify will not be opened. Financial bid will not be opened for those bidders, who don't qualify the technical evaluation. Bid Security amount shall be retuned for those who don't qualify the financial evaluation stage and after PBG is submitted by successful bidder.

3.4.2 Stage 2: Technical Evaluation

a. Set 3 "Technical bid" will be evaluated only for the bidders who succeed in Stage 1.

b. Evaluation Committee will review the technical bids of the short-listed bidders to determine whether the technical bids are substantially responsive. Bids that are not substantially responsive are liable to be disqualified at BSCDCL's discretion.

c. The bidders' technical solutions proposed in the bid document shall be evaluated as per the requirements specified in the RFP and technical evaluation framework as mentioned in Section 3.6.

d. Bidders may be asked to give demonstration of the envisaged solution to BSCDCL as per the demo scripts that shall be shared with the Bidders who qualify the Pre-Qualification Stage.

e. Bidders shall present the bid to BSCDCL as per the agenda mentioned in Section 3.6.2 (Point no. C) – "***Approach & Methodology & Solutions proposed*** "

f. Each Technical Bid will be assigned a technical score out of a maximum of 1000 marks. Only the bidders who get an Overall **Technical score of 70%** or more and minimum 50% in each section of the Technical Evaluation Framework as given in Section 3.6 will qualify for commercial evaluation stage. Failing to secure minimum marks shall lead to technical rejection of the Bid.

g. Technical bids of the Bidders qualifying in the Pre- Qualification criteria will be opened and will also be invited for doing the technical presentation.

3.4.3 Stage 3: Commercial Evaluation

a. All the technically qualified bidders will be notified to participate in Commercial Bid opening process.

b. The commercial bids for the technically qualified bidders shall then be opened on the notified date and time and reviewed to determine whether the commercial bids are substantially

responsive. Bids that are not substantially responsive are liable to be disqualified at BSCDCL's discretion.

c. Commercial Bids that are not as per the format provided in Section 8 (Annexure 4) shall be liable for rejection.

d. The Normalized commercial score of the technically qualified bidders will be calculated, while considering the Total Cost of Bid given by each of the Bidders in the Commercial Bid as follows:

Normalized Commercial Score of a Bidder = {Lowest TCB/ Bidders TCB} X 1000 (adjusted to 2 decimals)

1. The bid price will include all taxes and levies and shall be in Indian Rupees and mentioned separately.
2. Any conditional bid would be rejected
3. Errors & Rectification: Arithmetical errors will be rectified on the following basis:
    a. "If there is a discrepancy between the unit price and the total price that is obtained by multiplying the unit price and quantity, the unit price shall prevail and the total price shall be corrected.
    b. If there is a discrepancy between words and figures, the amount in words will prevail."
    c. If the Bidder does not accept the error correction, its Bid will be rejected and its EMD may be forfeited.
    d. Kindly note e that the indicative/estimated quantity provided in the RFP would be used for evaluation purposes; however the payment would be done on actual usage basis.

3.4.4 Stage 4: Final score calculation through QCBS

1. The final score will be calculated through Quality and Cost selection method based with the following weight-age:
   Technical: 80%
   Commercial: 20%
   Final Score = (0.80* Technical Score) + (0.20* Normalized Commercial Score)

2. The bidder with the highest Final score shall be treated as the Successful bidder.
   In the above example, Bidder-1 will be treated as successful bidder.

3. In the event the Final scores are 'tied', the bidders whose score is tied securing the lowest (among all the tied bidders) financial score will be adjudicated as the Best Value Bidder for award of the Project.

3.5 Pre-Qualification Criteria

Pre -Qualification Criteria for MSI and its Consortium Partner

#	Parameter	Pre-qualification criteria description	Evidence required	Applicability
1.	**Legal Entity**	MSI should be: • A company should be registered in India or abroad	• Copy of Certificate of Incorporation • Copy of Registration Certificates • Copy of purchase orders showing at least 5 years of operations OR Certified true copy of relevant extracts of balance sheet and PL statements for last 5 years	MSI
		Consortium Members should be: • A company should be registered in India or abroad	• Copy of Certificate of Incorporation	Consortium Members
2.	**Turnover**	Bidder should have an average annual turnover of at least INR 1000 Crores in over last 3 financial years (FY 2013-14, 2014-15, 2015-16) from IT system integration services / ICT system integration services / command & control center implementation / Network Operating Center (NOC) / Cloud service provider in India or abroad. Turnover of any parent, subsidiary, associated or other related entity will not be considered.	Certificate from the Company Secretary / Chartered Accountant. In case Chartered Accountant certificate is submitted the said certificate also need to be counter signed by Company Secretary / authorized signatory of the bidder.	MSI

#	Parameter	Pre-qualification criteria description	Evidence required	Applicability
3.	**Experience in development / implementation of Smart City Component**	Bidder (MSI or Any Consortium Partner) should have experience in implementation and maintenance of following project of value not less than INR 50 Crore each: a)Utility Management (Water OR Electricity) or b) Command & Control Centre / Network Operations Centre (NOC) or c) Surveillance command center or d) City ERP system In India or abroad in last 10 years. Note: • Bidder can propose separate (one or more) projects for each component for evaluation.	Case Study+ Copy of work order + Completion/Phase completion Certificates from the client (in case of ongoing project) In case the experience shown is that of the bidder's parent / subsidiary company, then the following additional documents are required: i. Letter from the Company Secretary of the bidder certifying that the entity whose experience is shown is parent/subsidiary Company ii. Shareholding pattern of the bidding entity as per audit reports	MSI or Any Consortium Partner
4.	**Blacklisting**	Bidder and Consortium partner should not have been blacklisted by Govt. of India/ Govt. of Madhya Pradesh on the date of bid submission.	Self-certificate on company's letter head duly signed by company secretary.	MSI and Consortium Partner
5.	**Earnest Money Deposit (EMD)**	The bidder should furnish, as part of its proposal, an Earnest Money Deposit (EMD) of INR Five Crores only (Rs. 5,00,00,000/-), it should be valid for 6 months from the date of submission of tender.	EMD may be submitted on line in the name of CEO, Bhopal Smart City Development Corporation Development Limited (BSCDCL) through website www.mpeproc.gov.in as part of tender submission process OR	MSI

#	Parameter	Pre-qualification criteria description	Evidence required	Applicability
			EMD may be submitted in the form of Bank Guarantee (BG) as per format mentioned in the RFP on stamp paper of value required under law duly signed by authorized representative of Bank.	

Pre-Qualification Criteria for ICCC Platform OEM

1. Solution should be deployed in at least 10 locations globally, with 5 use cases like smart lighting, Parking, environment, Parking video nodes, Wi-Fi etc. in cities globally with multiple smart city use cases project. Bidder to furnish OEM self- certification with the name of the cities.
2. OEM or its authorized partner should have local 24*7 support office / spare depot in Madhya Pradesh. If in case there is no local office in the state of Madhya Pradesh, in such case bidder will be required to submit undertaking of getting a 24*7 support office / spare depot of OEM in the state of Madhya Pradesh.
3. The solution should be implemented and compliant to industry open standard commercial-off-the-shelf (COTS) applications that are customizable.
4. OEM should have 24x7x365 technical assistance support center in India. TASC should provide online website and phone number to register service request, service request can be raise by bidder and customer.

Pre-Qualification for Cloud Service Provider

1. The Cloud Service Provider has to be empaneled with MeitY or should be in compliance with the requirements of such empanelment. The link of empaneled agencies and other requirements are available on website of MeitY. The link for the empanelment list is : http://meity.gov.in/content/gi-cloud-meghraj

Note:

1. For International projects, original client certificate and other documents shall be duly verified by Indian embassy / High Commission. The same shall be submitted with the bid document.

2. For projects where fee has been received in any currency other than Indian Rupees, than the foreign currency conversion rate available on Reserve Bank of India's portal as on the date of publication of the tender document shall be used for conversion of amount in foreign currency to Indian Rupees equivalent.

3. Bidders are allowed to submit experience in terms of technical qualification of their holding company and/or subsidiary company only. However, the parent/ subsidiary company of the Bidder should on its own meet the technical experience as stipulated in this RFP and should not rely for meeting the technical experience criteria on its sister subsidiary/ co-subsidiary company or through any other arrangement like Technical Collaboration agreement. For the purpose of this clause,

    a. a 'holding company', in relation to one or more other companies, means a company of which such companies are subsidiary companies; and

    b. a 'subsidiary company' in relation to any other company (that is to say the holding company), means a company in which the holding company— (a) controls the composition of the Board of Directors; or (b) exercises or controls more than one-half of the total share capital at its own

4. For the purpose of evaluation criteria, if the bidding company (the lead bidder in case of consortium) is 100% subsidiary of an international or Indian company then the lead bidder's parent company's or parent company's other subsidiary relevant experience can be considered as lead bidder's experience.

5. Projects executed for bidder's own or bidder's group of companies shall not be considered.

3.6 Technical Evaluation Framework

The Bidder's technical solution proposed in the Technical Evaluation bid shall be evaluated as per the evaluation criteria in the following table.

Section #	Evaluation Criteria	Total Marks
A	Bidder's Organizational Strength and Experience	450
B	Proposed Solution, Approach & Methodology (Common Cloud based DC and DR approach, Innovation, Command Center Platform Support during the contract period – L1, L2 and L3, etc.)	300
C	Resources Planning, Project Governance and Key Personnel	150
D	Technical Presentation (Common Cloud based DC and DR approach, Innovation, Command Center Platform Support during the contract period – L1, L2 and L3, etc.)	100
Overall Technical Score Total		1000

Important: Qualification criteria for technical evaluation and progression to commercial evaluation stage.

- Minimum 50% of the maximum allotted marks in each section as given in the table above

  AND

- Minimum 70% marks of the overall technical score total.

N.B- Evaluation Committee (or a nominated party) reserves the right to check/validate the authenticity of the information provided in the Pre-qualification and Technical Evaluation criteria and the requisite support must be provided by the Bidder.

OEM representative should be present at the time of Technical Presentation at BSCDCL.

The following sections explain how the Bidders shall be evaluated on each of the evaluation criteria.

Technical bids of the Bidders qualifying in the Pre- Qualification criteria will be opened and will also be invited for doing the technical presentation.

3.6.1 Bidder's Organizational Strength and Experience (Total Mark -450)

#	Criteria	Criteria Details	Documentary Evidence	Marks Allotted
1.	MSI should have an average annual turnover of at least INR 1000 Crores in any of the 3 financial years (FY 2013-14, 2014-15 and 2015-16)	Average annual turnover form IT system integration services / ICT system integration services/ communication infrastructure / city surveillance / utility management / Transport management / command & control center implementation in India. Turnover of any parent, subsidiary, associated or other related entity will not be considered. >1000 Crores to <= 1200 Crores – 5 Marks >1200 Crores to <= 1350 Crores – 10 Marks >1350 Crores to <= 1500 Crores – 20 Marks >1500 Crores – 30 Marks	Certificate from the Statutory Auditor / Chartered Accountant. In case Chartered Accountant certificate is submitted the said certificate also need to be counter signed by Company Secretary / authorized signatory of the bidder.	30
2.	CSP- Cloud service Provider capabilities	Single legal entity or its holding company, having annual revenue from the Data Centre or cloud related services for each of the last two financial years (2014-15 and 2015-16) either in India or Globally. ☐ INR 100 Crores- 90 Marks ☐ INR 75-100 Crores- 70 Marks ☐ INR 50-75 Crores- 50 Marks ☐ INR 20-50 Crores – 25 Marks	Certificate from the Statutory Auditor / Chartered Accountant. In case Chartered Accountant certificate is submitted the said certificate also need to be counter signed by Company Secretary / authorized signatory of the bidder.	90
3.	**Experience in Implementation and maintenance of large scale Utility**	MSI or its consortium members having experience in Implementation & maintenance of large Utility Management	Case study + Copy of work order/Client certificate detailing Scope & value +	60

	Management System in India or Abroad	System Project in last seven (7) financial years. Value of project should be at least of INR 10 crores. ☐ 3 citations (at least 1 should be successfully completed) =60 marks, ☐ 2 citation (at least 1 should be successfully completed) = 40 marks ☐ 1 citation successfully completed = 20 marks ☐ else 0 Marks	Completion/ Phase completion Certificates from the client In case the experience shown is that of the bidder's parent / subsidiary company, then the following additional documents are required: i. Letter from the Company Secretary of the bidder certifying that the entity whose experience is shown is parent/subsidiary Company. ii. Shareholding pattern of the bidding entity as per audit reports	
4.	**Experience in Implementation & maintenance of application in Cloud hosted environment in India or abroad**	MSI or its consortium members having experience in Implementation & maintenance of application in Cloud hosted environment in last 5 financial years. Value of project to be at least of INR 10 crores. ☐ 3 citations (at least 1 should be successfully completed) =60 marks, ☐ 2 citation (at least 1 should be successfully completed) = 40 marks ☐ 1 citation successfully completed = 20 marks ☐ else 0 Marks		60
5.	**Experience in Implementation of integrated Smart City / township / campus system including Command and Control Centre (CCC)**	MSI or its consortium members having experience in Implementation & maintenance of Command & Control Centre Project in last ten (10) financial years. Value of project to be at least of INR 10 crores. ☐ 3 citations (at least 1 should be successfully completed) =60 marks,		60

		☐ 2 citation (at least 1 should be successfully completed) = 40 marks ☐ 1 citation successfully completed = 20 marks ☐ else 0 Marks		
6.	**Experience in IT / Telecom services projects in last 7 years each of value greater than 50 Crores in India or Global.**	MSI or its consortium members having experience in IT / Telecom services projects in last 7 years each of value greater than 50 Crores in India or Global. ☐ 3 citations (at least 1 should be successfully completed) =60 marks, ☐ 2 citation (at least 1 should be successfully completed) = 40 marks ☐ 1 citation successfully completed = 20 marks ☐ else 0 Marks		60
7.	**City Command Center Digital Platform Experience**	Proposed platform for City Control and Command Centre by MSI should have been deployed in India or abroad on public cloud based data center in last 5 years. (MSI to get relevant citation and required documents as evidence from the OEM of City Control and Command Center Platform and submit along with other documents of technical bid.) • 4 citations (at least 1 should be successfully completed) =90 marks, • 3 citations (at least 1 should be successfully completed) =60 marks, • 2 citation (at least 1 should be successfully completed) = 30 marks • 1 citation successfully completed = 15 marks • else 0 Marks		90
Total				**450**

Note:

1. For parameter 3,4, 5, 6

i. Bidders are allowed to submit experience in terms of technical qualification of their holding company and/or subsidiary company only. However, the parent/ subsidiary company of the Bidder should on its own meet the technical experience as stipulated in this Volume and should not rely for meeting the technical experience criteria on its sister subsidiary/ co-subsidiary company or through any other arrangement like Technical Collaboration agreement. For the purpose of this clause,

   a. a 'holding company', in relation to one or more other companies, means a company of which such companies are subsidiary companies; and

   b. a 'subsidiary company' in relation to any other company (that is to say the holding company), means a company in which the holding company— (a) controls the composition of the Board of Directors; or (b) exercises or controls more than one-half of the total share capital at its own

ii. For the purpose of evaluation criteria, if the bidding company (the lead bidder in case of consortium) is 100% subsidiary of an international or Indian company then the lead bidder's parent company's or parent company's other subsidiary relevant experience can be considered as lead bidder's experience.

iii. For projects where fee has been received in any currency other than Indian Rupees, than the foreign currency conversion rate available on Reserve Bank of India's portal as on the date of publication of the tender document shall be used for conversion of amount in foreign currency to Indian Rupees equivalent Projects executed for bidder's own or bidder's group of companies shall not be considered.

3.6.2 Proposed Solution, Approach and Methodology (Total Marks-300)

Bidder has to provide answers of the below mentioned questions in form of write-up (maximum 3 A4 sheets per question except for question no 10, for which max 50 sheets are permitted) as a part of Technical Proposal evaluation.

Sr #	Questions	Maximum Marks
1.	Please explain your understanding of the project.	25
2.	Please provide the proposed solution for common cloud based DC and DR	20
3.	Please provide the proposed solution for common stack of applications to be hosted on common cloud based DC for city ICCC	20
4.	Please provide the proposed solution for network connectivity between common cloud based DC, DR, city ICCC and other applications to be integrated	20
5.	Please provide the proposed solution and network architecture for City ICCC	
6.	Please explain how would you ensure that the all 3 phases are completed within stipulated timeframe as defined in this RFP	20
7.	What will be approach towards the scalability, Interoperability and modularity features considering the future expansion of the project? The response to this question shall be given considering growth of Smart Cities as well as new applications or systems that may be envisaged / developed in the future.	20
8.	Please identify major risks for the project and also propose suitable mitigation plan for each of these risks.	15
9.	How the proposed solution ensures the fool proof security to the system from various threats including hacking attempts, internal threats, etc? Please explain in detail approach towards the security of the overall solution from external and internal threats	15
10.	What have been your key learnings from the similar projects and how do you propose to incorporate them in executing this assignment	15
11.	How SLAs mentioned under this RFP will be measured? What tools will be used for SLA measurement?	15
12.	What should be the Cloud Strategy with respect to scope of this RFP? Please elaborate on pros and cons of this strategy. Explain how the interoperability between DC and DR site is achieved for DR and backup purpose	15
13.	ICCC platform OEM roadmap for next 10 years along with planned L1, L2 and L3 support	25
14.	Please explain your detailed approach and methodology for executing this project	15
15.	Innovation in common platform and analytical layer for all city ICCC	30
16.	Innovation in ICCC solution.	30
	Total	**300**

3.6.4 Resource Planning (Total Marks-150)

#	Criteria	Criteria Details	Marks Allotted
1.	**Resource Deployment Plan & Governance structure**	Bidder would be evaluated for Resource Deployment Plan & Governance Structure	26
2.	**Program Manager**	Refer to Team Evaluation Matrix Below	14
3.	**Cloud DC / DR Expert**	Refer to Team Evaluation Matrix Below	14
4.	**Citizen Service/Municipal Domain expert**	Refer to Team Evaluation Matrix Below	8
5.	**Water SCADA or Electrical SCADA Expert**	Refer to Team Evaluation Matrix Below	8
6.	**GIS expert**	Refer to Team Evaluation Matrix Below	8
7.	**Command Center Design Expert (Civil)**	Refer to Team Evaluation Matrix Below	8
8.	**ITMS Expert**	Refer to Team Evaluation Matrix Below	8
9.	**Solution Architect**	Refer to Team Evaluation Matrix Below	8
10.	**Project Manager-Software**	Refer to Team Evaluation Matrix Below	8
11.	**Project Manager-Infrastructure**	Refer to Team Evaluation Matrix Below	8
12.	**Database Architect**	Refer to Team Evaluation Matrix Below	8
13.	**Security Expert**	Refer to Team Evaluation Matrix Below	8
14.	**Command and Control Centre management Expert**	Refer to Team Evaluation Matrix Below	8
15.	**Mobile App development Expert**	Refer to Team Evaluation Matrix Below	8
Total			**150**

Team Evaluation Matrix

Program Manager = 14 marks

a) Educational Qualification:

- BE / B. Tech / MCA with MBA/M. Tech = 2 Marks
- BE / B. Tech / MCA = 1 Marks
- Else 0

b) Certification :

- PMP / Prince 2 Certification = 2 Marks

c)Work experience in the capacity of Project/Program Manager in ICT implementation Projects:

- >=10 years = 6 marks
- >=8 and <10 year =4 Marks
- >=5 and <8 year =2 Marks
- Else 0

d)Project/Program management Experience in ICT implementation Project of value > 100 crores:

- >= 3 Projects= 2 Marks
- 2 Projects = 1 marks
- Else 0

e)Project/Program management Experience Smart City ICT implementation Project:

- 1 Project= 2 Marks
- Else 0

Cloud DC / DR Expert = 14 marks

a) Educational Qualification:

- **BE / B. Tech / MCA with MBA/M. Tech = 2 Marks**
- **BE / B. Tech / MCA = 1 Marks**
- **Else 0**

b) Certification :

- **Any professional certification = 2 Marks**

c)Work experience in the capacity of Cloud DC / DR Expert in ICT implementation Projects:

- **>=10 years = 6 marks**
- **>=8 and <10 year =4 Marks**
- **>=5 and <8 year =2 Marks**
- **Else 0**

d) Cloud implementation Experience in ICT implementation Project of value > 100 crores:

- **>= 3 Projects= 2 Marks**

- **2 Projects = 1 marks**
- **Else 0**

e) Experience Smart City ICT implementation Project:

- **1 Project= 2 Marks**
- **Else 0**

Citizen Service/Municipal Domain expert= 8 Marks

a) Educational Qualification:

- Bachelor's Degree in Engineering/MCA + MBA/PGDM (2 Years Full Time)= 2 Marks
- Else 0 Marks

b) Work experience in Implementation of Citizen Centric Service/Municipal domain ICT Projects:

- >=9 years = 3 Marks
- >=6 and <9 year =1 Marks
- Else 0

c) International work experience in Implementation of Citizen Centric Service/Municipal domain ICT Projects:

- At least 1 Project = 3 mark
- Else 0

Electrical or Water SCADA expert = 8 Marks

a) Educational Qualification:

- Bachelor's Degree in Engineering/MCA = 2 Marks
- Else 0 Marks

b) Work experience in Implementation of SCADA Projects:

- >=9 years = 4 marks
- >=6 and <9 year =2 Marks
- Else 0

c) International work experience in Implementation of SCADA Projects:

- At least 1 Project = 2 mark
- Else 0

GIS expert = 8 Marks

a) Educational Qualification:

- Bachelor's Degree in Engineering/MCA = 2 Marks
- Else 0 Marks

b) Work experience in Implementation of GIS Projects:

- >=9 years = 4 marks
- >=6 and <9 year =2 Marks
- Else 0

c) International work experience in Implementation of GIS Projects:

- At least 1 Project = 2 mark
- Else 0

Command Center Design Expert (Civil)= 8 Marks

a) Educational Qualification:

- Bachelor's Degree in Engineering/ Architect = 2 Marks
- Else 0 Marks

b) Work experience in designing of Command Center / Network Operating Centre Projects:

- >=9 years = 4 marks
- >=6 and <9 year =2 Marks
- Else 0

c) International work experience in designing of Command Center / Network Operating Centre Projects:

- At least 1 Project = 2 mark
- Else 0

Intelligent Transport Management System (ITMS) Expert= 8 Marks

a) Educational Qualification:

- Bachelor's Degree in Engineering/MCA = 2 Marks
- Else 0 Marks

b) Work experience in Implementation of ITMS Projects:

- >=9 years = 4 marks
- >=6 and <9 year = 2 Marks
- Else 0

c) International work experience in Implementation of ITMS Projects:

- At least 1 Project = 2 mark
- Else 0

Solution Architect= 8 Marks

a) Educational Qualification:

- Bachelor's Degree in Engineering/MCA = 2 Marks
- Else 0 Marks

b) Work experience as IT/ICT solution architect:

- >=9 years = 4 marks
- >=6 and <9 year = 2 Marks
- Else 0

c) International work experience as IT/ICT solution architect:

- At least 1 Project = 2 mark
- Else 0

Project Manager-Software = 8 Marks

a) Educational Qualification:

- Bachelor's Degree in Engineering/MCA = 2 Marks
- Else 0 Marks

b) Work experience as Project Manager in software Implementation Project:

- >=9 years = 4 Marks
- >=6 and <9 year = 2 Marks
- Else 0

c) International work experience as Project Manager in software Implementation Project:

- At least 1 Project = 2 Marks
- Else 0

Project Manager – IT/ICT Infrastructure= 8 Marks

a) Educational Qualification:

- Bachelor's Degree in Engineering/MCA = 2 Marks
- Else 0 Marks

b) Work experience as Project Manager in IT/ICT Infrastructure Project:

- >=9 years = 4 Marks
- >=6 and <9 year =2 Marks
- Else 0

c) International work experience as Project Manager in IT/ICT Infrastructure Project:

- At least 1 Project = 2 Marks
- Else 0

Database Architect= 8 Marks

a) Educational Qualification:

- Bachelor's Degree in Engineering/MCA = 2 Marks
- Else 0 Marks

b) Work experience as Database architect:

- >=9 years = 4 Marks
- >=6 and <9 year =2 Marks
- Else 0

c) International work experience as Database architect:

- At least 1 Project = 2 Marks
- Else 0

IT Security Expert= 8 Marks

a) Educational Qualification:

- Bachelor's Degree in Engineering/MCA = 1 Marks

- Else 0 Marks

b) Certification

- CISA= 2 Mark

c) Work experience as IT Security Expert:

- >=9 years = 4 Marks
- >=6 and <9 year = 2 Marks
- Else 0

d) International work experience as IT Security Expert:

- At least 1 Project = 1 Marks
- Else 0

Command and Control Centre (CCC) Expert = 8 Marks

a) Educational Qualification:

- Bachelor's Degree in Engineering/MCA = 2 Marks
- Else 0 Marks

b) Work experience as CCC Expert:

- >=9 years = 4 Marks
- >=6 and <9 year =2 Marks
- Else 0

c) International work experience as CCC Expert:

- At least 1 Project = 2 Mark
- Else 0

Mobile App development Expert= 8 Marks

a) Educational Qualification:

- Bachelor's Degree in Engineering/MCA = 2 Marks
- Else 0 Marks

b) Work experience as Mobile App development Expert:

- >=5 years = 4 Marks
- >=3 and <5 year =2 Marks
- Else 0

c) International work experience as Mobile App development Expert:

- At least 1 Project = 2 Marks
- Else 0

3.6.5 Demo and Presentation (Total Marks-100)

#	Criteria	Criteria Details	Marks Allotted
1	**Presentation (45 minutes presentation + 15 minutes Q&A)**	• Quality of presentation • Understanding of requirements • Innovation of the solution • Ability to clearly explain the proposed solution • Quality of responses given to queries of presentation panel • ICCC platform OEM roadmap for 24*7 support (L1, L2 and L3) for next 10 years	40
2	**Presentation on Uniqueness of Solution (Innovation & Futuristic Approach)**	Demonstrate uniqueness and fulfillment of proposed solution as per requirement of BSCDCL.	20
3	**Demonstration**	• Demonstration of Smart Governance Application or • Demonstration of Utility Management system or • Demonstration of Command and Control Centre or ITMS system or NOC system	40
Total			**100**

Note: The Presentation has to lead by proposed Program Manager and OEMs have to be present in BSCDCL during the presentation.

4. Award of Contract

4.1 Notification of Award

BSCDCL will notify the successful Bidder in writing by e-mail followed by courier to be confirmed by the Bidder in writing by email followed by courier.

4.2 Signing of Contract

After the notification of award, BSCDCL will issue Purchase Order (PO)/Letter of Intent (LOI). Accordingly, a contract shall be signed between successful bidder and BSCDCL or the agency designated by BSCDCL. As an acceptance of the PO/LOI, the Bidder shall sign and return back a duplicate copy of the Purchase Order to BSCDCL or the agency designated by BSCDCL. The bidder shall return the duplicate copy along with a Performance Bank Guarantee within 15 working days from the date of issuance of PO/LOI.
On receipt of the Performance Bank Guarantee, BSCDCL or the agency designated by BSCDCL shall enter into a contract with the successful bidder. The Master Service Agreement is provided in RFP.

4.3 Performance Bank Guarantee (PBG)

Within fifteen (15) working days from the date of issuance of LOI, the successful Bidder shall at his own expense submit unconditional and irrevocable Performance Bank Guarantee (PBG) to the BSCDCL. The PBG shall be from a Nationalized Bank or a Scheduled Commercial Bank in the format prescribed in Section 9 - Annexure 5 (a), payable on demand, for the due performance and fulfilment of the contract by the bidder.

This Performance Bank Guarantee shall be for an amount equivalent to 10% of total contract value. PBG shall be invoked by BSCDCL, in the event the Bidder:

a. fails to meet the overall penalty condition as mentioned in RFP or any changes agreed between the parties,

b. fails to perform the responsibilities and obligations as set out in the RFP to the complete satisfaction of BSCDCL,

c. Misrepresents facts/information submitted to BSCDCL

The performance bank guarantee shall be valid till satisfactory completion of Post Implementation Support. The performance bank guarantee may be discharged/returned by BSCDCL upon being satisfied that there has been due performance of the obligations of the bidder under the contract. However, no interest shall be payable on the performance bank guarantee.

In the event of the Bidder being unable to service the contract for whatever reason(s), BSCDCL shall have the right to invoke the PBG. Notwithstanding and without prejudice to any rights whatsoever of BSCDCL under the contract in the matter, the proceeds of the PBG shall be payable to BSCDCL as compensation for any loss resulting from the bidder's failure to perform/comply its obligations under the contract.

BSCDCL shall notify the bidder in writing of the exercise of its right to receive such compensation within 40 days, indicating the contractual obligation(s) for which the bidder is in default. BSCDCL shall also be entitled to make recoveries from the bidder's bills, performance bank guarantee, or from any other amount due to him, an equivalent value of any payment made to him due to inadvertence, error, collusion, misconstruction or misstatement.

In case the project is delayed beyond the project schedule as mentioned in RFP, the performance bank guarantee shall be accordingly extended by the Bidder till completion of scope of work as mentioned in RFP.

This Performance Bank Guarantee shall be valid only up to the completion of the period of 'Go- Live' + 84 months for the Solution.

`

On satisfactory performance and completion of the order in all respects and duly certified to this effect by the Project Coordinator, Contract Completion Certificate shall be issued and the PBG would be returned to the Bidder.

4.4 Warranty & Maintenance

Bidder shall also provide complete maintenance support for all the proposed integrated solution as outlined in this RFP for a period of Sixty months from the date of go-live i.e. "Go-Live" + 60 months. "Go-live" is the date on which the proposed solution is completely operational as per the requirements provided in this RFP and all the acceptance tests are successfully concluded to the satisfaction of BSCDCL.

During the warranty period, the bidder shall warrant that the goods supplied under the contract are new, unused, of the most recent version/models and incorporate all recent improvements in design and materials unless provided otherwise in the contract. The bidder further warrants that the goods supplied under this contract shall have no defects arising from design, materials or workmanship.

BSCDCL or designated representatives of the bidder shall promptly notify successful bidder in writing of any claims arising under this warranty. Upon receipt of such notice, the bidder shall, within the warranty period and with all reasonable speed, repair or replace the defective systems, without costs to BSCDCL and within time specified and acceptable to BSCDCL.

If the successful bidder, having been notified, fails to remedy the defect(s) within the period specified in the contract, BSCDCL may proceed to take such reasonable remedial action as may be necessary, at the successful bidder's risk and expense and without prejudice to any other rights, which BSCDCL may have against the bidder under the contract.

During the comprehensive warranty period, the successful bidder shall provide all product(s) and documentation updates, patches/fixes, and version upgrades within 15 days of their availability and should carry out installation and make operational the same at no additional cost to BSCDCL.

The successful bidder hereby warrants BSCDCL that:

The implemented integrated solution represents a complete, integrated solution meeting all the requirements as outlined in the RFP and further amendments if any and provides the functionality and performance, as per the terms and conditions specified in the contract.

ii. The proposed integrated solution shall achieve parameters delineated in the technical specification/requirement.

iii. The successful bidder shall be responsible for warranty services from licensers of products included in the systems.

iv. The successful bidder undertakes to ensure the maintenance of the acceptance criterion/standards in respect of the systems during the warranty period.

4.5 Failure to agree with the Terms & Conditions of the RFP

Failure of the successful bidder to agree with the Terms & Conditions of the RFP shall constitute sufficient grounds for the annulment of the award, in which event BSCDCL may award the contract to the next best value bidder or call for new bids.

In such a case, BSCDCL shall invoke the PBG and/or forfeit the EMD.

Schedule 2 – Detailed Scope of Work

1.1 Introduction

MSI (along with its consortium partner) will be responsible for implementation and maintain the Cloud based common DC and DR along with City Integrated Control and Command Centre (ICCC) for 7 Smart Cities. The 7 cities are- Bhopal, Indore, Jabalpur, Ujjain, Gwalior, Sagar and Satna. The scope includes software/solution development and implementation, Information Technology (IT) and required Non IT infrastructure procurement, deployment, implementation and maintenance of the city ICCC systems and a common cloud based data centre. DR of this data centre will be on cloud based technology. MSI will also provide necessary network connectivity between all the city command and control centre and cloud based data centre for efficient operations.

BSCDCL, on behalf of other cities and State, may ask for addition of more cities under this project during the project duration.

The maintenance phase will be for a period of 5 (five) years after Go-Live. Post completion of the 5 year period, the contract can be extended, at discretion of BSCDCL and City SPVs, for additional two years on yearly basis or part thereof on terms and conditions that may be mutually agreed to.

MSI needs to design, implement and operate the common cloud based DC and DR along with city ICCC on turnkey basis. MSI needs to do the appropriate solution design and sizing for the project as per the scope of work and other terms and conditions of the RFP. In case MSI has not considered any component/service which is necessary for the project requirement, the same needs to be brought by the MSI at no additional cost to BSCDCL / City SPVs.

Integration of various services pertaining to IT projects (DIAL 100, Smart Parking etc.) of various cities is the key component of scope of work of MSI. For all the services which belongs to other department (other than Municipal Corporations) like DIAL 100- Police Department or DAIL 108- Health Department etc., providing the necessary information, access and approvals will be the responsibility of BSCDCL. In the event for any reasons (beyond the control of BSCDCL or MSI for particular service) the approvals are not provided by the other government department, the scope and the fee would be adjusted proportionately.

1.2 Overview of Scope

The snapshot of scope is as below:

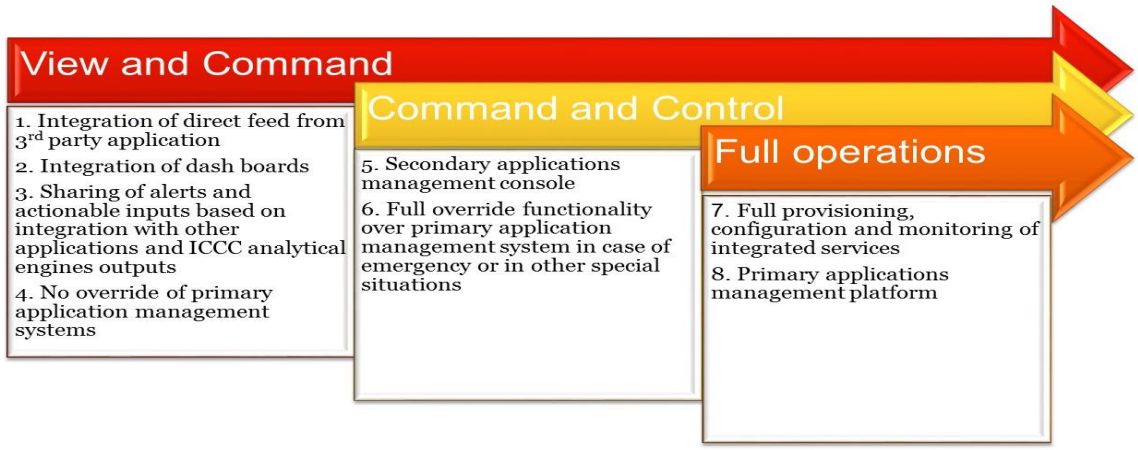
1. The MSI will conduct a detailed assessment and design a comprehensive technical architecture and project plan including:

    a. Design and establishment of state level Cloud based common data center and DR for all 7 cities. Disaster recovery will also be cloud based for this data center.
    b. Design and development of comprehensive application for city command and control operations. This application will also have an integrated platform (state and city level) for city operations for 7 cities and dashboard application that integrates various Smart City use cases on this platform.
    c. The common smart city software platform would be hosted at cloud.
    d. This platform would have facility of comprehensive viewing and performing operations at state level.
    e. There will be a provision for generating configurable reports through dashboard and also real time monitoring at state level.

f. City ICCC Module will be integrated various city level projects/initiatives. At City level, this application will have facility of city level operations on services which are integrated with city ICCC.
g. Establishment of city Integrated command and control center for 7 cities in MP.
h. Assessment of the business requirements and IT Solution requirements for ICCC and data center.
i. Design and build the solution for ICCC and Data Centre as per the Design Considerations
j. Plan for development, configuration and customization of software products
k. Conduct Integration test cases to achieve seamless integration with envisaged smart city systems and applications

2. MSI will design, customize, supply, implement and maintain the ICCC software platform with integration with three types of smart city components.

Illustrative example given below for Bhopal.
These components can be classified on the basis of their respective functions, in case of Bhopal these are:



A. Command and View:

Following are the components on which only view and command operations will be performed:

i. DIAL 100
ii. DIAL 108
iii. Traffic Management System
iv. Safe City Cameras Feed
v. Emergency Response and Disaster Management
vi. Met Department

B. Command and Control:
In command and control operations override functions will also be available. At command and control, there will be a provision of Management Console to provide override function**.**

Following are the components on which command and control operations will be performed specifically for Bhopal Smart City:

i. Smart Parking
ii. Public Bike Sharing
iii. Smart Pole & Smart Lighting
iv. Solid Waste Management Services

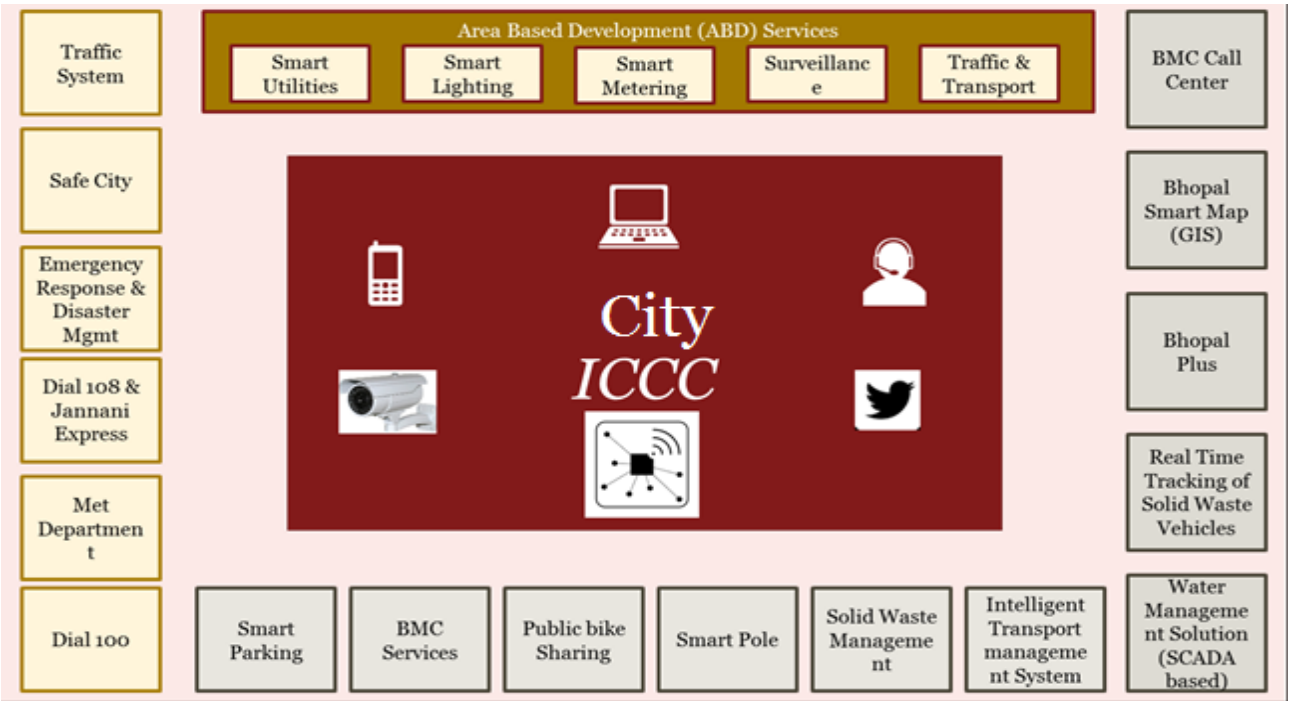
v. Intelligent Transport Management System
vi. Municipal Corporations Call Centre & Municipal Corporations Services
vii. Bhopal Smart MAP (GIS)
viii. Bhopal Plus (App)
ix. Water Management System
x. Dynamic Market Place (Mayor Express)
xi. Crowdsourcing Data
xii. Fire Brigade Control System
xiii. Solar Roof Top

C. Full Operations:

As the name suggest, full operations will be full-fledged system equipped with all the operations rights to its specified users. This will have integration with various components with data feed view and sharing. It will also have management console to perform all the operations. Full operations will be performed on the components with following services. These will be provided under Area Based Development (ABD).

i. Utilities
ii. Lighting
iii. Metering
iv. Surveillance

Following is the indicative diagram which depicts the City Integrated Command and Control Centre integrated with various other IT components of Bhopal Smart City.



For Indore, Ujjain, Jabalpur, Gwalior, Sagar and Satna these initiatives are mentioned in Annexure of this RFP

D. MSI will design, supply, install and maintain City Command and Control Centre for each city comprising of:

   a. Video Wall & controller system
   b. Integrated Command and Control Centre Application.
   c. Operator Workstation and accessories
   d. Local Server Room
   e. Situation Room
   f. Civil Work like false floor, ceiling, ducting etc.

E. MSI will be required to conduct the city survey of the existing systems and accordingly define the implementation roadmap for ICCC for each city.

   a. Assessment of the business requirements and IT Solution requirements for city ICCC
   b. Design and build the solution for city ICCC as per the Design Considerations
   c. Design and build the Cyber Security infrastructure
   d. Plan for development, configuration and customization of software products
   e. Conduct Integration test cases to achieve seamless integration with envisaged smart city systems and applications

F. MSI will design, supply, install and commission the network and backbone connectivity
G. MSI will supply, install and maintain Infrastructure including Hardware and Application Software
H. MSI will supply, install and maintain Infrastructure including ICT and non- ICT components

I. MSI will provide and maintain the Hardware and Software IT infrastructure services at Data Centre/ Recovery Center hosted on cloud for recovering the data in case of crash of server at the city ICCC.

J. MSI will be required to provide Help Desk in each city ICCC for following activities:

   a. Technical and operational support of the system
   b. Maintenance of the IT and Non-IT Infrastructure
   c. Technical & Operational Manpower for smooth running of the system
   d. This help desk will also act as a functional call center to send instructions to various field agencies to do the needful.

K. MSI will provide the design and area specific requirement for the Physical building for city ICCC for all 7 cities. MSI must appoint Civil Architect and Interior designer for doing a designing and defining the requirements for each city ICCC (with minimum area of 10,000 sq. feet).

L. ICCC design must be futuristic in nature keeping in view the future requirements of physically collocating all the other control and command centers under one roof.

M. MSI should present design of the ICCC using 3D modelling, which can be refined and present the final view of the actual ICCC (with minimum area of 10,000 sq. feet).

N. MSI will supply, install and maintain the Integrated Building Management System (IBMS) with following sub systems for ICCC building:

   a. Access control system
   b. Surveillance System
   c. Physical security system

d. Building Management System for controlling and monitoring the building's mechanical and electrical equipment such as HVAC, Water supply, fire systems etc.

1.3 Detailed Scope of Work

1.3.1 Preparation of detailed technical architecture and project plan

After signing of contract, the MSI needs to deploy the team proposed for the project at site during development phase to ensure that a Project Inception Report is submitted to BSCDCL which should cover following minimum aspects:

a. Project Charter, Project concept understanding
b. Names of the Project Team members, their roles & responsibilities
c. Approach & methodology to be adopted to implement the Project (which should be in line with what has been proposed during bidding stage, but may have value additions / learning in the interest of the project)
d. Define an organized set of activities for the project and identify the interdependence between them.
e. Establish and measure resource assignments and responsibilities
f. Highlight the milestones and associated risks
g. Responsibility matrix for all stakeholders
h. Communicate the project plan to stakeholders with meaningful reports.
i. Measure project deadlines and performance objectives.
j. Detailed Project Plan, specifying dependencies between various project activities / sub-activities and their timelines.
k. Define Project Progress Reporting Structure which should cover the following parameters:
    i. Cumulative deviations from the schedule date as specified in the finalized Project Plan
    ii. Corrective actions to be taken to return to planned schedule of progress
    iii. Plan for the next week
    iv. Proposed revision to planned schedule provided such revision is necessitated by reasons beyond the control of MSI
    v. Support needed
    vi. Highlights/lowlights
    vii. Issues/Concerns
    viii. Risks/Show stoppers along with mitigation

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

The MSI as part of the feasibility study shall conduct the following stages for activities for finalization of technical architecture of the proposed city Integrated Control and Command Centre (ICCC).

1.3.1.1 Requirement Gathering Stage

The MSI shall conduct the detailed assessment of the business requirements and IT Solution requirements for ICCC (in each city) and cloud based common data centre 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 BSCDCL and city SPV. For city specific needs MSI will consult city SPV and other relevant stakeholders, BSCDCL will play role of facilitation as project execution agency. While doing so, MSI at least is expected to do following:

a. MSI shall study and revalidate the requirements given in the RFP with BSCDCL and submit as an exhaustive FRS document.

b. MSI shall translate all the requirements as captured in the FRS document into SRS.

c. All the documents created for City ICCC will be submitted to CITY SPV and for common Cloud based DC and DR along with common applications will be submitted to BSCDCL for review and approval.

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

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

f. MSI must get the sign off from user groups formed by BSCDCL / City SPV.

g. For all the discussion with BSCDCL / City SPV team, MSI shall be required to be present at BSCDCL / City SPV office with the requisite team members.

h. BSCDCL / City SPV will provide necessary support for gathering required information and obtaining required data access for future technical integrations of external systems with ICCC from other departments.

i. MSI will prepare interoperability traceability matrix with third party systems (existing legacy systems with city ICCC) in consultation with BSCDCL / City SPV and other relevant stakeholders (of external systems). Interoperability is an ability of one system to interact with another system. This matrix will cover all the use cases of system interaction and data movement.

1.3.1.2 Design Stage

The MSI shall design and build the solution for each city ICCC and common data centre (cloud based hosting) as per the Design Considerations detailed in **Annexure – V**. The solution proposed by MSI should comply with the design considerations requirements as mentioned therein.

1.3.1.3 Development Phase

The MSI shall carefully consider the scope of work and provide a solution that best meets the proposed city ICCC requirements. Considering the scope set in this RFP, the MSI shall carefully understand the various prevailing Smart City solutions for each of the 7 cities which are currently under implementation and envisaged in near future under the Smart City Programme of various smart cities 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 shall be responsible for supplying the application and licenses of related software products and installing the same so as to meet ICCC requirements.
ii. MSI shall have provision for procurement of licenses in a staggered manner as per the actual requirement of the project.
iii. The 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. The MSI shall report any exceptions to license terms and conditions at the right time to BSCDCL. However, the responsibility of license compliance solely lies with the MSI. Any financial penalty imposed on BSCDCL 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, the MSI shall supply:

- Software & licenses.
- Supply tools, accessories, documentation and provide a list of the same. Tools and accessories shall be part of the solution.
- **System Documentation**: System Documentation both in hard copy and soft copy to be supplied along with licenses, document updates and shall include but not limited to following:
    - Functional Requirement Specification (FRS)
    - High level design of whole system
    - Low Level design for whole system / Module design level
    - System Requirements Specifications (SRS)
    - Any other explanatory notes about system
    - Traceability matrix
    - Technical and product related manuals
    - Installation guides
    - User manuals
    - System administrator manuals
    - Toolkit guides and troubleshooting guides
    - Other documents as prescribed by BSCDCL
    - Quality assurance procedures
    - Change management histories
    - Version control data
    - SOPs, procedures, policies, processes, etc. developed for BSCDCL
    - Programs:
        - Entire source codes
        - 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
        - Interoperability Testing
        - Overall System Testing
        - Acceptance test cases
- The above mentioned documents are required to be updated and to be maintained updated during entire project duration. The entire documentation will be the property of BSCDCL.

b. Bespoke (Custom Developments)

i. The successful MSI shall identify, design and develop the customization for components/functionalities that are required to address the requirements mentioned in this RFP.
ii. The MSI shall supply the following documents along with the developed components:

- Business process guides
- Program flow descriptions
- Data model descriptions
- Sample reports
- Screen formats
- Frequently asked question (FAQ) guides
- User manual
- Technical manual
- Any other documentation required for usage of implemented solution

1.3.1.4 Integration & Testing Phase

The Command and Control Centre Application (CCCA) at ICCC should be integrated with data feeds of the various Smart City systems envisaged under the each Smart City Programme.

Illustrative example for Bhopal Smart City:

i. Integration with Smart Parking
ii. Integration with Public Bike Sharing
iii. Integration with Smart Pole & Smart Lighting
iv. Integration with Solid Waste Mgmt. Services (Tracking of Solid Waste Vehicles)
v. Integration with Intelligent Traffic Management System (Police)
vi. Integration with Municipal Corporations Call Centre & Municipal Corporations Services
vii. Integration with Bhopal Smart MAP (GIS)
viii. Integration with Bhopal Plus
ix. Integration with DIAL 100
x. Integration with DIAL 108 & Jannani Express
xi. Integration with Transport Management System (BCLL)
xii. Integration with CCTV Surveillance (Police Deptt.)
xiii. Integration with Dynamic Market Place (Mayor Express)
xiv. Integration with Emergency Response and Disaster Mgmt.
xv. Integration with Water Management System
xvi. Integration with Met Department (Local Weather Forecast)
xvii. Integration with Area Based Development (ABD) Services
    - Utilities
    - Lighting
    - Metering
    - Surveillance
xviii. Integration with Crowdsourcing Data
xix. Integration with Fire Brigade Control System
xx. Integration with Solar Roof Top System
xxi. Any other services implemented in near future during the project period*

For Indore, Ujjain, Jabalpur, Gwalior, Sagar and Satna these initiatives are mentioned in Annexure of this RFP

*These other services will be additional work and will be taken up as "Change request" following the process defined in Schedule 3 of this RFP. Change request will be given by each individual city based on their requirement.

Broadly there are four kinds of data feed possible from all of the above systems. The software solution provided by MSI should have the capability to integrate these all four types of data.

Video Feed	CCTV Cameras or other Cameras
Sensor Data	SCADA Sensors, Environmental Sensor, SWM Vehicles, Smart Lights Sensor Data, Smart Parking Sensor Data
Structured Data Packets	SCADA GIS Data, DIAL 100 (GPS Co-ordinates of vehicles), Alert messages, ITMS, Bhopal Plus App,
Voice Call	Calls from DIAL 108 call center, DIAL 100, IVRS System.

The 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.

The detailed testing requirements are mentioned in subsequent section.

1.3.1.5 Integration of Future IT initiatives

The software solution should be scalable and modular in structure and should be able to integrate other future IT initiative of various Smart Cities of MP. The bidder should estimate and provide estimated cost of extra service integration in terms of man month rate (Rate Card). The Rate card will be valid for 5 (five) years. This rate card will be for extra work only and it should not be the part of commercial bid.

1.3.1.6 Go-Live Preparedness and Go-Live

a. MSI shall prepare and agree with BSCDCL / City SPV, the detailed plan for Go-Live for each city ICCC which should be in-line with City SPV's implementation plans.

b. MSI shall prepare and agree with BSCDCL / City SPV, the detailed plan for Go-Live for cloud based common data center which should be in-line with State's implementation plan as mentioned in RFP.

c. As per clause 2.6.20 Go-Live for ICCC will be considered when the identified 10 services are integrated, tested, and operational from ICCC.

d. These 10 services will be different for each city.

e. The MSI shall define and agree with BSCDCL, the criteria for Go-Live for each city ICCC.

f. The MSI shall ensure that all the system integration is done with existing systems of agreed 10 services.

g. MSI shall submit signed-off UAT report (issue closure report) for each city ICCC ensuring all issues raised during UAT are being resolved prior to Go-Live.

h. MSI shall ensure that Go –Live criteria as mentioned in User acceptance testing section is met and MSI needs to take approval from BSCDCL team on the same.

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

1.3.2 Procurement, Supply, Installation and Commissioning of IT infrastructure at ICCC

The MSI shall be responsible for procurement, supply and installation of entire ICT hardware and software infrastructure at each City Integrated Command and Control Centre (ICCC) for successful operations of the systems. The Primary Data Centre and DR both of all the smart cities will be on cloud. The ICT infrastructure includes servers, storages, back up, networking, security equipment, operating systems, database, enterprise management system, help desk system, and other related IT infra required for running and operating the envisaged system. The ICT infra procurement will be planned considering the below factors:

a. Ensure redundancy for all the key components to ensure that no single point of failure affects the performance of the overall system
b. Support peak loads
c. MSI will not procure Infrastructure including Hardware, COTS Software licenses and other system software etc. at the start of the project, but will procure after discussion and receipt of go ahead from BSCDCL / City SPV.
d. MSI shall optimize procurement of ICT infrastructure i.e. the equipment shall not be procured earlier than its requirement.
e. Virtualization technologies to be used to reduce the physical space required for hosting and storage at city ICCC.
f. ICT infra deployed for ICCC should be dedicated for the project and MSI shall not use the same for any other purpose.
g. The ownership of infrastructure for Cloud based common DC and DR along with licenses of common hosted applications for all 7 smart cities command centers shall get transferred to BSCDCL after "Acceptance and Go Live" of such items by BSCDCL/ appointed TPAs.
h. The ownership of infrastructure for City ICCC shall get transferred to City SPV after "Acceptance and Go Live" of such items by city SPV/ appointed TPAs.

i. MSI to ensure warranties/AMCs are procured for all the hardware components for entire duration of the project. For software components the support from OEM to be obtained for prescribed components. There would be a mechanism to verify these details on annual basis.

1. Following are the benchmark requirements which the MSI shall comply while designing the ICCC:

a. Design, Supply, Installation and Commissioning of IT Infrastructure including site preparation of ICCC.
b. Establishment of LAN and WAN connectivity with cloud based data center, ICCC and connectivity of individual Command centers with ICCC.
c. Application Integration Services within each city ICCC building premises
    - Indoor CCTV Cameras would be required to be installed to monitor the physical access of the system from remote location
    - Physical Access to the building of Command and Control Centre should be armed and it must be possible to even depute police personnel for physical security of the premises if felt necessary.

- Networking & Security Infrastructure and other associated IT Components.

d. 24 x 7 Helpdesk and other monitoring and management services.
e. Purchase of all the Non IT and IT Equipment for the ICCC.
f. Physical infrastructure components for each city ICCC such as UPS, Diesel Generator Units, Power, and cabling for power and data connectivity, etc. The recurring charges of diesel consumption for DG set will be borne by MSI.
g. IT Infrastructure components such as Servers, Databases, System Software , Networking & Security components, Storage Solution, Software and other IT components required for the ICCC Project.
h. No Products supplied under the RFP should be nearing their date of "end of life". The MSI is supposed to provide the declaration at the time of delivery and installation.
i. All IT equipment models offered should be latest released with bundled version update.
j. Seamless Integration with other Smart City Systems and applications with city ICCC.
k. Procurement and supply of requisite licenses (Commercial off the shelf - COTS), Installation and implementation (including configuration /customization and Testing) of proposed ICCC.
l. All documentation generated inclusive of IT architecture, functional specifications, design and user manuals of the IT solution and documentation of non-IT components during design, installation and commissioning phase shall always be made available to the BSCDCL.
m. Standard business process management framework should be followed for workflow management with capabilities of configurability at user level.
n. Acceptance of the source code is by installing and generating the object code on a test environment performing identically to that of the production environment.

2. The MSI shall provide system integration services to customize and integrate the applications procured. The ICCC application proposed by the MSI should have open APIs and should be able to integrate and fetch the data from other third party systems already available or coming up in the near future.

3. As part of preparing the final bill of material for the physical hardware, the successful bidder will be required to list all passive & active components required in the command and control centre.

   a. The bill of material proposed by the MSI bidder will be approved by BSCDCL for its supply and installation. Indicative IT Infrastructure to be commissioned as part of the ICCC project at Command and Control Centers are as under:
      i. Servers (inclusive of OS)
         - Application Servers
         - Enterprise Backup Server
         - Failover Servers for application Servers
         - Any other Server required to the cater to the scope of work mentioned in this
      ii. Application & System Software
         - Integrated Command and Control Centre Application
         - Enterprise Management Software (EMS)
         - GIS software
         - RDBMS (if required)
         - Anti-virus Software
         - Backup Software
         - Virtualization software
         - Host Intrusion Prevention System (HIPS) software
         - Security Information & Event Management (SIEM) software

- Customised Software to cater to requirements of Project Requirements

iii. Other systems

- Primary Storage Solution
- Secondary Storage Solution
- Storage Management Solution
- Core Router
- Blade Chassis
- Core and Access Switches
- Intranet and Internet Routers
- KVM Switches
- Firewall
- IP Phones
- Racks (Caged)
- Indoor Fixed Dome Cameras
- All required Passive Components

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

4. The MSI shall prepare the overall data centre establishment & 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 setting up the data centre shall be approved by BSCDCL. The detailed plan shall be also comprise of the scalability, expandability and security that such data centre will implement under this project.

5. The MSI shall establish a state of the art Command Centre, the key components of the Command Centre will be as follows:
    i. Video Walls
    ii. Operator workstations
    iii. IP Phones
    iv. Network printer
    v. Indoor Fixed Dome Cameras for Internal Surveillance
    vi. Active Networking Components (Switches, Routers)
    vii. Passive Networking Components
    viii. Electrical Cabling and Necessary Illumination Devices
    ix. Fire Safety System with Alarm
    x. Access Control System (RFID/ Proximity based, for all staff)
    xi. Full Biometric System to control entry / exit
    xii. Office Workstations (Furniture and Fixtures)
    xiii. Comfort AC
    xiv. Inline UPS (12 hour backup) – 100% for ICT equipment and 50% for lighting
    xv. Furniture and fixtures

6. Benchmark specifications for various items mentioned above are given in the **Annexure 1 and 2** to this RFP document. The MSI is required to size and provide IT infra to meet the project functional requirements and Service Level Agreements (SLAs).

7. The 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.

1.3.3 Open Data Platform

The ICCC software solution should have provision for open data platform. The intent for creation of open data platform is to share the data with general public which is useful for citizen. The open data platform should be able to share the APIs for development of useful application for public in general. Open data platform should be implemented as the implementation guidelines issue by Govt. of India and it should adhere to the open data policy of Govt. of India.

1.3.4 Document Management

a. System should support the storing of document (Image & Metadata)
b. Support for archiving a large number of file formats. The system should support all commonly used file formats as MSOffice, Acrobat, TIF, JPEG, GIF, BMP, etc.
c. Provision for an integrated scanning engine with capability for centralized and decentralized Scanning & Document Capturing. The scanning solution should directly upload documents in Document management system.
d. Association of the document with Workflow Management System
e. Movement of the document based on selected parameters
f. Provision to edit the document Metadata
g. Versioning of the document
h. Provision for marking comments
i. Archival of data on pre-defined parameters
j. Role based access to the documents
k. Final Decision by the Decision Authority
l. Should be platform independent and should support both Linux and Windows both with and without virtualization. It should support multiple databases i.e. MSSQL, Oracle and Postgre.
m. The inbuilt image viewer shall support comprehensive annotation features like highlighting, marking text, underlining putting sticky notes on documents, and support for text and image stamps etc.
n. Should include record management to manage lifecycle of documents through record retention, storage, retrieval and destruction policies and should be certified for record management standard like DoD 5015.02/ISO 15489.

1.3.5 Workflow Management System

a. Movement of Proposals on various parameters
b. Facility to mark the application to pre-defined hierarchy
c. Inbox for officers (listing applications received)

d. FIFO principle for taking action on application
e. Creation of a Note Sheet for Scanned Documents
f. Alerts for delay in action
g. Compliance to workflow standards: BPMN, BPEL and WFMC
h. Shall support Inbuilt Graphical workflow designer for modelling complex Business Processes using drag and drop facilities.
i. Information/Alert to be sent to higher authority in case of delay in action by specific employee of the department
j. Pre-defined scrutiny for citizen applications
k. Display of all application data during scrutiny process
l. Check-list for rejection
m. Should have inbuilt Rule Engine for defining rules
n. Facility to mark the application to other officer
o. Facility to mark the application to other department for their NOC / Comments / Input
p. Final Decision by the Decision Authority
q. Shall provide graphical and tabular tools to create reports and view progress of each individual process.

1.3.6 File Tracking System

a. Scanning & Marking the inward to the respective department.
b. Capturing of DAKs using inbuilt scanning solution.
c. Incorporation of separate hierarchy for RTI letter movements & Commissioner Office.
d. Capturing of Fresh applications & Appeals
e. Tracking of the Inward and outward correspondence
f. File Closure to be carried out as per the final decision of respective authorities.
g. DAK and File Management system should build using robust Enterprise Document Management and Workflow Management and should comply with the Manual of Office Procedure (MOP), published by the Department of Administrative Reforms and Public Grievances (DARPG).
h. Shall have an In-built Web based Text Editor with basic functionalities such as bold, alignment, font, color etc. for writing the notes.
i. The system shall provide a facility to view correspondences (DAKs) on RHS and indexing fields on LHS.
j. Shall support the Whitehall view of the file. The system shall replicate the Present file handling in the same manner as followed i.e. electronic files shall give the same look and feel of Physical file with documents on the right hand side and green note sheet on the left hand side.

1.3.7 Data Analytics Capabilities

a. The ICCC software solutions should have inbuilt capability of data analytics/ business intelligence.
b. The Data Analytics/ BI Tool of software solution should work as single platform for analyzing data coming/input from all the IT components/initiative of Bhopal smart city like DIAL 100, DIAL 108 or Safe City project.
c. The system should be able to generate report in the user defined manner.

d. There should be a provision for a dash board which may take input from various system like individual sensors of multiple IT components (SCADA sensor, Environment sensors etc.)
e. Apart from basic analytics system should also have provision to perform Predictive Analysis.
f. User should be able to choose any permutation and combinations of data fields to perform predictive analysis.
g. System should be able to predict the events, make scenarios which helps in decision making to city authorities.
h. The Data analytics/BI tool should have ability to analyze the useful information and sharing it with general public. For example in case of water supply effected areas and traffic situation awareness etc.
i. System should have capabilities to suggest best response options on the basis of current and historic data sets.
j. Solution should enable the department to monitor activities and operations relating to the citizen (Municipal) service being provided, feedback and grievances received
k. Solution should help department understand the level of responsiveness of the officers concerned in terms of their response to the grievances.
l. The solution should also contain abilities for forecasting and scenario analysis, this will help the department understand the trends of different concern areas.
m. Forward looking decision making – BI and analytics tool provide the predictive and forecasting capabilities which can help department in forward looking policy and decision making.
n. Analysis of citizen sentiment across topics as represented through news and social media
o. Identification of recently emerging and trending topics of interest
p. Providing analytical platform for identification of misclassified events reported by citizens and inadequacies in action taken versus relief requested
q. System shall provide an Enterprise Reporting and Visualization solution to author, manage, and deliver all types of highly formatted reports
r. The solution should have mining, analytical and querying capabilities, and should be able to interoperate with other DBMS.
s. The BI Platform should have the capability to schedule reports on the basis of a time calendar i.e. by hour, day, week, month, etc.
t. The BI Platform should have the capability to schedule reports on the basis of a trigger or an occurrence such as an email, database refresh, etc.
u. Solution should provide capability to :
    - Understand issues and concerns of citizens in a quick and effective manner
    - Monitor progress of grievances and quality of grievance redressal
    - Understand special / specific needs for different part of cities / subject areas affecting citizens (such as water, electricity etc.)

1.3.8 Helpdesk

a. MSI will be required to provide Help Desk cum Contact center in each city ICCC for following activities:
    - Technical and operational support of the system
    - Maintenance of the IT and Non-IT Infrastructure

- Technical & Operational Manpower for smooth running of the system
- This help desk will also provide support to do the effective incident management in case of any emergency or disaster

In case of delay of responses or breach of SLAs in terms of resolution for any emergency, this help desk will play a critical role of getting services rendered effectively where ever needed.

b. This help desk will also act as a functional call center to disseminate actionable tasks to various field agencies to do the needful.

1.3.9 Disaster Management

MSI has to provide a separate module of Disaster Management as part of software solution. The Disaster Management module should be able to collect, gather and analyze the critical data of city from various components. The system should be able to create a strategic view or big picture of probable disaster. The system should be intelligent enough to make decisions that protect life and property. The system should disseminate such decisions to all concerned agencies and individuals. The critical data elements my decided in consultation with BSCDCL. The system should be able to use predictive analysis which can finally reduce response time and improve SLAs. Disaster Management module should be able to communicate or to be integrated with National Emergency Operation Centre (NEOC) of National Disaster Response Force (NDRF) based on defined SOPs. The Disaster Management system should be in compliance to applicable laws.

The Disaster management module should have interoperability between cities, here it refers that disaster management module of any city should be able to cater the disaster management operation of any of the other 6 city.

Standard Operating Procedures (SoPs) must adhere with the Governance structure of BSCDCL and Municipal Corporations, as in case of any incident or disaster decision making ability lies with the authority.

1.3.10 Integration of GIS Platform

Each city may have its own GIS application for providing GIS MAP based services. The MSI should be able to integrate these GIS layers on user interface of command and control software application.

MSI will be required to study the current GIS platform and enhance the same as per the requirements for city and it's ICCC.

1.3.11 Data Centre Solution and Disaster Recovery (DC/DR)

BSCDCL is looking for a Cloud Service Provider (CSP) for providing Cloud Services such as:

- Managed hosting (VM instances & Storage)
- Auto Scaling
- Network Connectivity
- IaaS (Infrastructure as a Service)
- DR as a Service
- Self Service provisioning Portal

- MIS, Reporting Services

The MSI shall be responsible for establishing/providing cloud based hosting for applications of all the 7 cities. The MSI shall be responsible for establishing complete data center solution including design, procurement, supply and installation of entire ICT hardware and software infrastructure at data center. The Data Center will be planned considering the below factors:

a. Data Centre should be minimum Tier 3+ as per the Uptime Institute/ EIA-TIA 942 standards.
b. Ensure redundancy for all the key components to ensure that no single point of failure affects the performance of the overall system
c. Support peak loads
d. MSI shall optimize procurement of ICT infrastructure i.e. the equipment shall not be procured earlier than its requirement.
e. Virtualization technologies to be used to reduce the physical space required for hosting
f. ICT infra deployed for ICCC should be dedicated for the project and MSI shall not use the same for any other purpose.
g. The ownership of Data Centre shall get transferred to BSCDCL after "Acceptance and Go Live" of such items by BSCDCL/ BSCDCL appointed TPAs.
h. MSI to ensure warranties/AMCs are procured for all the hardware components for entire duration of the project including O&M Phase (1+5 years). For software components the support from OEM to be obtained for prescribed components. There would be a mechanism to verify these details on annual basis.
i. MSI shall provision skilled and experienced manpower resources to administer and manage the entire system at data center (Managed Services).
j. Data Center should be as per Telecommunications Infrastructure Standard for Data Center and should be Certified 27001.
k. Access to the Data Center Space and physical access to the place would be given only to the authorized personnel.
l. Indoor CCTV Cameras would be required to be installed to monitor the physical access of the system from remote location
m. Physical Access to the building hosting Data Center should be armed and it must be possible to even depute police personnel for physical security of the premises if felt necessary.
n. Networking & Security Infrastructure and other associated IT Components.

1.3.12 Local Server Room (at city ICCC)

a. MSI shall propose to create a Local Server Room in the each city ICCC premises, which will help in storing local video feeds for 7 days.
b. MSI shall do the necessary civil work for the Local Server room.
c. Local video feeds will be archived in flash drives for 30 days. After which incident specific feed will only be saved on cloud based DC.
d. MSI shall do the required sizing of the Local Server Room based on the quantum of video feeds planned to be received.
e. MSI shall procure the required hardware for establishing the local server room.

1.3.13 Situation Room (at city ICCC)

a. MSI shall propose to create a Situation Room in the each city ICCC premises, which will help top management of Smart Cities to monitor any real time incident situation and take necessary actions.

b. MSI shall do the necessary civil work and furnishing for the Situation room.
c. This room will also be used to do the discussion on the analysis done by ICCC system based on the data feeds.
d. This room will provide privacy features like acoustic treatment and will have limited access (using access management system)
e. This room must have the following
   i. Small Video wall (1 x 2) with 55 inch screens
   ii. Video Conferencing facility
   iii. Sitting capacity for 20 personal on a round table (with table top touch screens/capacitive, 84")
   iv. 2 workstations (same as provided in ICCC) – these system should be capable of triggering any command on the ICCC system.

MSI must define Standard Operating Procedures (SoPs) for situation rooms. These SoPs must adhere with the Governance structure of BSCDCL and Municipal Corporations, as in case of any incident or disaster decision making ability lies with the Authority.

1.3.14 Disaster Recovery

a. MSI shall propose to host Applications and storage on cloud for complete Data Recovery (DR) operations.
b. MSI should select the Cloud Service Provider from who adheres the guidelines of MeiTY and empaneled vendors of MeiTY.
c. Below are the key factors to be considered for cloud hosting-
   i. The 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.
   ii. There should be physical and logical separation (of space, servers, storage, network infrastructure and networks) to protect data, applications and servers.
   iii. The system will be hosted in the site identified by the MSI and as agreed by the BSCDCL for DR.
   iv. There should be sufficient capacity (compute, network and storage capacity offered) available for near real time provisioning (as per the SLA requirement of the BSCDCL) during any unanticipated spikes in the user load.
   v. DR site will be located in India only.
   vi. Ensure redundancy at each level
   vii. MSI shall provide interoperability support with regards to available APIs, data portability etc. for the BSCDCL to utilize in case of Change of cloud service provider, migration back to in-house infrastructure, burst to a different cloud service provider for a short duration or availing backup or DR services from a different service provider.
   viii. The MSI is fully responsible for tech refreshes, patch management and other operations of infrastructure that is in the scope of the MSI.
   ix. BSCDCL retains ownership of all virtual machines, templates, clones, and scripts/applications created for the BSCDCL's application. BSCDCL retains the right to request (or should be able to retrieve) full copies of these virtual machines at any time

x. Provide a robust, fault tolerant infrastructure with enterprise grade SLAs with an assured uptime of 99.5%, SLA measured at the VM Level & SLA measured at the Storage Levels
xi. Cloud services should be accessible via internet and MPLS.
xii. Required Support to be provided to the BSCDCL in migration of the VMs, data, content and any other assets to the new environment created by the BSCDCL or any Agency (on behalf of the BSCDCL) on alternate cloud service provider's offerings to enable successful deployment and running of the BSCDCL's solution on the new infrastructure.
xiii. The 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
   a) Perform and store data and file backups consisting of an initial full back up with daily incremental backups for files;
   b) For the files, perform weekly backups;
   c) For the databases, perform a twice weekly full database backup, with a three times daily backup of database log files
   d) 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.
   e) Retain database backups for thirty (30) days
xiv. The MSI should offer dashboard to provide visibility into service via dashboard.
xv. 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 express approval of the BSCDCL.

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 Authority 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

The service provider shall provide DR Management Solution to Authority 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 out-of-the-box, 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
7	The proposed solution should be able to manage hosts by either deploying agents or without deploying any agent and should not require any change in the existing environment
8	The proposed solution must support all major platforms including Linux, Windows, Solaris, HP-UX, and AIX with native high availability options. It must support both physical and virtual platforms
9	The proposed solution should facilitate workflow based, single-click recovery mechanism for single or multiple applications
10	The proposed DRM solution should integrate seamlessly with the existing setup without the need to reconfigure or remove existing application setup including clusters
11	The proposed solution should cover all the functionalities mentioned in the specifications and all the required licenses should be provisioned

Periodic Disaster Recovery Plan Update

The service provider shall be responsible for –

- Devising and documenting the DR policy discussed and approved by Authority.
- Providing data storage mechanism with from the Go-Live date till the date of contract expiry for the purpose of compliance and audit.

1.3.15 Design, Supply, Installation and Commissioning of Network & Backbone Connectivity between cloud based common data center and various city ICCC

1. Network & Backbone Connectivity is one of the most 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 provisioned within the required timelines but also ensure that it is reliable, secure and supports the required SLA parameters of Latency, Jitter, Packet Loss and Performance.
2. It is envisaged that the each city ICCC system shall leverage Network Backbone infrastructure that is being created by BSCDCL under other smart city initiatives.
3. It is proposed that the MSI would procure bandwidth as a service for the entire duration of project period for the various locations (city) based on the approval from BSCDCL.
4. MSI should provide the network backbone infrastructure requirements for connectivity between individual command centres and cloud based common data centre.

   Illustrative Example for Bhopal Smart City is listed below:

a. Integration with Smart Parking
b. Integration with Public Bike Sharing
c. Integration with Smart Pole & Smart Lighting
d. Integration with Solid Waste Mgmt. Services (Tracking of Solid Waste Vehicles)
e. Integration with Intelligent Traffic Management System (Police)
f. Integration with Municipal Corporations Call Centre & Municipal Corporations Services
g. Integration with Bhopal Smart MAP (GIS)
h. Integration with Bhopal Plus
i. Integration with DIAL 100
j. Integration with DIAL 108 & Jannani Express
k. Integration with Transport Management System (BCLL)
l. Integration with CCTV Surveillance (Police Deptt.)
m. Integration with Dynamic Market Place (Mayor Express)
n. Integration with Emergency Response and Disaster Mgmt.
o. Integration with Water Management System
p. Integration with Met Department (Local Weather Forecast)
q. Integration with Area Based Development (ABD) Services
    i. Utilities
    ii. Lighting
    iii. Metering
    iv. Surveillance
r. Integration with Crowdsourcing Data
s. Integration with Fire Brigade Control System
t. Integration with Solar Roof Top System
u. Any other services implemented in near future during the project period*

*These other services will be additional work and will be taken up as "Change request" following the process defined in Schedule 3 of this RFP. Change request will be given by each individual city based on their requirement. Available details of individual command centers of ICT projects in other 6 cities is provided in Annexure.

5. MSI has to provide the network connectivity between all 7 city ICCC and cloud based common data centre. MSI has to coordinate with, BSCDCL and telecom service provider for setting up last mile connectivity.

6. MSI will be required to maintain the network backbone infrastructure for connectivity between the following individual city Command Centres / Components and cloud based common data centre.

7. MSI shall be providing the network backbone infrastructure requirement for connectivity between the following Command Centres / Components, city ICCC and cloud based common data centre.

   Illustrative Example of Bhopal Smart City given below:

S. No	From	To	Bandwidth Requirements
1	Smart Parking CCC	ICCC	
2	Public Bike Sharing CCC	ICCC	
3	Smart Pole CCC	ICCC	
4	Solid Waste Mgmt.	ICCC	
5	Intelligent Transport Management System (BCLL)	ICCC	

6	Municipal Corporations Call Centre	ICCC	To be recommended by MSI to BSCDCL
7	Water Mgmt. System	ICCC	
8	DIAL 100 CCC	ICCC	
9	DIAL 108 CCC & Jannani Express	ICCC	
10	Traffic Mgmt. System		
11	Safe City Cameras Feed	ICCC	
12	Emergency Response and Disaster Mgmt.	ICCC	
13	Met Department (Local Weather Forecast)	ICCC	
14	Mayor Express (Dynamic Market Place)	ICCC	
15	Fire Brigade Control System	ICCC	
16	Solar Roof Top	ICCC	

8. To ensure the easy accessibility of the application by users, MSI need to provide the redundant network connectivity as per the connectivity requirement mentioned below:

    a. MSI will provide connectivity between various city ICCC and systems to be integrated with ICCC, point to point connectivity will also be provided by MSI.

    b. MSI should provide the MPLS Connectivity to meet the application data replication requirement between DC and DR to meet the required Recovery Point Objective (RPO). This should include connectivity between Data Centre /each city ICCC site and Data Recovery site.

    c. MSI will also provide internet connectivity at each city CCC site.

    d. MSI to provide primary and second line (standby line) for internet connectivity at each ICCC site.

    e. MSI to provide internal connectivity within each city ICCC site between Command Centre, Situation Room, DC, meeting rooms and other working areas.

    f. MSI to monitor the network connectivity (being provided by service provider) as per the service levels and highlight the non-compliance.

9. The MSI should provide a detailed network architecture of the proposed overall network system. The network so envisaged should be able to provide real time data streams to the DC and each city ICCC. All the components of the technical network architecture should be of industry best standard and assist MSI in ensuring that all the connectivity SLAs are adhered to during the operational phase.

10. The MSI shall prepare the overall network connectivity plan for this project. The plan shall comprise of deployment of required network equipment in the field to be connected over network, any

clearances required from other government departments for setting up of the entire network. The network architecture proposed should be scalable and in adherence to network security standards. It is necessary that 100% of the proposed connectivity should be wired.

11. MSI shall ensure that bandwidth utilization should not cross 70% at any point of time. During the operations if bandwidth utilization reaches 70%, MSI will require to increase the Bandwidth without any additional cost to BSCDCL.

12. The MSI through EMS should also provide network related reports including the below:

    a. Link up/down (real-time as well as periodic)

    b. Link utilization in % (real-time as well as periodic) (Link utilization should not be more than 70% in each case, barring acceptable occasional surges)

    c. Router up/down (real-time as well as periodic)

    d. Top and Bottom N graphs showing the best and worst links in terms of availability (periodic)

    e. Reports on threshold violations. Provisions for setting thresholds and getting alerts on threshold violations should be there in the system. (real-time as well as periodic)

    f. Bandwidth utilization report for each link and utilization trends. The report should have provisions for displaying the minimum, maximum and average for each link. (real-time as well as periodic)

    g. The monitoring solution provides for application/port level traffic analysis with source and destination identifications

    h. Report on jitters, latency due to network parameters, closely linked to reachability shall be available. (real-time as well as periodic)

13. Router Statistics: CPU utilization and free memory reports of all the routers in the network should be available. Memory and CPU utilization reports will show maximum and minimum against a predefined threshold.

14. In case the Telecommunication guidelines of Government of India require the purchaser to place Purchase Order to the Service Provider for bandwidth, BSCDCL shall do so. However, MSI shall sign a contract with Telecom Service Provider(s) and ensure the performance. Each city based on pay per use shall make payments to the MSI.

15. The 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.

1.3.16 Preparation and implementation of the Information security policy, including policies on backup

The MSI shall prepare the Information Security Policy for the overall Project and the same would be reviewed and then finalized by BSCDCL & its authorized committees. The Security policy needs to be submitted by the MSI within 1st quarter of the successful Final Acceptance Tests.

The MSI should then obtain ISO 27001 certification for CCDCSC, all the ICCC and Data Recovery (DR) centre within 2 quarters of Final Acceptance Test. Payment from 3rd Quarter onwards shall be withheld till this certification is obtained by the MSI.

1.3.17 Training and Capacity Building

1. The purpose of this section is to define the scope of work for training and capacity building to be implemented at various levels namely:

    a. Employees of each SPV of 7 Smart cities
    b. Municipal Corporations' employees of 7 cities
    c. Stakeholder departments
    d. Command Center Operators of each city

2. The MSI's scope of work also includes preparing the necessary documentation and aids required for successful delivery of such trainings.

3. The details provided in this section are indicative and due to the complex nature of the project the number of training sessions may increase. Over and above the team considered for performing the training as detailed in subsequent sections,

4. Further the MSI has to provide cost for additional and optional training sessions in its commercial proposal in case more training's are required. MSI has to conduct such additional training sessions on City SPV's request.

5. MSI will develop a training and capacity building strategy that will also include a detailed plan of implementation. MSI should have comprehensive hands on system training strategy and schedule for users doing CCDCSC and ICCC Operations.

6. MSI will get the Training and capacity building strategy including training material finalized with City SPV before starting the training programs.

7. MSI will prepare all the requisite audio/visual training aids that are required for successful completion of the training for all stakeholders. These include the following for all the stakeholders:

    a. Training manuals for City SPV employees / stakeholder departments such as Municipal Corporation, Police, and Electricity Board etc.

    b. Computer based training modules

    c. Video (recorded sessions) for ICCC operations, back end modules, business intelligence, dynamic reporting

    d. Presentations

e. User manuals

f. Operational and maintenance manuals for the ICCC modules

g. Regular updates to the training aids prepared under this project

8. MSI must plan all the training and its material keeping defined and agreed SOPs of ICCC as prime focus.

9. MSI will maintain a copy of all the training material on the knowledge Portal and access will be provided to relevant stakeholders depending on their need and role. The access to training on the portal would be finalized with City SPV. MSI has to ensure the following points:

   a. For each training session, the MSI has to provide the relevant training material copies to all the attendees.

   b. The contents developed shall be the property of BSCDCL / City SPV with all rights.

10. There are estimated 350 users who need to be trained. MSI may accordingly plan the training budget.

11. MSI has to ensure that the training sessions held are effective and that the attendees would be able to carry on with their work efficiently. For this purpose, it is necessary that the effectiveness of training sessions is measured. The MSI will prepare a comprehensive feedback form that will capture necessary parameters on measuring effectiveness of the training sessions. This form will be discussed and finalized with City SPV.

12. After each training session, feedback will be sought from each of the attendees on either printed feedback forms or through a link available on the web portal. One member of the stakeholder group would be involved in the feedback process and he/she has to vet the feedback process. The feedback received would be reported to City SPV for each training session.

13. For each training session, the MSI will categorize the feedback on a scale of 1 to 10, where 10 will denote excellent and 1 will denote unsatisfactory.

14. The training session would be considered effective only after the cumulative score of the feedback (sum of all feedback divided by number of attendees) is more than 7.5.

1.3.18 Acceptance Testing

1. MSI shall demonstrate the following mentioned acceptance testing plan prior to acceptance of the solution as well as during project operations phase, in respect of scalability and performance etc. The MSI may propose further detailed Acceptance plan which the city SPV for each city will review. Once the city SPV provides its approval, the Acceptance plan can be finalized. In case required, parameters might be revised by city SPV 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.

2. 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	1. MSI to perform System testing 2. MSI to prepare test plan and test cases and maintain it. City SPV may request the MSI to share the test cases and results 3. Should be performed through manual as well as automated methods 4. Automation testing tools to be provided by MSI. City SPV doesn't intend to own these tools.
Integration Testing	MSI	1. MSI to perform Integration testing 2. MSI to prepare and share with BSCDCL/city SPV the Integration test plans and test cases 3. MSI to perform Integration testing as per the approved plan 4. Integration testing to be performed through manual as well as automated methods 5. Automation testing tools to be provided by MSI. City SPV doesn't intend to own these tools
Interoperability Testing	MSI	1. MSI will prepare interoperability traceability matrix with third party systems (existing legacy systems with ICCC) in consultation with city SPV and other relevant stakeholders (of external systems). Interoperability is an ability of one system to interact with another system. This matrix will cover all the use cases of system interaction and data movement.

		2. MSI to perform Interoperability testing 3. MSI to prepare and share with city SPV the Interoperable test plans and test cases with scenarios 4. MSI to perform Interoperable testing as per the approved plan 5. In Interoperability testing all the functions / components will be tested of a particular third party system which is integrated with ICCC.
Performance and load Testing	• MSI • BSCDCL / Third Party Auditor (to monitor the performance testing)	1. MSI to do performance and load testing. 2. Various performance parameters such as transaction response time, throughput, and page loading time should be taken into account. 3. Load and stress testing of the ICCC System to be performed on business transaction volume 4. Test cases and test results to be shared with city SPV. 5. Performance testing to be carried out in the exact same architecture that would be set up for production. 6. MSI need to use performance and load testing tool for testing. City SPV doesn't intend to own these tools. • BSCDCL if required, could involve third party auditors to monitor/validate the performance testing. Cost for such audits to be paid by city SPV.

Security Testing (including Penetration and Vulnerability testing)	• MSI • BSCDCL / Third Party Auditor (to monitor the security testing)	1. The solution should demonstrate the compliance with security requirements as mentioned in the RFP including but not limited to security controls in the application, at the network layer, network, data Centre(s), security monitoring system deployed by the MSI 2. The solution shall pass vulnerability and penetration testing. The solution should pass web application security testing for the portal, mobile app and other systems and security configuration review of the infrastructure if applicable. 3. MSI should carry out security and vulnerability testing on the developed solution. 4. Security testing to be carried out in the exact same environment/architecture that would be set up for production. 5. Security test report and test cases should be shared with city SPV 6. Testing tools if required, to be provided by MSI. City SPV doesn't intend to own these tools 7. During O&M phase, penetration testing to be conducted on yearly basis and vulnerability assessment to be conducted on half-yearly basis. BSCDCL 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 city SPV.

User Acceptance Testing of ICCC System	• BSCDCL appointed third party auditor	1. City SPV appointed third party auditor to perform User Acceptance Testing 2. MSI to prepare User Acceptance Testing test cases 3. UAT to be carried out in the exact same environment/architecture that would be set up for production 4. MSI should fix bugs and issues raised during UAT and get approval on the fixes from city SPV / third party auditor before production deployment 5. Changes in the application as an outcome of UAT shall not be considered as Change Request. MSI has to rectify the observations.

Note:

a. MSI 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. City SPV does not intend to own the tools.

b. The MSI shall work in a manner to satisfy all the testing requirements and adhere to the testing strategy outlined. The MSI must ensure deployment of necessary resources and tools during the testing phases. The 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 the MSI meets all the requirements specified in the RFP. The MSI shall take remedial action based on outcome of the tests.

c. The 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 the 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 city SPV directly. All tools/environment required for testing shall be provided by the MSI.

e. STQC/Other agencies appointed by city SPV 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. 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 the MSI.

1.3.19 Operations and Maintenance for a period of 5 years

MSI will operate and maintain all the components of the DC, DR and ICCC 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 city SPV. After Go-Live, if any system/sub-system/appliance that is deployed during the O&M phase must be added in the ICCC 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 ICCC project. MSI need to submit its detailed approach for PIP in its technical proposal. Every process and procedure implemented in ICCC 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 DC and ICCC be ported outside the geographical limits of the country.

Some broad details of O&M activities are mentioned below:

1.3.19.1 Helpdesk and Facilities Management Services

The MSI shall be required to establish the helpdesk and provide facilities management services to support the city SPV and stakeholder department officials in performing their day-to-day functions related to this system.

The MSI shall setup a central helpdesk dedicated (i.e. on premise) for the Project, which shall be supported by individual smart city command centres, implemented and proposed to be setup under Smart City Programme of various cities. 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, are provided in **Annexure 2**. 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 the 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 at each city. The deployed resource shall report to City SPV'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:

#	Type of Resource	Minimum Quantity	Minimum Deployment during Operation and Maintenance phase
1.	Project Manager	1	100%

2.	Cloud DC / DR Expert		100%
3.	Solution Architect	1	Onsite Support to Project team on need basis
4.	Project Manager-Software	1	100%
5.	Project Manager – Infrastructure	1	100%
6.	Database Architect/DBA	1	100%
7.	Security Expert	1	Onsite Support to Project team on need basis
8.	Command Centre Expert	1	100%
9.	GIS expert	1	Onsite Support to Project team on need basis
10.	Help Desk Manager	1	100%
11.	Help Desk Executives (24*7 – 1 in each shift)	3 for each city	100%
12.	Command Center Operators (24*7 – 5 in each shift)	15 for each city	100%

Note: Numbers provided for staff providing 24*7 support is excluding relievers.

1.3.19.2 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 city SPV 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 city SPV.

b. Annual Technology Support

The MSI shall be responsible for arranging for annual technology support for the OEM products to each city SPV for each city ICCC provided by respective OEMs during the entire project duration (1+5 = 6 Years).

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 city SPV'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 city SPV 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 city SPV approval. A detailed process in this regard will be finalized by MSI in consultation with city SPV/ BSCDCL.

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 city SPV team.

vi. MSI, at least on a monthly basis, will inform city SPV about any new updates/upgrades available for all software components of the solution along with a detailed action report. 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 city SPV team 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 city SPV personnel whenever there is any change in the functionality. Training plan has to be mutually decided with city SPV team.

h. Maintain System documentation

MSI shall maintain at least the following minimum documents with respect to the ICCC 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 enhancements including FRS and SRS, in accordance with the defined standards
iv. User manuals and training manuals are updated to reflect on-going changes/enhancements

v. 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 city SPV 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. City SPV 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.

1.3.19.3 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.

1.3.19.4 Technology Refresh

Technology refresh refers to the adoption of newer technology to meet changing needs or to mitigate the risk of obsolescence of existing technology. State (on behalf of all City SPVs) intends to use IT as strategic enabler instead of just a backend support system. Hence it is imperative to keep provision for Technology refresh.

Key Drivers for technology refresh:

- Aging /obsolete technology
- Out-of-support technology
- Skill set shortage
- Compliance
- Cost reduction
- Standardization
- Performance Improvement
- Vendor stability

- MSI has to mention latest IT Infrastructure (Hardware and Software) during bid submission
- MSI has to deliver latest (At the time of commissioning of ICCC) IT Infrastructure (Hardware and Software)
- The MSI has to make provision for technology refresh from time of bid submission to time of actual commissioning of Hardware and Software in ICCC
- Technology refresh will be applicable on all the components of Hardware and Software.

1.3.19.5 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 city SPV 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 city SPV 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 city SPV, 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 city SPV.

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 city SPV 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 ICCC System.

1.3.19.6 *Maintenance of ICT Infrastructure of CCDCSC and ICCC*

a. Management of ICT Infrastructure

MSI need to deploy requisite mix of L1, L2 and L3 resources (on 24X7 basis) for management of entire ICCC System including ICT infrastructure deployed at Command Center. 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 ICCC project. Any change in the team once deployed will require approval from city SPV. It is expected that the majority of resources have worked with MSI for at least preceding 1 year and have proven track record and reliability. Considering the criticality of the project, city SPV 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 city SPV and keep the same updated. A detailed process in this regard will be finalized between city SPV 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 BSCDCL on monthly basis. city SPV 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 city SPV. MSI shall comply with this.

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

i. ICCC/DR operations to be in compliance with industry leading ITSM frameworks like ITIL, ISO 20000 & ISO 27001

ii. Ensure compliance to relevant SLA's

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

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

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

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

vii. Preventive maintenance plan for every quarter

viii. Performance tuning of system as required

ix. Design and maintain Policies and Standard Operating Procedures

x. User access management

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

xii. 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 city SPV.

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 city SPV 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 city SPV on need basis.

vii. MSI shall implement a password change mechanism in accordance with the security policy formulated in discussion with BSCDCL 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 city ICCC.

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 city SPV.

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 city SPV at all times.

vii. city SPV 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 city SPV.

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 latest technologies such as virtualization and cloud computing so as to provision the existing and applicable infrastructure on a requirement based scenario.

e. Database Administration

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

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

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

iv. MSI will follow guidelines issued by city SPV 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 city SPV. The MSI is responsible for getting acquainted with the storage policies of city SPV before installation and configuration. It should be noted that the activities performed by the MSI may be reviewed by city SPV.

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 city SPV 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 city SPV.

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/DR etc.

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

h. Security Management

i. Regular hardening and patch management of components of the data center and ICCC system as agreed with city SPV/ BSCDCL

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

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 city SPV 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 city SPV

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 city SPV 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 city SPV/ BSCDCL

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 city SPV, any changes in the configuration manual need to be approved by city SPV. 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 city SPV 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. Disaster Recovery management services

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

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.

1.3.19.7 Compliance to SLA

a. 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 ICCC System shall be accordingly planned by MSI for ensuring the SLA requirements.

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

c. Reports for SLA measurement must be produced city SPV officials as per the project requirements.

1.3.20 Project Implementation Timelines

Common Cloud based DC and DR		
1	Project Inception Report	T+ 15 Days
2	Requirement Analysis and Report	T+21 Days
3	Solution Design Document including DC & DR and application design (State level and city level Integration Layers)	T+ 30 Days
4	Implementation of common city command center applications on state level common cloud based DC and DR	T+ 45 Days
5	Go - Live of common Cloud Based Data Center and DR	T+ 60 Days
City ICCC		
1	Implementation Roadmap	T1+15 Days
2	Complete System Design and submission of Design Report along with engineering drawings Including ICCC building design (using 3D Simulation along with physical report)	T1+90 Days
3	Installation of Hardware and S/W Infrastructure and acceptance testing + Submission of Installation Report+ Go Live of Cloud Based Data Center (Hosting Services)	T2+120 Days
4	Integration with various service components	T3+ 90 Days
5	Go Live and Go Live Report	T2 + 240 Days
6	Operation and Maintenance (Submission of Quarterly SLA Report)	G+5 Years

T = Date of signing contract Agreement

T1 = Date of Starting engagement with CITY SPV for CITY ICCC. This may be same in as T in some cases.

T2 = Date of handing over physical building of ICCC to MSI

T3= Readiness/Service Availability for integration with common platform at City level

G = Go Live Date

Go – Live Report: Go – Live report will consists of 2 parts:

- Testing reports of DC/DR Cloud bases Solution. This should be approved by BSCDCL.
- Go live report of ICCC will be different for each city ICCC. Each city SPV will define the Go-Live for them. Go-Live definition should be approved by city SPV authorities.

Note: T1, T2 and T3 will different for each city.

List of service to be integrated with city ICCC

Below is the table with list of services to be integrated with ICCC. In the below table requirement of advanced analytics and co-location is defined.

Co-location of services will be done based on the agreed plan with respective city SPV and Municipal Corporations, current service provider and any other relevant stakeholder of the identified service. MSI has to ensure physical capacity in ICCC for co-locating the identified services.

MSI is required to prepare the co-location plan along with Implementation plan, which will be part of the inception report as indicated in table above.

List of service to be integrated with timelines are provided in the Annexure.

1.3.21 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.

d. The MSI shall provide the following documentation at the stage of exit management:
   i) SOPs for common cloud based DC and DR
   ii) License details of current cloud based DC and DR
   iii) License details of common applications hosted on common cloud based DC and DR

iv) As-build drawing with marking of field devices, controllers and sensors
v) As-implemented configurations
vi) As-implemented architecture and topology diagrams
vii) Completed UAT and FAT results
viii) Standard operating procedures for administration of the installed devices.
ix) Each Site specific user manual and standard operating procedures for end users
x) Hardware-devices warranty details
xi) License details

e. For common infrastructure required items wil be handed over to BSCDCL and for City ICCC to CITY SPV.

1.3.21.1 *Cooperation and Provision of Information*

During the exit management period:

a. The MSI will allow the city SPV 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 BSCDCL to assess the existing services being delivered

b. Promptly on reasonable request by the city SPV, the 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 the MSI or sub-contractors appointed by the MSI). The city SPV shall be entitled to copy of all such information. Such information shall include details pertaining to the services rendered and other performance data. The MSI shall permit the BSCDCL or its nominated agencies to have reasonable access to its employees and facilities, to understand the methods of delivery of the services employed by the MSI and to assist appropriate knowledge transfer.

1.3.21.2 *Confidential Information, Security and Data*

a. The MSI will promptly on the commencement of the exit management period supply to the BSCDCL or its nominated agency the following:

i. information relating to the current services rendered and customer and performance data relating to the performance of sub-contractors in relation to the services;

ii. documentation relating to Intellectual Property Rights;

iii. documentation relating to sub-contractors;

iv. all current and updated data as is reasonably required for purposes of city SPV or its nominated agencies transitioning the services to its Replacement MSI in a readily available format nominated by the city SPV, its nominated agency;

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

Services to city SPV or its nominated agencies, or its Replacement System integrator (as the case may be).

b. Before the expiry of the exit management period, the MSI shall deliver to the city SPV 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 the MSI shall be permitted to retain one copy of such materials for archival purposes only.

1.3.21.3 *Employees*

a. Promptly on reasonable request at any time during the exit management period, the MSI shall, subject to applicable laws, restraints and regulations (including in particular those relating to privacy) provide to the BSCDCL or its nominated agency a list of all employees (with job titles) of the MSI dedicated to providing the services at the commencement of the exit management period.

b. Where any national, regional law or regulation relating to the mandatory or automatic transfer of the contracts of employment from the MSI to the BSCDCL or its nominated agency, or a Replacement MSI ("Transfer Regulation") applies to any or all of the employees of the System integrator, then the Parties shall comply with their respective obligations under such Transfer Regulations.

c. To the extent that any Transfer Regulation does not apply to any employee of the MSI, department, or its Replacement MSI may make an offer of employment or contract for services to such employee of the MSI and the MSI shall not enforce or impose any contractual provision that would prevent any such employee from being hired by the BSCDCL or any Replacement MSI.

1.3.21.4 *Transfer of Certain Agreements*

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

1.3.21.5 *General Obligations of the MSI*

a. The MSI shall provide all such information as may reasonably be necessary to effect as seamless a handover as practicable in the circumstances to the city SPV or its nominated agency or its Replacement MSI and which the 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 the MSI.

c. The MSI shall commit adequate resources to comply with its obligations under this Exit Management Schedule.

1.3.21.6 Exit Management Plan

a. The MSI shall provide the BSCDCL 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.

   i. 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;

   ii. plans for the communication with such of the MSI's sub-contractors, staff, suppliers, customers and any related third party as are necessary to avoid any material detrimental impact on the city SPV's operations as a result of undertaking the transfer;
   iii. (if applicable) proposed arrangements for the segregation of the MSI's networks from the networks employed by city SPV and identification of specific security tasks necessary at termination;

   iv. Plans for provision of contingent support to city SPV, and Replacement MSI for a reasonable period after transfer.

b. The 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 the MSI to and approved by the city SPV or its nominated agencies.

d. The terms of payment as stated in the Terms of Payment Schedule include the costs of the 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, the 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 city SPV or its nominated agencies within 90 days from the Effective Date of this Agreement.

2 Compliance to Standards & Certifications

1. For a large and complex set up such as the Integrated Control and Command Centre (ICCC) System, it is imperative that the highest standards applicable are adhered to. In this context, the MSI will ensure that the entire ICCC solution is developed in compliance with the applicable standards.

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

Sl. No.	Component/Application/System	Prescribed Standard
1.	Information Security	ISO 27001
2.	IT Infrastructure Management	ITIL specifications
3.	Service Management	ISO 20000 specifications
4.	Project Documentation	IEEE/ISO/CMMi (where applicable) specifications for documentation
6.	Cloud Service Provider	As per the MeitY guidelines and empaneled with MeitY

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

   a. The Information Technology Act, 2000" and amendments thereof and

   b. 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.

4. While writing the source code for application modules the 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:

   a. The name of the module

   b. The date when module was created

   c. A description of what the module does

   d. A list of the calling arguments, their types, and brief explanations of what they do

   e. A list of required files and/or database tables needed by the module

f. Error codes/Exceptions
g. Operating System (OS) specific assumptions

h. A list of locally defined variables, their types, and how they are used

i. Modification history indicating who made modifications, when the modifications were made, and what was done.

5. 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 -

a. Proper and consistent indentation

b. Inline comments

c. Structured programming

d. Meaningful variable names

e. Appropriate spacing

f. Declaration of variable names

g. Meaningful error messages

6. Quality Audits

a. BSCDCL or city SPV, at its discretion, may also engage independent auditors to audit any/some/all standards/processes. The MSI shall support all such audits as per calendar agreed in advance. The result of the audit shall be shared with the MSI who has to provide an effective action plan for mitigations of observations/non-compliances, if any.

3 Project Management and Governance

1.1 Project Management Office (PMO)

A Project Management office will be set up during the start of the project. The PMO will, at the minimum, include a designated full time Project Manager from MSI. It will also include key persons from other relevant stakeholders including members of city SPV and other officials/representatives by invitation. The operational aspects of the PMO need to be handled by the MSI including maintaining weekly statuses, minutes of the meetings, weekly/monthly/project plans, etc.

PMO will meet formally on a weekly basis covering, at a minimum, the following agenda items:

i. Project Progress
ii. Delays, if any – Reasons thereof and ways to make-up lost time
iii. Issues and concerns
iv. Performance and SLA compliance reports;
v. Unresolved and escalated issues;
vi. Project risks and their proposed mitigation plan
vii. Discussion on submitted deliverable
viii. Timelines and anticipated delay in deliverable if any
ix. Any other issues that either party wishes to add to the agenda.

During the development and implementation phase, there may be a need for more frequent meetings and the agenda would also include:

i. Module development status
ii. Testing results
iii. IT infrastructure procurement and deployment status
iv. Status of setting up/procuring of the Helpdesk, DC hosting
v. Any other issues that either party wishes to add to the agenda.

Bidder shall recommend PMO structure for the project implementation phase and operations and maintenance phase.

1.2 Steering Committee

The Steering Committee will consist of senior stakeholders from City SPVs, its nominated agencies and MSI. MSI will nominate its Project Head to be a part of the Project Steering Committee

The 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, BSCDCL may call for a Steering Committee meeting with prior notice to the MSI.

1.3 Project Monitoring and Reporting

The MSI shall circulate written progress reports at agreed intervals to BSCDCL, City SPV Authorities 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. BSCDCL and City SPV authorities reserves the right to ask the bidder for the project review reports other than the standard weekly review reports.

1.4 Risk and Issue management

The MSI shall develop a Risk Management Plan and shall identify, analyze and evaluate the project risks, and shall develop cost effective strategies and action plans to mitigate those risks.

The MSI shall carry out a Risk Assessment and document the Risk profile of City SPV based on the risk appetite and shall prepare and share the City SPV Enterprise Risk Register. The 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 City SPV.

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

1.5 Staffing requirements

BSCDCL has identified certain key positions that should be part of MSI's team during execution. MSI shall provide resource deployment schedule including these key positions and other team members as mentioned in RFP.

CVs of the key resources need to be submitted along with the proposal.

Please note that BSCDCL shall require that all project related discussion should happen in BSCDCL office. While the identified key personnel will operate out of BSCDCL's office, other key members of the development/Data Centre team may need to travel to BSCDCL office for critical Project/Steering Committee meetings at their own expenses.

1.6 Governance procedures

MSI shall document the agreed structures in a procedures manual.

1.7 Planning and Scheduling

The 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. The MSI has to get the plan approved from BSCDCL 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 BSCDCL 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 BSCDCL

2. Change Management & Control

2.1 Change Orders / Alterations / Variations

a. The 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 the 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 the 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.

2.2 Change Order

a. The Change Order will be initiated only in case (i) the Purchaser directs in writing the 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 the 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 as stated in Clause 2 a. 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 the MSI for approval, the 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.

Schedule 3 – General Conditions of Contract

A. General Conditions of Contract (GCC)

1. Definition of Terms

1.1. **"Authority":** Bhopal Smart City Development Corporation Limited (BSCDCL).

1.2. **"Acceptance of System":** The system including the hardware, software, solution or any deliverable shall be considered to have been accepted by designated authority, subsequent to its installation, rollout and deployment of trained manpower, when all the activities as defined in Scope of Work as laid down in the RFP have been successfully executed and completed by the MSI to the satisfaction of designated authority and the designated authority has indicated its acceptance by signing the Acceptance Certificate. Deliverable which are city specific like city ICCC and hardware/software/servers would be approved by city SPV authorities. Deliverables which are common to state will be reviewed and approved by BSCDCL.

1.3. "**Acceptance Certificate**" - means that document issued by the designated authority signifying Acceptance of a hardware, software, solution, or any other deliverable pursuant to the successful completion of the acceptance test of the System.

1.4. **"Applicable Law(s):** Any statute, law, ordinance, notification, rule, regulation, judgment, order, decree, bye-law, approval, directive, guideline, policy, requirement or other governmental restriction or any similar form of decision applicable to the relevant party and as may be in effect on the date of the execution of this Agreement and during the subsistence thereof, applicable to the Project.

1.5. **"Bidder"** shall mean organization/ consortium submitting the proposal in response to this RFP.

1.6. **"MSI**" or "**Lead Bidder**" means the bidder including the consortium who is selected by the designated authority at the end of this RFP process and shall be deemed to include the MSI's successors, representatives (approved by the designated authority), heirs, executors, administrators and permitted assigns, as the case may be, unless excluded by the terms of the contract. The word MSI when used in the pre-award period shall be synonymous with parties bidding against this RFP.

1.7. '**Confidential Information**' means all information including any information (whether in written, oral, electronic or other format) which relates to the technical, financial and business affairs, dealers, suppliers, products, developments, operations, processes, data, trade secrets, design rights, know-how, plans, budgets and personnel of designated authority which is disclosed to or otherwise learned by MSI in the course of or in connection with the Contract but does not include information which is available lawfully in the public domain

1.8. "**Contract**" or the "**Agreement**" means the Contract entered into by the parties and includes the RFP, the Proposal, the Letter of Award issued by the designated authority, the acceptance of Letter of Award from the MSI together with all Annexures, Schedules,

referenced documents and all amendments, corrigendum, addendums and changes thereto.

1.9. **"Contract Value"** means _____the amount quoted by the MSI in its commercial bid.

1.10. **"Commercial Off-The-Shelf (COTS)"** refers to software products that are ready-made and available for sale, lease, or license to the general public.

1.11. **"Document**" means any embodiment of any text or image however recorded and includes any data, text, images, sound, voice, codes, databases or any other electronic documents as per IT Act 2000.

1.12. **"Effective Date"** means the date on which this Contract is signed or LoI is issued by designated authority. If this Contract is executed in parts, then the date on which the last of such Contracts is executed shall be construed to be the Effective Date.

1.13. **"Goods"** means all of the equipment, sub-systems, hardware, software, products accessories, software and/or other material / items includes their user manuals, technical manuals, operating manuals, service mechanisms, policies and guidelines (such as security related, data migration related) and all its modifications which MSI is required to supply, install and maintain under the contract.

1.14. **"Integrated Command and Control Center"** means the integrated/centralized operation center to implement holistic and integrated solution for multiple (existing and future) IT initiative for the designated authority. The IT initiative may of any department for example whether it is safe city (CCTV surveillance) and DIAL 100 of police department, DIAL 108 of health department or network of Municipal Corporation. The end objective of establishing ICCC is to drive the actions by designated authority on behalf of all the departments for city operations.

1.15. **"Cloud Service Provider"** means an entity responsible to provide cloud based DC , DR and network services infrastructure business services and computing solutions.

1.16. **"Delivery of Goods"**- shall be deemed to have completed when the delivery of all the Goods under the proposed bill of material has reached the respective designated sites or locations wherein the delivery, installation, integration, management and maintenance services as specified under the Scope of Work are to be carried out for the purpose of this RFP / Contract and has been duly acknowledged by the designated authority's representative.

1.17. **"Intellectual Property Rights"** means any patent, copyright, trademark, trade name, service marks, brands, proprietary information whether arising before or after the execution of this Contract and the right to ownership and registration of these rights.

1.18. **"Go- Live"** means commissioning and acceptance of ICCC at the cities mentioned in the RFP, installation and commencement of all smart city components, including training as per Scope of Work mentioned in RFP. Bidder should have the approval from the designated authority for user acceptance testing.

1.19. **"BSCDCL"** means the Bhopal Smart City Development Corporation Ltd. BSCDCL is designated authority to coordinate supervise and project manage the implementation of ICCC at state level.

1.20. '**BSCDCL's Representative / Project Coordinator**' means the person or the persons appointed by the designated authority from time to time to act on its behalf for overall coordination, supervision and project management.

1.21. "**Scope of Work**" means all Goods and Services, and any other deliverables as required to be provided by the MSI under the RFP.

1.22. **"MSI's Team"** means MSI who along with all of its Consortium Members who have to provide Goods & Services to the designated authority under the scope of this Contract.

This definition shall also include any and/or all of the employees of SI, Consortium Members, authorized service providers/ partners and representatives or other personnel employed or engaged either directly or indirectly by MSI for the purposes of this Contract.

1.23. **"SPV"** means special Purpose Vehicles designed and established in each of the 7 cities to lead smart city project for respective city. They will be responsible for supervising monitoring and driving the implementation of command and control center and its integration with necessary services for respective cities.

1.24. '**Service Level(s)**' means the service level parameters and targets and other performance criteria which will apply to the Services and Deliverables as described in the RFP; 'SLA' or 'Service Level Agreement' means the service level agreement specified in the RFP;

1.25. '**Service Specifications'** means and includes detailed description, statements to technical data, performance characteristics, and standards (Indian as well as International) as applicable and as specified in the RFP and the Contract, as well as those specifications relating to industry standards and codes applicable to the performance of work, work performance quality and specifications affecting the work or any additional specifications required to be produced by the MSI to meet the design criteria.

1.26. '**System'** means integrated system/solution emerging out of all the Goods indicated in the Scope of Work and covered under the scope of each Purchase Order issued by the designated authority.

1.27. "**Purchase Order**' means the purchase order(s) issued from time to time by the designated authority to the MSI to provide Goods and Services as per the terms and conditions of this Contract.

1.28. "**Consortium**" means _____, _____and _____entering into the Contract with the designated authority and includes their respective successors and assignees.

1.29. "**Replacement Service Provider**" means the organization replacing MSI in case of contract termination for any reasons

1.30. "**Sub-Contractor**" shall mean the entity named in the contract for any part of the work or any person to whom any part of the contract has been sublet with the consent in writing of the designated authority and the heirs, legal representatives, successors and assignees of such person.

1.31. **"Services"** means the work to be performed by the agency pursuant to the RFP and to the contract to be signed by the parties in pursuance of any specific assignment awarded by the designated authority. In addition to this, the definition would also include other related / ancillary services that may be required to execute the Scope of Work under the RFP.

1.32. '**Timelines'** means the project milestones for performance of the Scope of Work and delivery of the Services as described in the RFP;

1 Interpretation

1.1 In this Contract unless a contrary intention is evident:

a. the clause headings are for convenient reference only and do not form part of this Contract;
b. unless otherwise specified a reference to a clause number is a reference to all of its sub-clauses;
c. the word "include" or "including" shall be deemed to be followed by "without limitation" or "but not limited to" whether or not they are followed by such phrases;
d. unless otherwise specified a reference to a clause, sub-clause or section is a reference to a clause, sub-clause or section of this Contract including any amendments or modifications to the same from time to time;
e. a word in the singular includes the plural and a word in the plural includes the singular;
f. a word importing a gender includes any other gender;

g. a reference to a person includes a partnership and a body corporate;
h. a reference to legislation includes legislation repealing, replacing or amending that legislation;
i. where a word or phrase is given a particular meaning it includes the appropriate grammatical forms of that word or phrase which have corresponding meanings.

2 Documents forming part of Agreement

2.1 The following documents shall be deemed to form and be read and constructed as part of the Contract viz.:

(a) The Contract;

(b) The RFP comprising of all volumes and any corrigenda thereto;

(c) The Proposal of the MSI as accepted by the designated authority along with any related documentation

(d) The designated authority's Letter of Award;

(e) The MSI's Acceptance of Letter of Award, if any;

(f) The tripartite agreement to be entered into between <***> for provision of bandwidth services, if any; and

(g) The Corporate Non-disclosure agreement and any other document to be submitted by the MSI and appended to this Agreement.

3 Ambiguities within Agreement

In case of ambiguities or discrepancies within the Contract, the following principles shall apply:

i. As between the provisions of RFP and any Corrigendum issued thereafter, the provisions of the Corrigendum shall, to that extent only, prevail over the corresponding earlier provision of the RFP;

ii. As between the provisions of the Contract and the RFP and the Proposal, the Contract shall prevail; and

iii. As between any value written in numerals and that in words, the value in words shall prevail.

4 Conditions Precedent

The payment obligations of under the Contract shall take effect upon fulfillment of the following conditions precedent by MSI.

a) Furnishing by MSI, an unconditional and irrevocable Performance Bank Guarantee (PBG) (Annexure 7 (a) of this RFP) within 15 (fifteen) days after issuance of the Letter of Award and acceptable to the designated authority which would remain valid until such time as stipulated by the designated authority.

b) Obtaining of all statutory and other approvals required for the performance of the Services under the Contract. This may include approvals/clearances, wherever applicable, that may be required for execution of this contract e.g. clearances from Government authorities for

importing equipment, exemption of Tax/Duties/Levies, work permits/clearances for Bidder/Bidder's team, etc.

c) Furnish notarized copies of any/all contract(s) duly executed by MSI and its OEMs existing at the time of signing of the contract in relation to the Project. Failure to do so within stipulated time of signing of contract would attract penalty as defined in clause 42 in this Section.

d) Furnishing of such other documents as the designated authority may specify/ demand.

e) All the members of the Consortium shall have executed a binding Consortium Contract / Agreement copy of which shall have been delivered to the designated authority without the commercials;

f) The designated authority reserves the right to waive any or all of the conditions specified in Clause 5 above in writing and no such waiver shall affect or impair any right, power or remedy that the designated authority may otherwise have.

5 Key Performance Measurements

a. Unless specified by the designated authority to the contrary, MSI shall deliver the Goods, perform the Services and carry out the Scope of Work in accordance with the terms of the Contract, Scope of Work and the Service Specifications as laid down under Section C (Service Level).

b. If the Goods and Service Specification includes more than one document, then unless the designated authority specifies to the contrary, the later in time shall prevail over a document of earlier date to the extent of any inconsistency.

c. The MSI shall commence the performance of its obligations under the Agreement from Effective Date and shall proceed to provide Goods and carry out the Services with diligence and expedition in accordance with any stipulation as to the time, manner, mode, and method of execution contained in this Agreement. The MSI shall be responsible for and shall ensure that all the Goods and Services are performed in accordance with the specifications and that the MSI's Team complies with such specifications and all other standards, terms and other stipulations/conditions set out hereunder.

d. The Goods supplied under this Agreement shall conform to the standards mentioned in the technical specifications given in the RFP, and, when no applicable standard is mentioned, to the authoritative standards, such standards shall be the latest issued by the concerned institution. Delivery of Goods shall be made by the MSI in accordance with the Agreement and the terms specified by the designated authority. In case if it is found that the Goods provided by MSI do not meet one/ more criteria, the MSI shall remain liable to provide a replacement for the same which meets all the required specifications and as per choice of MSI, at no additional cost to MSI.

6 Commencement and Progress

a. The MSI shall commence the performance of its obligations in a manner as specified in the Scope of Work, Service Level agreements and other provisions of the Contract from the Effective Date.

b. MSI shall proceed to carry out the activities / services with diligence and expedition in accordance with any stipulation as to the time, manner, mode, and method of execution contained in this Contract.

c. MSI shall be responsible for and shall ensure that all activities / services are performed in accordance with the Contract, Scope of Work and Service Specifications and that MSI's Team complies with such specifications and all other standards, terms and other stipulations/conditions set out hereunder.

d. MSI shall perform the activities / services and carry out its obligations under the Contract with due diligence, efficiency and economy, in accordance with generally accepted techniques and practices used in the industry and shall observe sound management, engineering and security practices. It shall employ appropriate advanced technology and engineering practices and safe effective equipment, machinery, material and methods.SI shall always act, in respect of any matter relating to this Contract, as faithful advisors to the designated authority and shall, at all times, support and safeguard the designated authority 's legitimate interests in any dealings with Third parties.

e. The Goods supplied under this Agreement shall confirm to the Standards mentioned in the technical specifications given in the RFP, and, when no applicable standard is mentioned, to the authoritative standards, such standard shall be the latest issued by the MSI to be proposed and approved by the designated authority in accordance with the Agreement and the terms specified by the designated authority in the Purchase Order.

7 Constitution of Consortium

a. For the purposes of fulfillment of its obligations as laid down under the Contract, where the designated authority deems fit and unless the contract requires otherwise, Prime Bidder shall be the sole point of interface for the designated authority and would be absolutely accountable for the performance of its own, the other member of Consortium and/or its Team's functions and obligations.

b. The Consortium member has agreed that MSI is the prime point of contact between the Consortium member and the designated authority and it shall be primarily responsible for the discharge and administration of all the obligations contained herein and, the designated authority, unless it deems necessary shall deal only with MSI.MSI along with all consortium members shall be jointly and solely responsible for the Project execution

c. Without prejudice to the obligation of the Consortium member to adhere to and comply with the terms of this Contract, each Consortium member, shall, in addition to a binding Consortium Agreement, has executed and submitted a Power of Attorney in favour of MSI authorizing him to act for and on behalf of such member of the Consortium and do all acts as may be necessary for fulfillment of contractual obligations.

d. The MSI and each of the Consortium Members shall be bound by all undertakings and representations made by their authorized representative and any covenants stipulated hereunder with respect to the Contract, for and their behalf.

e. MSI shall submit the Consortium Agreement to be entered into between MSI, _____ and _____ for the designated authority's review without commercials. MSI shall not, except with the prior approval of the designated authority, have any provision in the consortium agreement or make any amendments to the said consortium agreement which affects the rights and/or obligations of MSI, OEM-ES and/or _____ under this Agreement or any amendment which is contrary to the provisions of this Agreement.

f. A notice of at least 3 months in advance is required to be given by the MSI to the designated authority if during the Term of the Contract the MSI desires to terminate any contract/arrangement relating to the performance of Services hereunder with any member of the Consortium. Where, during the Term of the Contract, MSI terminates any contract/arrangement or agreement relating to the performance of Services with any consortium member (subject to approval of the designated authority), MSI shall be liable for any consequences resulting from such termination. MSI shall in such case ensure the smooth continuation of Services by providing a suitable replacement to the satisfaction of the designated authority at no additional charge and at the earliest opportunity.

8 MSI's Obligations

a. The obligations of the MSI described in this clause is in addition to, and not in derogation of, the obligations mentioned in the RFP and the two are to be read harmoniously. MSI's obligations shall include all the activities as specified by the designated authority in the Scope of Work and other sections of the RFP and Contract and changes thereof to enable designated authority to meet the objectives and operational requirements.

b. The MSI shall also be the sole point of contact for all matters relating to the RFP and Contract thereof.

c. It shall be MSI's responsibility to ensure the proper and successful implementation, performance and continued operation of the proposed solution in accordance with and in strict adherence to the terms of his the RFP and the Contract.

d. In addition to the aforementioned, MSI shall provide services to manage and maintain the said system and infrastructure as mentioned in the RFP.

e. The designated authority reserves the right to interview the personnel proposed by the MSI that shall be deployed as part of the project team. If found unsuitable, the designated authority may reject the deployment of the personnel. But ultimate responsibility of the project implementation shall lie with MSI.

f. The designated authority reserves the right to require changes in personnel which shall be communicated to MSI. MSI with the prior approval of the designated authority may make additions to the project team. MSI shall provide the designated authority with the resume of Key Personnel and provide such other information as the designated authority may reasonably require. The designated authority also reserves the right to interview the personnel and reject, if found unsuitable. In case of change in its team members, for any

reason whatsoever, MSI shall also ensure that the exiting members are replaced with at least equally qualified and professionally competent members.

g. MSI shall ensure that none of the Key Personnel and manpower exit from the project during first 6 months of the beginning of the project. In such cases of exit, replacement has to be approved by the designated authority.

h. MSI should submit profiles of only those resources who shall be deployed on the Project. Any change of resource should be approved by the designated authority and compensated with equivalent or better resource. The designated authority may interview the resources suggested by MSI before their deployment on board. It does not apply in case of change requested by the designated authority.

i. In case of change in its team members, MSI shall ensure a reasonable amount of time overlap in activities to ensure proper knowledge transfer and handover / takeover of documents and other relevant materials between the outgoing and the new member.

j. MSI shall ensure that MSI's Team is competent, professional and possesses the requisite qualifications and experience appropriate to the task they are required to perform under this Contract. MSI shall ensure that the services are performed through the efforts of MSI's Team, in accordance with the terms hereof and to the satisfaction of the designated authority. Nothing in the Contract relieves MSI from its liabilities or obligations under the Contract to provide the Services in accordance with the designated authority's directions and requirements and as stated in this Contract and the Bid to the extent accepted by the designated authority and MSI shall be liable for any non-performance, non-compliance, breach or other loss and damage resulting either directly or indirectly by or on account of its Team.

k. MSI shall be fully responsible for deployment / installation / development/ laying of network fibre and integration of all the software and hardware components and resolve any problems / issues that may arise due to integration of components.

l. MSI shall ensure that the OEMs supply equipment/ components including associated accessories and software required and shall support MSI in the installation, commissioning, integration and maintenance of these components during the entire period of contract. MSI shall ensure that the COTS OEMs supply the software applications and shall support MSI in the installation / deployment, integration, roll-out and maintenance of these applications during the entire period of contract. It must clearly be understood by MSI that warranty and AMC of the system, products and services incorporated as part of system would commence from the day of Go-Live of system as a complete Smart city solutions including all the solutions proposed. MSI would be required to explicitly display that he/ they have a back to back arrangement for provisioning of warranty/ AMC support till the end of contract period with the relevant OEMs. The annual maintenance support shall include patches and updates the software, hardware components and other devices.

m. All the software licenses that MSI proposes should be perpetual software licenses. The software licenses shall not be restricted based on location and the designated authority

should have the flexibility to use the software licenses for other requirements if required within the territory of Madhya Pradesh.

n. All the OEMs that Bidder proposes should have Dealer possession licenses.

o. The designated authority reserves the right to review the terms of the Warranty and Annual Maintenance agreements entered into between MSI and OEMs.

p. Shall ensure that none of the components and sub-components is declared end-of-sale or end-of-support by the respective OEM at the time of submission of bid. If the OEM declares any of the products/ solutions end-of-sale subsequently, the MSI shall ensure that the same is supported by the respective OEM for contract period.

q. If a product is de-supported by the OEM for any reason whatsoever, from the date of Acceptance of the System till the end of contract, MSI should replace the products/ solutions with an alternate that is acceptable to the designated authority at no additional cost to the designated authority and without causing any performance degradation.

r. Further, the MSI shall be obliged to ensure that all approvals, registrations, licenses, permits and rights which are, inter-alia, necessary for use of the Deliverables, goods, services, applications, services etc. provided by the MSI / Consortium / MSI's subcontractors under the Contract shall be acquired in the name of the designated authority and MSI shall have the non-exclusive, limited right to use such licenses till the Term on behalf of the designated authority solely for the purpose of execution of any of its obligations under the terms of the Contract. However, subsequent to the Term of this Contract, such approvals etc. shall endure to the exclusive benefit of the designated authority.

s. That the MSI shall procure all the necessary permissions and adequate approvals and licenses for **use** of various software and any copyrighted process/product for use of the copyright/process/products that the MSI has proposed to supply under the Contract free from all claims, titles, interests and liens thereon;

t. MSI shall ensure that the OEMs provide the support and assistance to MSI in case of any problems / issues arising due to integration of components supplied by him with any other **component**(s)/ product(s) under the purview of the overall solution. If the same is not resolved for any reason whatsoever, MSI shall replace the required component(s) with an equivalent or better substitute that is acceptable to designated authority without any additional cost to the designated authority and without impacting the performance of the solution in any manner whatsoever.

u. MSI shall ensure that the OEMs for hardware servers/equipment supply and/or install all type of updates, patches, fixes and/or bug fixes for the firmware or software from time to time at no additional cost to the designated authority.

v. MSI shall ensure that the OEMs for hardware servers/ equipment or Bidder's trained engineers conduct the preventive maintenance on a Quarterly basis and break-fix maintenance in accordance with the best practices followed in the industry.MSI shall ensure that the documentation and training services associated with the components shall be provided by the OEM partner or OEM's certified training partner without any additional cost to the designated authority.

w. The training has to be conducted using official OEM course curriculum mapped with the hardware / **Software** Product's to be implemented in the project.

x. MSI and their personnel/representative shall not alter / change / replace any hardware component proprietary to the designated authority and/or under warranty or AMC of third party without prior consent of the designated authority.

y. MSI shall provision the required critical spares/ components at the designated Datacenter Sites / office locations of the designated authority for meeting the uptime commitment of the components supplied by him.

z. MSI's representative(s) shall have all the powers requisite for the execution of Scope of Work and performance of services under the Contract. MSI's representative(s) shall liaise with the designated authority's Representative for the proper coordination and timely completion of the works and on any other matters pertaining to the works. MSI shall extend full co-operation to designated authority's Representative in the manner required by them for supervision/ inspection/ observation of the equipment/ goods/ material, procedures, performance, progress, reports and records pertaining to the works. He shall also have complete charge of MSI's personnel engaged in the performance of the works and to ensure compliance of rules, regulations and safety practice. He shall also cooperate with the other Service Providers/Vendors of the designated authority working at the designated authority's office locations & field locations and DC sites. Such Bidder's representative(s) shall be available to the designated authority Representatives at respective Datacenter during the execution of works.

aa. MSI shall be responsible on an ongoing basis for coordination with other vendors and agencies of the designated authority and its nominated agency in order to resolve issues and oversee implementation of the same. MSI shall also be responsible for resolving conflicts between vendors in case of borderline integration issues.

bb. MSI shall set up a project office in each Smart City for City ICCC. The technical manpower deployed on the project should work from the same office. However, some resources may be required to work from the office assigned by designated authority during the contract period.

9 Access to Sites

a. Sites would include Command control center itself and different command and control center of projects which are to be integrated with ICCC like DIAL 100 and Safe City. Access will be provided to different command and control center only after approval of their respective authorities and as per access policy.

b. The designated authority's Representative upon receipt of request from MSI intimating commencement of activities at various locations shall give to MSI access to as much of the Sites, on a non-permanent basis, as may be necessary to enable MSI to commence and proceed with the installation of the works in accordance with the program of work subject to compliance by the MSI with any safety and security guidelines which may be provided by the designated authority and notified to the MSI in writing. Any reasonable proposal of MSI for access to Site to proceed with the installation of work in accordance with the program of work shall be considered for approval and shall not be unreasonably withheld by the designated authority. Such requests shall be made to the designated authority's Representative in writing at least 7 days prior to start of the work.

c. At the site locations, the designated authority's Representative shall give to MSI access to as much as may be necessary to enable MSI to commence and proceed with the installation of the works in accordance with the program of work or for performance of Facilities Management Services.

d. Access to locations, office equipment and services shall be made available to the MSI on an "as is, where is" basis by the designated authority as the case may be or its nominated agencies. The MSI agrees to ensure that its employees, agents and contractors/Sub-Contractors shall not use the location, services and equipment referred to in the RFP for the following purposes:

   i. For the transmission of any material which is defamatory, offensive or abusive or of an obscene or menacing character; or
   ii. In a manner which constitutes violation of any law or a violation or infringement of the rights of any person, firm or company (including but not limited to rights of copyright or confidentiality); or
   iii. For their own purpose or for conducting their own business or for providing services to any third party.

10 Start of Installation

a. Bidder shall co-ordinate with the designated authority and stakeholders for the complete setup of sites before commencement of installation of other areas as mentioned in Volume II document. MSI shall also co-ordinate regarding Network / Bandwidth connectivity in order to prepare the installation plan and detailed design / architectural design documents.

b. As per TRAI guidelines, resale of bandwidth connectivity is not allowed. In such a case tripartite agreement should be formed between designated authority, selected Bidder and

Internet Service Provider(s).Such tripartite agreement entered for provision of bandwidth services will form an integral part of the Contract.

c. The plan and design documents thus developed shall be submitted by MSI for written approval by the designated authority.

d. After obtaining the approval from the designated authority, MSI shall commence the installation.

11 Reporting Progress

a. MSI shall monitor progress of all the activities related to the execution of the Contract and shall submit to the designated authority, progress reports with reference to all related work, milestones and their progress during the contract period.

b. Formats for all above mentioned reports and their dissemination mechanism shall be discussed and finalized with the designated CITY SPV authority along with project plan. The designated authority on mutual agreement between both parties may change the formats, periodicity and dissemination mechanism for such reports.

c. Periodic meetings shall be held between the representatives of the City SPV designated authority and MSI once in every 15 days during the implementation phase to discuss the progress of implementation. After the implementation phase is over, the meeting shall be held as an ongoing basis, as desired by designated City SPV authority, to discuss the performance of the contract.

d. MSI shall ensure that the respective solution teams involved in the execution of work are part of such meetings.

e. Several review committees involving representative of the designated authority and senior officials of MSI shall be formed for the purpose of this project. These committees shall meet at intervals, as decided by the designated City SPV authority later, to oversee the progress of the implementation.

f. All the Goods, Services and manpower to be provided / deployed by MSI under the Contract and the manner and speed of execution and maintenance of the work and services are to be conducted in a manner to the satisfaction of City SPV designated authority's Representative in accordance with the Contract.

g. Should the rate of progress of the works or any part of them at any time fall behind the stipulated time for completion or is found to be too slow to ensure completion of the works by the stipulated time, or is in deviation to Tender requirements/ standards, the City SPV / BSCDCL designated authority's Representative shall so notify MSI in writing.

h. MSI shall reply to the written notice giving details of the measures it proposes to take to expedite the progress so as to complete the works by the prescribed time or to ensure compliance to RFP requirements. MSI shall not be entitled to any additional payment for taking such steps. If at any time it should appear to the designated authority or designated authority's Representative that the actual progress of work does not conform to the approved plan MSI shall produce at the request of the designated authority's Representative a revised plan showing the modification to the approved plan necessary to

ensure completion of the works within the time for completion or steps initiated to ensure compliance to the stipulated requirements

i. The submission seeking approval by the designated authority or designated authority's Representative of such plan shall not relieve MSI of any of his duties or responsibilities under the Contract.

j. In case during execution of works, the progress falls behind schedule or does not meet the Tender requirements, MSI shall deploy extra manpower/ resources to make up the progress or to meet the RFP requirements. Plan for deployment of extra man power/ resources shall be submitted to the designated authority for its review and approval. All time and cost effect in this respect shall be borne, by MSI within the Contract Value.

k. The designated authority reserves the right to inspect and monitor/ assess the progress/ performance of the work / services at any time during the course of the Contract, after providing due notice to the MSI. The designated authority may demand and upon such demand being made, MSI shall provide documents, data, material or any other information pertaining to the Project which the designated authority may require, to enable it to assess the progress/ performance of the work / service under the Contract.

l. At any time during the course of the Contract, the designated authority shall also have the right to conduct, either itself or through another agency as it may deem fit, an audit to monitor the performance by MSI of its obligations/ functions in accordance with the standards committed to or required by the designated authority and MSI undertakes to cooperate with and provide to the designated authority / any other agency appointed by the designated authority, all documents and other details as may be required by them for this purpose. Such audit shall not include Bidder's books of accounts. Any deviations or contravention, identified as a result of such audit/assessment, would need to be rectified by the MSI failing which the designated authority may, without prejudice to any other rights that it may have issue a notice of default. Cost of acquisition of deliverables by the MSI and other Sub-Contractors is out of the purview of audit/inspections.

m. Without prejudice to the foregoing, the MSI shall allow access to the designated authority or its nominated agencies to all information which is in the possession or control of the MSI and which relates to the provision of the Services/Deliverables as set out in the Audit, Access and Reporting Schedule and which is reasonably required by the designated authority to comply with the terms of the Audit, Access and Reporting provision set out in this Contract.

n. Knowledge of Network Operations Center (NOC), Server Room, Command and Control Center, City Operation Center and areas of city kiosk centers

o. MSI shall be granted access to the command and control center of other IT project like DIAL 100, DIAL 108 and Safe City etc. for inspection by the designated authority before commencement of installation of integrated command and control center. The plan shall be drawn mutually at a later stage.

p. MSI shall be deemed to have knowledge of the cloud Data Centers, Server Room, Command and Control Center, its surroundings and information available in connection therewith and to have satisfied itself the form and nature thereof including, the data contained in the Bidding Documents, the physical and climatic conditions, the quantities and nature of the works and materials necessary for the completion of the works, the means of access, etc. and in general to have obtained itself all necessary information of all risks, contingencies and circumstances affecting his obligations and responsibilities therewith under the Contract and his ability to perform it. However, if during pre-installation survey / during delivery or installation, MSI detects physical conditions and/or obstructions affecting the work, MSI shall take all measures to overcome them.

12 Project Plan

a. Within 15 calendar days of Effective Date of the contract/ Issuance of LoI, MSI shall submit to the designated authority for its approval a detailed Project Plan with details of the project showing the sequence, procedure and method in which it proposes to carry out the works. The Plan so submitted by MSI shall conform to the requirements and timelines specified in the Contract. The designated authority and MSI shall discuss and agree upon the work procedures to be followed for effective execution of the works, which MSI intends to deploy and shall be clearly specified. The Project Plan shall include but not limited to project organization, communication structure, proposed staffing, roles and responsibilities, processes and tool sets to be used for quality assurance, security and confidentiality practices in accordance with industry best practices, project plan and delivery schedule in accordance with the Contract. Approval by the designated authority's Representative of the Project Plan shall not relieve MSI of any of his duties or responsibilities under the Contract.

b. If MSI's work plans necessitate a disruption/ shutdown in designated authority's operation, the plan shall be mutually discussed and developed so as to keep such disruption/shutdown to the barest unavoidable minimum. Any time and cost arising due to failure of MSI to develop/adhere such a work plan shall be to his account.

13 Compliance with Applicable Law

a. MSI's Team shall comply with the provision of all laws including labour laws, rules, regulations and notifications issued there under from time to time. All safety and labour laws enforced by statutory agencies and by the designated authority shall be applicable in the performance of the Contract and Bidder's Team shall abide by these laws. The MSI shall take all measures necessary or proper to protect the personnel, work and facilities and shall observe all reasonable safety rules and instructions.

b. Access to the Data centers of other IT systems (DIAL 100, CM Helpline, safe city etc.) and its Server Room shall be strictly restricted. No access to any person except the essential members of MSI's Team who are authorized by the designated authority and are genuinely

required for execution of work or for carrying out management/ maintenance shall be allowed entry. Even if allowed, access shall be restricted to the pertaining equipment of the designated authority only. MSI shall maintain a log of all activities carried out by each of its team personnel.

c. All such access should be logged in a loss free manner for permanent record with unique biometric identification of the staff to avoid misrepresentations or mistakes

d. Each Party to the Contract accepts that its individual conduct shall (to the extent applicable to its business like the MSI as an Information Technology service provider) at all times comply with all laws, rules and regulations of government and other bodies having jurisdiction over the area in which the Services are undertaken provided that changes in such laws, rules and regulations which result in a change to the Services shall be dealt with in accordance with the Change Management and Control set out in the RFP.

e. MSI shall take all measures necessary or proper to protect the personnel, work and facilities and shall observe all reasonable safety rules and instructions. MSI's Team shall adhere to all security requirement/ regulations of the designated authority during the execution of the work. Designated authority's employee also shall comply with safety procedures/ policy.

f. MSI shall report as soon as possible any evidence, which may indicate or is likely to lead to an abnormal or dangerous situation and shall take all necessary emergency control steps to avoid such abnormal situations.

14 Statutory Requirements

a) During the tenure of the Contract the MSI shall comply with all Applicable Laws and shall obtain and maintain all statutory and other approvals required for the performance of the Services under the Contract and nothing shall be done by MSI or his team including Consortium in contravention of any law, act and/ or rules/regulations, there under or any amendment thereof governing inter-alia customs, stowaways, foreign exchange etc. and shall keep designated authority indemnified in this regard.

15 Representations and Warranties

a) Representations and warranties of the MSI

The MSI hereby represents and warrants as of the date hereof, which representations and warranties shall remain in force during the Term and extension thereto, the following:

(i) it is duly organized and validly existing under the laws of India, and has full power and authority to execute and perform its obligations under this Contract and other agreement and to carry out the transactions contemplated hereby;

(ii) it is a competent provider of a variety of Information Technology and business process management services. It has taken all necessary corporate and other actions under laws applicable to its business to authorize the execution and

delivery of this Contract and to validly exercise its rights and perform its obligations under this Contract;

(iii) That all conditions precedent under the Contract have been satisfied;

(iv) That the selected MSI along with its consortium members have the power and the authority that would be required to enter into this Contract and the requisite experience, the technical know-how and the financial wherewithal required to successfully execute the terms of this Contract and to provide services sought by the designated authority under this Contract;

(v) That the MSI and its team has the professional skills, personnel, infrastructure and resources/ authorizations that are necessary for providing all such services as are necessary to fulfil the scope of work stipulated in the tender and this Contract;

(vi) That the MSI shall ensure that all assets/ components including but not limited to equipment, software, licenses, processes, documents, etc. installed, developed, procured, deployed and created during the term of this Contract are duly maintained and suitably updated, upgraded, replaced with regard to contemporary requirements;

(vii) The MSI/ MSI's team shall use such assets of the designated authority, as the designated authority may permit for the sole purpose of execution of its obligations under the terms of the Bid, Tender or this Contract. The MSI shall however, have no claim to any right, title, lien or other interest in such property, and any possession of property for any duration whatsoever shall not create any right in equity or otherwise, merely by fact of such use or possession during or after the term thereof;

(viii) it has the financial standing and capacity to undertake the Project and obligations in accordance with the terms of this Contract;

(ix) in providing the Services, it shall spare no effort to prevent any disruption to designated authority 's normal business operations;

(x) this Contract has been duly executed by it and constitutes a legal, valid and binding obligation, enforceable against it in accordance with the terms hereof, and its obligations under this Contract shall be legally valid, binding and enforceable against it in accordance with the terms hereof;

(xi) the information furnished in the Proposal is to the best of its knowledge and belief, true and accurate in all respects as at the date of this Contract;

(xii) the execution, delivery and performance of this Contract shall not conflict with, result in the breach of, constitute a default by any of the terms of its Memorandum and Articles of Association or any Applicable Laws or any covenant, contract, Contract, arrangement, understanding, decree or order to which it is a party or by which it or any of its properties or assets is bound or affected;

(xiii) there are no material actions, suits, proceedings, or investigations pending or, to its knowledge, threatened against it at law or in equity before any court or before any other judicial, quasi-judicial or other authority, the outcome of which may result in the breach of this Contract or which individually or in the aggregate may

result in any material impairment of its ability to perform any of its material obligations under this Contract;

(xiv) it has no knowledge of any violation or default with respect to any order, writ, injunction or decree of any court or any legally binding order of any Government Instrumentality which may result in any adverse effect on its ability to perform its obligations under this Contract and no fact or circumstance exists which may give rise to such proceedings that would adversely affect the performance of its obligations under this Contract;

(xv) it has complied with Applicable Laws in all material respects and has not been subject to any fines, penalties, injunctive relief or any other civil or criminal liabilities which in the aggregate have or may have an Adverse Effect on its ability to perform its obligations under this Contract;

(xvi) no representation or warranty by it contained herein or in any other document furnished by it to the designated authority or its nominated agencies in relation to the any consents contains or shall contain any untrue or misleading statement of material fact or omits or shall omit to state a material fact necessary to make such representation or warranty not misleading;

(xvii) no sums, in cash or kind, have been paid or shall be paid, by it or on its behalf, to any person by way of fees, commission or otherwise for entering into this Contract or for influencing or attempting to influence any officer or employee of the designated authority or its nominated agencies in connection therewith;

(xviii) That the MSI shall procure all the necessary permissions and adequate approvals and licenses for use of various software and any copyrighted process/product for use of the copyright/process/products that the MSI has proposed to supply under this Contract free from all claims, titles, interests and liens thereon;

(xix) That the sub-contractor proposed and/or deployed by the MSI meets the technical and financial qualifications prescribed in the RFP; and

(xx) That the representations made by the MSI in its Proposal and in this Contract are and shall continue to remain true and fulfil all the requirements as are necessary for executing the obligations and responsibilities as laid down in the Contract and the RFP and unless the designated authority specifies to the contrary, the MSI shall be bound by all the terms of the Contract;

(xxi) That the MSI certifies that all registrations, recordings, filings and notarizations of the Contract and all payments of any tax or duty, including but not limited to stamp duty, registration charges or similar amounts which are required to be effected or made by the MSI which is necessary to ensure the legality, validity, enforceability or admissibility in evidence of the Contract have been made;

(xxii) That the MSI confirms that there has not and shall not occur any execution, amendment or modification of this contract without the prior written consent of the designated authority;

(xxiii) That the MSI owns or has good, legal or beneficial title, or other interest in, to the property, assets and revenues of the MSI on which it grants or purports to grant or create any interest pursuant to-the Contract, in each case free and clear-of any-

encumbrance and further confirms that such Interests created or expressed to be created are valid and enforceable;

(xxiv) That the MSI-owns, has license to use or otherwise has the right to use, free of any pending or threatened liens or other security or other interests all Intellectual Property Rights, which are required or desirable for the project. In case of any infringement, designated authority is not responsible. Action will be taken as per the clauses defined in this RFP.

(xxv) That the MSI shall provide adequate and appropriate support and participation, on a continuing basis, in tuning/ upgrading all supplied hardware and software to meet the requirements of the applications;

b) **Representations and warranties of the** designated authority

The designated authority represents and warrants to the MSI that:

i. it has full power and authority to execute, deliver and perform its obligations under this Contract and to carry out the transactions contemplated herein and that it has taken all actions necessary to execute this Contract, exercise its rights and perform its obligations, under this Contract and carry out the transactions contemplated hereby;

ii. it has taken all necessary actions under Applicable Laws to authorize the execution, delivery and performance of this Contract and to validly exercise its rights and perform its obligations under this Contract;

iii. it has the financial standing and capacity to perform its obligations under the Contract;

iv. this Contract has been duly executed by it and constitutes a legal, valid and binding obligation enforceable against it in accordance with the terms hereof and its obligations under this Contract shall be legally valid, binding and enforceable against it in accordance with the terms thereof;

v. the execution, delivery and performance of this Contract shall not conflict with, result in the breach of, constitute a default under any of the Applicable Laws or any covenant, contract, Contract, arrangement, understanding, decree or order to which it is a party or by which it or any of its properties or assets is bound or affected;

vi. it has complied with Applicable Laws in all material respects.

16 Obligations of the designated authority

a. The obligations of the designated authority described in this clause is in addition to, and not in derogation of, the obligations mentioned in the RFP are to be read harmoniously. Without prejudice to any other undertakings or obligations of the designated authority under the Contract or the RFP, the designated authority shall perform the following:

b. The designated authority or his/her nominated representative shall act as the nodal point for implementation of the contract and for issuing necessary instructions, approvals, commissioning, Acceptance Certificate(s), payments etc. to MSI.

c. The designated authority shall ensure that timely approval is provided to MSI as and when required, which may include approval of project plans, implementation methodology,

design documents, specifications, or any other document necessary in fulfillment of the contract.

d. The designated authority's Representative shall interface with MSI, to provide the required information, clarifications, and to resolve any issues as may arise during the execution of the Contract. Designated authority shall provide adequate cooperation in providing details, coordinating and obtaining of approvals from various governmental agencies, in cases, where the intervention of the designated authority is proper and necessary.

e. The designated authority may provide on Bidder's request, particulars/ information/ or documentation that may be required by MSI for proper planning and execution of work and for providing Goods and Services covered under the contract and for which MSI may have to coordinate with respective vendors.

f. The designated authority shall provide to MSI only sitting space and basic infrastructure not including, stationery and other consumables at the designated authority's office locations.

g. The designated authority reserves the right to procure the hardware including devices on quarterly basis in first year based on actual deployment and AMC shall be applicable whenever the devices are procured and deployed till end of the contract.

h. Site Not Ready: The designated authority hereby agrees to make the project sites ready as per the agreed specifications, within the agreed timelines. The designated authority agrees that MSI shall not be in any manner liable for any delay arising out of designated authority's failure to make the site ready within the stipulated period.

17 Payments

1. Payments to MSI will be done on monthly based on the activities completed in the particular month.
2. No Pro-rata payment will be done, payment for only activities completed will be done in the particular month at the end of each month.
3. The following steps will be followed:
    - 3.1 MSI will create separate monthly invoice for City ICCC work by 5th of the following month
    - 3.2 MSI will submit invoice to respective city along with monthly progress report and proof of the work delivered
    - 3.3 City SPV or its authorized personnel will approve / reject the invoice based on the performance of the MSI for the previous month
    - 3.4 After approvals from all the cities, MSI will submit all the approved invoices to BSCDCL.
    - 3.5 BSCDCL or its authorized personal will review the submitted invoices and reports
    - 3.6 After all approvals, claims will be processed and payment will be made to MSI

18 Ownership and Intellectual Property Rights

a. The designated authority shall have a right in perpetuity to use all newly created Intellectual Property Rights which have been developed solely during execution of the Contract, including but not limited to all processes, products, specifications, reports and other documents which have been newly created and developed by MSI solely during the performance of Services and for the purposes of inter-alia use or sub-license of such Services under the Contract. MSI undertakes to disclose all such Intellectual Property Rights arising in performance of the Services to the designated authority, execute all such agreements/documents and obtain all permits and approvals that may be necessary in regard to the Intellectual Property Rights of the designated authority.

b. If designated authority desires, MSI shall be obliged to ensure that all approvals, registrations, licenses, permits and rights etc. which are inter-alia necessary for use of the Goods Deliverables, Services supplied / installed by MSI/Consortium/MSI's Sub-Contractors under the Contract shall be acquired in the name of the designated authority and MSI shall have the non-exclusive, limited right to use such licenses till the Term on behalf of the designated authority solely for the purpose of execution of any of its obligations under the terms of the Contract. However, subsequent to the Term of this Contract, such approvals, registrations, licenses, permits and rights etc. shall endure to the exclusive benefit of the designated authority.

c. Pre-existing work: All intellectual property rights existing prior to the Effective Date of the Contract shall belong to the Party that owned such rights immediately prior to the Effective Date. Subject to the foregoing, the designated authority will also have rights to use and copy all intellectual property rights, process, specifications, reports and other document, drawings, manuals provided or used by the MSI as part of the Scope of Works under the Contract for the purpose of the Contract on non-exclusive, non-transferable, perpetual, royalty-free license to use basis.

d. Third Party Products: If license agreements are necessary or appropriate between the MSI and third parties for purposes of enabling / enforcing/implementing the provisions hereinabove, the MSI shall enter into such agreements at its own sole cost, expense and risk and all such licenses etc. shall be bought in name of the designated authority unless otherwise directed in writing by the designated authority.

e. MSI shall not copy, reproduce, translate, adapt, vary, modify, disassemble, decompile or reverse engineer or otherwise deal with or cause to reduce the value of the Materials except as expressly authorized by the designated authority in writing

19 Taxes

a. MSI shall bear all personnel taxes levied or imposed on its personnel, or any other member of MSI's Team, etc. on account of payment received under the Contract. MSI shall bear all corporate taxes, levied or imposed on MSI on account of payments received by it from the designated authority for the work done under the Contract. The MSI shall bear all taxes and duties etc. levied or imposed on the MSI under the Contract including but not limited to Customs duty, Excise duty and all Income Tax levied under Indian Income Tax Act – 1961 or any amendment thereof up to the date for submission of final price bid, i.e., on account of payments received by him from the designated authority for work done under the Contract. The MSI shall also be responsible for having his Sub-Contractors under its Sub-Contract(s) to pay all applicable taxes on account of payment received by the Sub-Contractors from the MSI for works done under the Sub-contracts in relation to this Agreement and the designated authority will in no case bear any responsibility for such payment of taxes.

b. MSI agrees that he shall comply with the Indian Income Tax Act in force from time to time and pay Indian Income Tax, as may be imposed/ levied on them by the Indian Income Tax Authorities, for the payments received by them for the works under the Contract

c. MSIs shall fully familiarize themselves about the applicable domestic taxes (such as value added or sales tax, service tax, income taxes, duties, fees, levies, etc.) on amounts payable by the designated authority under the Agreement.

d. Should MSI fail to submit returns/pay taxes in times as stipulated under applicable Indian/State Tax Laws and consequently any interest or penalty is imposed by the concerned authority, MSI shall pay the same. MSI shall indemnify the designated authority against any and all liabilities or claims arising out of this Contract for such taxes including interest and penalty by any such Tax Authority may assess or levy against the designated authority.

e. Payment agreed to be made by the designated authority to the MSI in accordance with the Proposal.

f. Supplies of materials from abroad are exempted from levy of Sales Tax/VAT on works/works Contract tax (Central or state). However, the Sales Tax/VAT on works (central or state) if levied on supplies made from indigenous vendors for the works shall be borne by MSI within the Contract Price. Service Tax/ Terminal Sales Tax/ Works Contract Tax, etc., if any applicable, shall be payable extra, at actuals by the designated authority in accordance with the conditions of the Contract and upon submission of proof of payment of such taxes.

g. The designated authority shall if so required by Applicable Laws in force, at the time of payment, deduct income tax payable by MSI at the rates in force, from the amount due to MSI and pay to the concerned tax authority directly.

h. Should the MSI and/or other Consortium members fail to submit returns/pay taxes in times as stipulated under the Indian Income Tax Act and consequently any interest or penalty is imposed by the Indian Income Tax authority, the MSI and/or other Consortium members, as the case may be shall pay the same. MSI and/or other Consortium members shall jointly and severally indemnify the designated authority against any and all liabilities or claims arising out of this Agreement for such taxes including interest and penalty any such Tax Authority may assess or levy against the designated authority /MSI and/or other Consortium members.

20 Indemnity

21.1 General Indemnity

Subject to Clause 21.2 below, the MSI (the "Indemnifying Party") undertakes to indemnify the designated authority and its nominated agencies (the "Indemnified Party") from and against all losses, claims, damages, compensation etc. on account of bodily injury, death or damage to tangible personal property arising in favour of any person, corporation or other entity (including the Indemnified Party) attributable to the Indemnifying Party's negligence, willful default, lack of due care or breach of terms of this Agreement.

21.2 IPR Indemnity

If the Indemnified Party promptly notifies the Indemnifying Party in writing of a third party claim against the Indemnified Party that any Goods / Deliverables/ Services provided by the Indemnifying Party infringes a copyright, trade secret, patent or other intellectual property rights of any third party, the Indemnifying Party will defend such claim at its expense and will pay any costs or damages that may be finally awarded against the Indemnified Party. The Indemnifying Party will not indemnify the Indemnified Party, however, if the claim of infringement is caused by (a) The Indemnified Party's misuse or modification of the Deliverables; (b) The Indemnified Party's failure to use corrections or enhancements made available by the Indemnifying Party; (c) The Indemnified Party's use of the Deliverables in combination with any product or information not owned or developed or supplied by the Indemnifying Party. If any of the Deliverables is or likely to be held as infringing, the Indemnifying Party shall at its expense and option either (i) procure the right for the Indemnified Party to continue using it, (ii) replace it with a non-infringing equivalent, (iii) modify it to make it non-infringing.

21.3 Conditions for Indemnity

Without prejudice to the rights of the designated authority in respect of indemnification for any claim:

i. The designated authority shall notify the MSI upon receipt of any notice of claim setting out in reasonable particulars, the details of such notice of claim;

ii. Immediately upon receipt of notification of any claim from the designated authority, the

MSI within a period of 5 days from date of receipt of such notice from the designated authority, notify the designated authority whether the MSI wish to assume the defense in relation to such claim (including settlement or resolution thereof). Thereafter, the MSI shall be entitled in consultation with the designated authority, and only to the extent such action does not in any manner compromise, prejudice or adversely affect the interests of the designated authority, to take such action as mutually agreed upon by MSI and the designated authority to avoid, dispute, deny, resist, appeal, compromise or consent such claim, within a period of 30 days from the date of receipt of such claim notification;

iii. Notwithstanding anything contained herein, the MSI and the designated authority agree and covenant that a notice by the designated authority to the MSI in relation to the claim as aforesaid shall amount to express acceptance and consent by the MSI to indemnify the designated authority for all losses in relation to such claim. Upon notice by the MSI, the designated authority shall reasonably co-operate with the MSI at the sole costs of the MSI, only to the extent the same does not in any manner compromise, prejudice or adversely affect the rights of the designated authority. The designated authority shall have the right, at its option, to participate in the defense of such claim;

If the MSI fails to take any action as per the above clause within the time period as specified therein, the designated authority shall have the right, in its absolute discretion, to take such action as it may deem necessary to avoid, dispute, deny, resist, appeal, compromise or contest or settle any claim (including without limitation, making claims or counterclaims against third parties). If the MSI does not assume control of the defense of such claims (as mentioned above), the entire defense, negotiation or settlement of such claim by the designated authority shall be deemed to have been consented to by, and shall be binding upon, MSI as fully as though the MSI alone had assumed the defence thereof and a judgement had been entered into by the MSI, for such claim in respect of the settlement or judgement.

22 Warranty

22.1 The warranties and remedies provided in this Clause are in addition to, and not in derogation of, the warranties provided in the RFP and the two are to be read harmoniously.

22.2 A comprehensive warranty applicable on goods/solutions supplied under the Contract by the respective OEMs and the warranties shall be passed on to the designated authority. The MSI shall be responsible for making any and all claims under the warranty on behalf of the designated authority. Generally the warranty for goods and solutions shall be for a period of two (2) years from the date of installation and commissioning of the respective hardware and solution. If the warranty period provided by the OEM is for more than two (2), then the same warranty period shall be passed on to the designated authority. The AMC / ATS shall commence from the date of expiry of the warranty period of the respective goods and solutions.

22.3 Technical Support for Software applications shall be provided by the respective OEMs for the period of contract. The Technical Support should include all upgrades, updates and patches to the respective Software applications.

22.4 The MSI warrants that the Goods supplied under the Contract are new, non-refurbished, unused and recently manufactured; shall not be nearing End of sale / End of support; and shall be supported by the MSI and respective OEM along with service and spares support to ensure its efficient and effective operation for the entire duration of the contract.

22.5 The MSI warrants that the Goods supplied under the Contract shall be of the highest grade and quality and consisted with the established and generally accepted standards for materials of this type. The goods shall be in full conformity with the specifications and shall operate properly and safely. All recent design improvements in goods, unless provided otherwise in the Contract, shall also be made available.

22.6 The MSI further warrants that the Goods supplied under the Contract shall be free from all encumbrances and defects/faults arising from design, material, manufacture or workmanship (except insofar as the design or material is required by the designated authority 's Specifications) or from any act or omission of the MSI, that may develop under normal use of the supplied Goods in the conditions prevailing at the respective Datacenter / Server Room Sites.

22.7 Warranty for Services – The MSI warrants that all services under the Contract will be performed with promptness and diligence and will be executed in a workmanlike and professional manner, in accordance with the practices and high professional standards used in well-managed operations performing services similar to the services under the Contract. The MSI represents that it shall use adequate numbers of qualified individuals with suitable training, education, experience and skill to perform the Services hereunder.

22.8 The designated authority shall promptly notify the MSI in writing of any claims arising under this warranty.

22.9 Upon receipt of such notice, the MSI shall, with all reasonable speed, repair or replace the defective goods or replace such goods with similar goods free from defect at MSI's own cost and risk. Any goods repaired or replaced by the MSI shall be delivered at the designated authority's premises without costs to the designated authority. Notwithstanding the foregoing, these are not the sole and exclusive remedies available to the designated authority in case of breach of any warranty and are also not the sole and exclusive obligations on the MSI in case of breach of any warranty.

22.10 If the MSI, having been notified, fails to remedy the defect(s) within a reasonable period, the designated authority may proceed to take such remedial action as may be necessary, at the MSI's risk and expense and without prejudice to any other rights which the designated authority may have against the MSI under the Contract.

22.11 Any OEM specific warranty terms that do not conform to conditions under this Contract shall not be acceptable.

22.12 The representations, warranties and covenants provided by the MSI under the Contract will not be affected by designated authority's modification of any portion of the software so long as the MSI can discharge its obligations despite such modifications, or following their removal by the designated authority

22.13 Notwithstanding anything contained in the Contract, unless the designated authority has otherwise agreed in writing, the designated authority reserves the right to reject Goods which do not conform to the specifications provided in the RFP.

23 Term and Extension of the Contract

23.1 The Contract period shall come into effect on .....i.e. from the date of signing of contract or Issuance of LoI, whichever is earlier((hereinafter the "Effective Date"), and shall remain valid for 60 Months from the date of Go Live of the system ("Term")

23.2 If the delay occurs due to any Force Majeure event, a reasonable extension of time shall be granted by the designated authority.

23.3 The designated authority shall reserve the sole right to grant any extension to the Term abovementioned and shall notify in writing to MSI, at least 3 (three) months before the expiration of the Term hereof, whether it shall grant MSI an extension of the Term. The decision to grant or refuse the extension shall be at the designated authority's discretion and such extension of the contract, if any, shall be as per terms agreed mutually between the designated authority and MSI.

23.4 Where the designated authority is of the view that no further extension of the Term be granted to MSI, the designated authority shall notify MSI of its decision at least 3 (three) months prior to the expiry of the Term. Upon receipt of such notice, MSI shall continue to perform all its obligations hereunder, until such reasonable time beyond the Term of the Contract within which, the designated authority shall either appoint an alternative agency/MSI or create its own infrastructure to operate such Services as are provided under this Contract.

24 Dispute Resolution

24.1 In case, a dispute is referred to arbitration, the arbitration shall be under the **Indian Arbitration and Conciliation Act, 1996** and any statutory modification or re-enactment thereof.

24.2 If during the subsistence of this Contract or thereafter, any dispute between the Parties hereto arising out of or in connection with the validity, interpretation, implementation, material breach or any alleged material breach of any provision of this Contract or regarding any question, including as to whether the termination of this Contract by one Party hereto has been legitimate, the Parties hereto shall endeavor to settle such dispute amicably and/or by Conciliation to be governed by the Arbitration and Conciliation Act, 1996 or as may be agreed to between the Parties. The attempt to bring

about an amicable settlement is considered to have failed as soon as one of the Parties hereto, after reasonable attempts; which attempt shall continue for not less than thirty (30) days, gives thirty (30) day notice to refer the dispute to arbitration to the other Party in writing.

24.3 The Arbitration proceedings shall be governed by the Arbitration and Conciliation Act, 1996.

24.4 The Arbitration proceedings shall be held in Madhya Pradesh, India.

24.5 The Arbitration proceeding shall be governed by the substantive laws of India.

24.6 The proceedings of Arbitration shall be in Hindi/English language.

24.7 Except as otherwise provided elsewhere in the contract if any dispute, difference, question or disagreement arises between the parties hereto or their respective representatives or assignees, at any time in connection with construction, meaning, operation, effect, interpretation or out of the contract or breach thereof the same shall be referred to a Tribunal of three (3) Arbitrators, constituted as per the terms of and under the (Indian) Arbitration and Conciliation Act, 1996. MD of MPUDC or the Commissioner of UADD will be the Arbitrator in this case, along with the arbitrators nominated by each party.

24.8 In case, a party fails to appoint an arbitrator within 30 days from the receipt of the request to do so by the other party or the two Arbitrators so appointed fail to agree on the appointment of third Arbitrator within 30 days from the date of their appointment upon request of a party, the Chief Justice of the Madhya Pradesh High Court or any person or institution designated by him shall appoint the Arbitrator/Presiding Arbitrator upon request of one of the parties.

24.9 Any letter, notice or other communications dispatched to MSI relating to either arbitration proceeding or otherwise whether through the post or through a representative on the address last notified to the designated authority by MSI shall be deemed to have been received by MSI although returned with the remarks, refused 'undelivered' where about not known or words to that effect or for any other reasons whatsoever

24.10 If the Arbitrator so appointed dies, resigns, incapacitated or withdraws for any reason from the proceedings, it shall be lawful for the designated authority to appoint another person in his place in the same manner as aforesaid. Such person shall proceed with the reference from the stage where his predecessor had left if both parties consent for the same; otherwise, he shall proceed de novo.

24.11 It is a term of the contract that the party invoking arbitration shall specify all disputes to be referred to arbitration at the time of invocation of arbitration and not thereafter.

24.12 It is also a term of the contract that neither party to the contract shall be entitled for any interest on the amount of the award.

24.13 The Arbitrator shall give reasoned award and the same shall be final, conclusive and binding on the parties.

24.14 The fees of the arbitrator, costs and other expenses incidental to the arbitration proceedings shall be borne equally by the parties.

25 . Conflict of interest

25.1 MSI shall disclose to the designated authority in writing, all actual and potential conflicts of interest that exist, arise or may arise (either for MSI or MSI's Team) in the course of performing the Services as soon as practical after it becomes aware of that conflict.

26 Trademarks, Publicity

26.1 Neither Party may use the trademarks of the other Party without the prior written consent of the other Party except that the MSI may, upon completion, use the Project as a reference for credential purpose. Except as required by law or the rules and regulations of each stock exchange upon which the securities of one of the Parties is listed, neither Party shall publish or permit to be published either alone or in conjunction with any other person any press release, information, article, photograph, illustration or any other material of whatever kind relating to this Agreement, the SLA or the business of the Parties without prior reference to and approval in writing from the other Party, such approval not to be unreasonably withheld or delayed provided however that the MSI may include the designated authority or its client lists for reference to third parties subject to the prior written consent of the designated authority not to be unreasonably withheld or delayed. Such approval shall apply to each specific case and relate only to that case.

27 Force Majeure

27.1 Definition of Force Majeure

The MSI or the designated authority, as the case may be, shall be entitled to suspend or excuse performance of its respective obligations under the Contract to the extent that such performance is impeded by an event of force majeure ('Force Majeure').

27.2 Force Majeure Events

A Force Majeure event means any event or circumstance or a combination of events and circumstances referred to in this Clause, which:

i. is beyond the reasonable control of the affected Party;

ii. such Party could not have prevented or reasonably overcome with the exercise of

reasonable skill and care;

iii. does not result from the negligence of such Party or the failure of such Party to perform its obligations under the Contract;

iv. is of an incapacitating nature and prevents or causes a delay or impediment in performance; and

v. may be classified as all or any of the following events:

a) act of God like earthquake, flood, inundation, landslide, storm, tempest, hurricane, cyclone, lightning, thunder or volcanic eruption that directly and adversely affect the performance of services by the MSI under the Contract;
b) radioactive contamination or ionizing radiation or biological contamination (except as may be attributable to the MSI's use of radiation or radioactivity or biologically contaminating material) that directly and adversely affect the performance of services by the MSI under the Contract;
c) industry wide strikes, lockouts, boycotts, labour disruptions or any other industrial disturbances, as the case may be, not arising on account of the acts or omissions of the MSI and which directly and adversely affect the timely implementation and continued operation of the Project; or
d) an act of war (whether declared or undeclared), hostilities, invasion, armed conflict or act of foreign enemy, blockade, embargo, prolonged riot, insurrection, terrorist or military action, civil commotion or politically motivated sabotage, for a continuous period exceeding seven (7) days that directly and adversely affect the performance of services by the MSI under the Contract.

For the avoidance of doubt, it is expressly clarified that the failure on the part of the MSI under the Contract or the SLA to implement any disaster contingency planning and back-up and other data safeguards in accordance with the terms of the Contract or the SLA against natural disaster, fire, sabotage or other similar occurrence shall not be deemed to be a Force Majeure event. For the avoidance of doubt, it is further clarified that any negligence in performance of Services which directly causes any breach of security like hacking shall not be considered as arising due to forces of nature and shall not qualify under the definition of "Force Majeure". The MSI will be solely responsible to complete the risk assessment and ensure implementation of adequate security hygiene, best practices, processes and technology to prevent any breach of security and any resulting liability therefrom (wherever applicable).

27.3 Notification procedure for Force Majeure

i. The affected Party shall notify the other Party of a Force Majeure event within seven (7) days of occurrence of such event. If the other Party disputes the claim for relief under Force Majeure it shall give the claiming Party written notice of such dispute within thirty (30) days of such notice. Such dispute shall be dealt with in accordance with the dispute resolution mechanism in the Agreement.

ii. Upon cessation of the situation which led the Party claiming Force Majeure, the claiming Party shall within seven (7) days thereof notify the other Party in writing of

the cessation and the Parties shall as soon as practicable thereafter continue performance of all obligations under the Contract.

27.4 Allocation of costs arising out of Force Majeure

i. Upon the occurrence of any Force Majeure event prior to the Effective Date, the Parties shall bear their respective costs and no Party shall be required to pay to the other Party any costs thereof.

ii. Upon occurrence of a Force Majeure event after the Effective Date, the costs incurred and attributable to such event and directly relating to the Project ('Force Majeure Costs') shall be allocated and paid as follows:

a) Upon occurrence of an event mentioned in clause 28.2 (i), (ii), (iii) and (iv), the Parties shall bear their respective Force Majeure Costs and neither Party shall be required to pay to the other Party any costs thereof.
b) Save and except as expressly provided in this Clause, neither Party shall be liable in any manner whatsoever to the other Party in respect of any loss, damage, costs, expense, claims, demands and proceedings relating to or arising out of occurrence or existence of any Force Majeure event or exercise of any right pursuant hereof.

27.5 Consultation and duty to mitigate

Except as otherwise provided in this Clause, the affected Party shall, at its own cost, take all steps reasonably required to remedy and mitigate the effects of the Force Majeure event and restore its ability to perform its obligations under the Contract as soon as reasonably practicable. The Parties shall consult with each other to determine the reasonable measures to be implemented to minimize the losses of each Party resulting from the Force Majeure event. The affected Party shall keep the other Party informed of its efforts to remedy the effect of the Force Majeure event and shall make reasonable efforts to mitigate such event on a continuous basis and shall provide written notice of the resumption of performance hereunder.

28 Delivery

28.1 MSI shall bear the cost for packing, transport, insurance, storage and delivery of all the goods for "Selection of Master System Integrator And Cloud Service Provider for Integrated Data Centre for Smart Cities and City Integrated Command and Control Centers for the State of Madhya Pradesh" at all locations identified by the designated authority for selected cities within Madhya Pradesh.

28.2 The Goods and manpower supplied under the Contract shall conform to the standards mentioned in the RFP, and, when no applicable standard is mentioned, to the authoritative standards; such standard shall be approved by the designated authority.

28.3 MSI shall only procure the hardware and software after approvals from the designated Committee.

29 . Insurance

29.1 The Goods supplied under this Contract shall be comprehensively insured by MSI at his own cost, against any loss or damage, for the entire period of the contract. MSI shall submit to the designated authority, documentary evidence issued by the insurance company, indicating that such insurance has been taken.

29.2 MSI shall bear all the statutory levies like customs, insurance, freight, etc. applicable on the goods and also the charges like transportation charges, octroi, etc. that may be applicable till the goods are delivered at the respective sites of installation shall also be borne by MSI.

29.3 MSI shall take out and maintain at its own cost, on terms and conditions approved by the designated authority, insurance against the risks, and for the coverages, as specified below;

a. at the designated authority's request, shall provide evidence to the designated authority showing that such insurance has been taken out and maintained and that the current premiums therefor have been paid.

b. Employer's liability and workers' compensation insurance in respect of the Personnel of the Company, in accordance with the relevant provisions of the Applicable Law, as well as, with respect to such Personnel, any such life, health, accident, travel or other insurance as may be appropriate

30 Transfer of Ownership

30.1 MSI must transfer all titles to the assets and goods procured for the purpose of the project to the designated authority at the time of Acceptance of System. This includes all licenses, titles, certificates, hardware, devices, equipment's etc. related to the system designed, developed, installed and maintained by MSI. Ownership of Goods that are part of this Agreement shall not pass to the designated authority unless and until the Goods is accepted in accordance with the conditions of the Contract and to the entire satisfaction of the designated authority and an acceptance notification is provided by the designated authority for to the MSI. MSI is expected to transfer IPR and ownership right of only those solutions which would be customized by MSI for the use of designated authority. For any pre-existing work, MSI and the designated authority shall be held jointly responsible and its use in any other project by MSI shall be decided on mutual consent.

30.2 Forthwith upon expiry or earlier termination of the Contract and at any other time on demand by the designated authority, MSI shall deliver to the designated authority all Documents provided by or originating from the designated authority and all Documents produced by or from or for MSI in the course of performing the Services, unless otherwise directed in writing by the designated authority at no additional cost. MSI shall not, without

the prior written consent of the designated authority store, copy, distribute or retain any such Documents.

30.3 The MSI shall execute such documents as may be required by the designated authority for documenting the transfer of title and ownership of Goods. Upon transfer of ownership of the Goods to the designated authority, the MSI shall treat such Goods as Assets as detailed above in this Agreement.

31 Exit Management Plan

31.1 An Exit Management plan shall be furnished by MSI in writing to the designated authority within 90 days from the date of signing the Contract, which shall deal with at least the following aspects of exit management in relation to the contract as a whole and in relation to the Project Implementation, and Service Level monitoring.

i. A detailed program of the transfer process that could be used in conjunction with a Replacement Service Provider 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;
ii. Plans for provision of contingent support to Project and Replacement Service Provider for a reasonable period after transfer.
iii. Exit Management plan in case of normal termination of Contract period
iv. Exit Management plan in case of any eventuality due to which Project is terminated before the contract period.
v. Exit Management plan in case of termination of MSI
vi. Exit Management Plan shall be presented by the MSI to and approved by the designated authority or its nominated agencies

31.2 Exit Management plan at the minimum adhere to the following:

i. Three (3) months of the support to Replacement Service Provider post termination of the Contract
ii. Complete handover of the Planning documents, bill of materials, functional requirements specification, technical specifications of all equipment, change requests if any, reports, documents and other relevant items to the Replacement Service Provider/ Designated Authority
iii. Certificate of Acceptance from authorized representative of Replacement Service Provider issued to MSI on successful completion of handover and knowledge transfer

31.3 In the event of termination or expiry of the contract, Project Implementation, or Service Level monitoring, both Bidder and the designated authority shall comply with the Exit Management Plan.

31.4 During the exit management period, MSI shall use its best efforts to deliver the services.

32 Performance Security

32.1 MSI shall furnish Performance Security to the designated authority at the time as indicated in the RFP which shall be equal to 10% of the Contract Value and shall be in the form of a **Bank Guarantee Bond** from a Nationalized / Scheduled Bank in the Proforma given in Annexure of this RFP within 15 days after issuance of letter of intent (LOI) or Letter of Award (LoA) which would be valid up to a period of six months after the contract period.

32.2 In the event of the MSI being unable to service the Contract for reasons attributable to the MSI, its Consortium members or any subcontractors, or any team members, the designated authority would invoke the PBG. Notwithstanding and without prejudice to any rights whatsoever of the designated authority under the Agreement in the matter, the proceeds of the PBG shall be payable to the Contract as compensation for any loss resulting from the failure of MSI, its Consortium members or any subcontractors, or any team members to perform/comply its obligations under the contract. The designated authority shall notify the MSI in writing of the exercise of its right to receive such compensation within 30 days, indicating the contractual obligation(s) for which the MSI is in default.

32.3 The designated authority shall also be entitled to make recoveries from the MSI's bills, PBG, or from any other amount due to him, an equivalent value of any payment made to him due to inadvertence, error, collusion, misconstruction or misstatement.

32.4 In case the Project is delayed beyond the Timelines as mentioned in RFP due to reasons attributable to MSI, its Consortium members or any subcontractors, or any team members, the PBG (any one or both, if not returned) shall be accordingly extended by the MSI till completion of Scope of Work as mentioned in RFP.

33 Liquidated Damages

33.1 If MSI fails to supply, install or maintain any or all of the goods as per the contract, within the time period(s) specified in the RFP and the Service Levels provided in the Contract, the designated authority without prejudice to its other rights and remedies under the Contract, deduct from the Contract price, as liquidated damages, a sum equivalent to 0.02 % per week or part thereof of Contract Value for a milestone/quarter. In case the MSI is not solely liable for the breach of the Timelines or the Service Levels, amount of liquidated damages shall be deducted on proportionate / pro rata basis depending upon the MSI's extent of fault in such breach of the Timelines or the Service Levels. The designated authority shall have the right to determine such extent of fault and liquidated damages in consultation with the MSI and any other party it deems appropriate.

33.2 The deduction shall not in any case exceed **10 % of the contract value**. If the liquidated damages cross the cap on liquidated damages as mentioned above, the designated authority shall have the right to terminate the Agreement for default and consequences for such termination as provided in this Agreement shall be applicable.

33.3 The designated authority may without prejudice to its right to effect recovery by any other method, deduct the amount of liquidated damages from any money belonging to MSI in its hands (which includes the designated authority's right to claim such amount against MSI's Bank Guarantee) or which may become due to MSI. Any such recovery or liquidated damages shall not in any way relieve MSI from any of its obligations to complete the Work or from any other obligations and liabilities under the Contract.

33.4 Delay not attributable to MSI shall be considered for exclusion for the purpose of computing liquidated damages.

33.5 Payment of liquidated damages shall not be the sole and exclusive remedies available to the designated authority and the MSI shall not be relieved from any obligations by virtue of payment of such liquidated damages. Each of the Parties shall ensure that the range of the Services/Deliverables under the SLA shall not be varied, reduced or increased except with the prior written agreement between the designated authority and the MSI in accordance with the provisions of Change Control set out in the Contract.

34 Limitation of Liability:

Limitation of Bidder's Liability towards the designated authority:

34.1 Neither Party shall be liable to the other Party for any indirect or consequential loss or damage (including loss of revenue and profits) arising out of or relating to the Contract.

34.2 The liability of the MSI (whether in contract, tort, negligence, strict liability in tort, by statute or otherwise) for any claim in any manner related to the Contract, including the work, deliverables or Goods and Services covered by the Agreement, shall be the payment of direct damages only which shall in no event in the aggregate exceed the Contract Value

34.3 Notwithstanding anything contained in the foregoing, the liability cap and exclusion for the MSI given under this Clause shall not be applicable to the breach of indemnification obligations, confidential obligations and breach committed by MSI to the safety and security measures as provided in the Contract.

35 Ownership and Retention of Documents

35.1 The designated authority shall own the Documents, prepared by or for MSI arising out of or in connection with the Contract.

35.2 Forthwith upon expiry or earlier termination of this Contract and at any other time on demand by the designated authority, MSI shall deliver to the designated authority all

documents provided by or originating from the designated authority and all documents produced by or for MSI in the course of performing the Services, unless otherwise directed in writing by the designated authority at no additional cost. MSI shall not, without the prior written consent of the BSCDCL store, copy, distribute or retain any such documents.

36 Information Security

36.1 MSI shall not carry any written/printed document, layout diagrams, CD, hard disk, storage tapes, other storage devices or any other goods /material proprietary to the designated authority into / out of any location without written permission from the designated authority. The designated authority. The MSI's personnel shall follow the designated authority's Information Security policy. The MSI acknowledges that the designated authority's business data and other designated authority proprietary information or materials, whether developed by the designated authority or being used by the designated authority pursuant to a license agreement with a third party (the foregoing collectively referred to herein as "proprietary information") are confidential and proprietary to the designated authority; and the MSI agrees to use reasonable care to safeguard the proprietary information and to prevent the unauthorized use or disclosure thereof, which care shall not be less than that used by the MSI to protect its own proprietary information.

36.2 MSI shall not destroy any unwanted documents, defective tapes/media present at any location on their own. All such documents, tapes/media shall be handed over to the designated authority.

36.3 All documentation and media at any location shall be properly identified, labeled and numbered by MSI. MSI shall keep track of all such items and provide a summary report of these items to the designated authority whenever asked for.

36.4 Access to designated authority's data and systems, Internet facility by MSI at any location shall be in accordance with the written permission by the designated authority. The designated authority shall allow MSI to use facility in a limited manner subject to availability. It is the responsibility of MSI to prepare and equip himself in order to meet the requirements.

36.5 MSI must acknowledge that designated authority's business data and other designated authority proprietary information or materials, whether developed by the designated authority or being used by the designated authority pursuant to a license agreement with a third party (the foregoing collectively referred to herein as "proprietary information") are confidential and proprietary to designated authority; and MSI along with its team agrees to use reasonable care to safeguard the proprietary information and to prevent the unauthorized use or disclosure thereof, which care shall not be less than that used by MSI to protect its own proprietary information. MSI recognizes that the goodwill of designated authority depends, among other things, upon MSI keeping such proprietary information confidential and that unauthorized disclosure of the same by MSI or its team could damage the goodwill of designated authority, and that by reason of MSI's

duties hereunder. MSI may come into possession of such proprietary information, even though MSI does not take any direct part in or furnish the services performed for the creation of said proprietary information and shall limit access thereto to employees with a need to such access to perform the services required by this agreement. MSI shall use such information only for the purpose of performing the said services.

36.6 MSI shall, upon termination of this agreement for any reason, or upon demand by designated authority, whichever is earliest, return any and all information provided to MSI by designated authority, including any copies or reproductions, both hardcopy and electronic.

36.7 By virtue of the Contract, MSI team may have access to personal information of the designated authority and/or a third party. The designated authority has the sole ownership of and the right to use, all such data in perpetuity including any data or other information pertaining to the citizens that may be in the possession of MSI team in the course of performing the Services under the Contract

37 Records of contract documents

37.1 MSI shall at all-time make and keep sufficient copies of the process manuals, operating procedures, specifications, Contract documents and any other documentation for him to fulfil his duties under the Contract.

37.2 MSI shall keep on the Site at least three copies of each and every specification and Contract Document, in excess of his own requirement and those copies shall be available at all times for use by the designated authority's Representative and by any other person authorized by the designated authority's Representative.

38 Security and Safety

38.1 The MSI shall comply with the technical requirements of the relevant security, safety and other requirements specified in the Information Technology Actor any other Applicable Law, IT Security Manual of the designated authority and the directions issued from time to time by the designated authority and follow the industry standards related to the security and safety, in so far as it applies to the provision of the Services.

38.2 The Parties shall use reasonable endeavours to report forthwith in writing to each other all identified attempts (whether successful or not) by unauthorized persons (including unauthorized persons who are employees of any Party) either to gain access to or interfere with the designated authority as the case may be or any of their nominees data, facilities or the Confidential Information.

38.3 MSI shall upon reasonable request by the designated authority, or its nominee(s) participate in regular meetings when safety and information technology security matters are reviewed.

38.4 As per the provisions of the Contract, the MSI shall promptly report in writing to the designated authority or its nominated agencies, any act or omission which they are aware that could have an adverse effect on the proper conduct of safety and Information Technology security at the facilities of the designated authority as the case may be

39 Confidentiality

39.1 The designated authority may allow the MSI to utilize highly Confidential Information including confidential public records and the MSI shall maintain the highest level of secrecy, confidentiality and privacy with regard to such Confidential Information. The MSI shall use its best efforts to protect the confidentiality, integrity and proprietary of the Confidential Information. No member of MSI's Team shall, without prior written consent from the designated authority, make any use of any Confidential and Proprietary Information given by the designated authority, except for purposes of performing the Contract. Each member of MSI's Team shall keep all the Confidential and Proprietary Information, provided by the- designated authority to them or their respective employees as confidential.

39.2 Additionally, the MSI shall keep confidential all the details and information with regard to the Project, including systems, facilities, operations, management and maintenance of the systems/facilities. The MSI shall use the information only to execute the Project.

39.3 The designated authority shall retain all rights to prevent, stop and if required take the necessary punitive action against the MSI regarding any forbidden disclosure. The designated authority reserves the right to adopt legal proceedings, civil or criminal, against the MSI in relation to a dispute arising out of breach of obligation by the MSI under this clause.

39.4 The MSI shall execute a corporate non-disclosure agreement with designated authority in the format provided by the BSCDCL and shall ensure that all its employees, agents and Sub-Contractors execute individual non-disclosure agreements, which have been duly approved by the designated authority with respect to this Project.

39.5 The MSI may only disclose the Confidential Information in the following circumstances:

a) with the prior written consent of the designated authority;

b) to a member of the MSI's Team ("Authorised Person") provided the Authorised Person needs to know the Confidential Information for accomplishment of the Services and the Authorised Person has executed a confidentiality agreement with the designated authority prior to receiving such information (SI and every other member of MSI's Team shall ensure that such Authorised Person to whom such information is disclosed are bound by the similar confidentiality obligations as applicable to each member of MSI's Team. Disclosure to any such Authorised Person shall be made in confidence on need to know basis i.e., so far as may be necessary for such Authorised Person for the purposes of-performance of the

obligations of the Contract); and

c) if and to the extent that the MSI is compelled legally to disclose the Confidential Information.

39.6 When the MSI is aware of any steps being taken or considered to compel legally the MSI or an Authorised Person to disclose the Confidential Information, it shall:

a. to the extent legally permitted, defer and limit the disclosure with a view to preserving the confidentiality of the Confidential Information as much as possible;

b. promptly notify the designated authority; and

c. do anything reasonably required by the designated authority to oppose or restrict that disclosure.

39.7 The MSI shall notify the designated authority promptly if it is aware of any disclosure of the Confidential Information otherwise than as permitted by the Contract or with the authority of the designated authority.

39.8 Any Confidential Information disclosed by MSI shall be treated as Confidential Information by the designated authority on the same terms and conditions above as applicable to the Confidential Information of the designated authority.

39.9 All documentation and media at the respective Datacenter Sites shall be properly identified, labelled and numbered by the MSI. MSI shall keep track of all such items and provide a summary report of these items to the designated authority on a monthly basis.

39.10 The obligations of confidentiality under the Contract shall remain in force for the Term of the Contract and shall survive for a period of three (3) years after expiry of the Term or earlier termination.

39.11 Obligations under this clause shall not apply to any information which is: (a) previously known to the MSI at the time of disclosure without obligation of confidentiality, (b) independently developed by MSI and not derived from the Confidential Information supplied by the MSI or the participation of individuals who have had access to Confidential Information, (c) disclosed to MSI by a third party without an obligation of confidentiality, (d) in or subsequently comes into the public domain (other than as a result of a breach of the Contract); or (e) required to be disclosed by the MSI by law, regulation, court order or other legal process, provided, where legally permissible, MSI provides written notice to the designated authority prior to such disclosure and provide reasonable assistance to the designated authority in retaining the confidentiality of such information.

40 Events of Default by MSI

40.1 The failure on the part of MSI to perform any of its obligations or comply with any of the terms of the Contract shall constitute an Event of Default on the part of MSI. The events of default are but not limited to:

i. MSI/ Bidder's Team has failed to perform the obligations under the Contract failed to execute the Scope of Work or provide Services under the Contract, or

ii. MSI/ Bidder's Team has failed to confirm / adhere to any of the key performance indicators as laid down in the RFP and in the Contract. The above mentioned failure on the part of MSI may be in terms of failure to adhere to performance, quality, timelines, specifications, requirements or any other criteria as defined by the designated authority;

iii. MSI has failed to remedy a defect or failure to perform its obligations in accordance with the specifications issued by the designated authority, despite being served with a default notice which laid down the specific deviance on the part of MSI/ MSI's Team to comply with any stipulations or standards as laid down by the designated authority; or

iv. MSI/ MSI's Team has failed to adhere to any amended direction, instruction, modification or clarification as issued by the designated authority during the Term of this Contract and which the designated authority deems proper and necessary for the execution of the Scope of Work under this Contract

v. MSI/ MSI's Team has failed to demonstrate or sustain any representation or warranty made by it in this Contract, with respect to any of the terms of its Bid, the RFP and this Contract

vi. There is a proceeding for bankruptcy, insolvency, winding up or there is an appointment of receiver, liquidator, assignee, or similar official against or in relation to MSI.

vii. MSI/ Bidder's Team has failed to comply with or is in breach or contravention of any Applicable Laws.

viii. Undue delay in achieving the agreed timelines for delivering the services under the Contract.

ix. Quality of Deliverables and services consistently not being to the satisfaction of the designated authority;

40.2 Where there has been an occurrence of such defaults inter alia as stated above, the designated authority shall issue a notice of default to SI, setting out specific defaults / deviances / omissions / non-compliances / non-performances and providing a notice of thirty (30) days to enable such defaulting party to remedy the default committed.

40.3 Where despite the issuance of a default notice to MSI by the designated authority, SISI fails to remedy the default to the satisfaction of the designated authority, the designated authority may, where it deems fit, issue to the defaulting party another default notice or proceed to contract termination.

40.4 Consequences for Events of Default

Where an Event of Default subsists or remains uncured, the designated authority shall be entitled to:

i. Impose any such obligations and conditions and issue any clarifications as may be necessary to, inter alia, ensure smooth continuation of the Services and the project which the MSI shall be obliged to comply with, which may include unilateral re-determination of the consideration payable to the MSI under the Contract. The MSI shall in addition take all available steps to minimize loss resulting from such event of default.

ii. Suspend all payments to the MSI under the Agreement by written notice of suspension to the MSI provided that such notice of suspension shall (a) specify the nature of failure; and (b) request the MSI to remedy such failure within a specified period from the date of receipt of such notice of suspension by the SI

iii. Where the designated authority deems it necessary, it shall have the right to require replacement of any of the Sub-Contractors with another suitable sub-contractor. The Sub-Contractor/ MSI shall in such case terminate forthwith all their agreements/contracts, other arrangements with such Sub-Contractor and find out the suitable replacement for such outgoing subcontractor with another Sub-Contractor to the satisfaction of the designated authority, who shall execute such contracts with the designated authority as the designated authority may require. Failure on the part of the MSI to find a suitable replacement and/or terminate all agreements/contracts with such member, shall amount to a breach of the terms hereof and the designated authority in addition to all other rights, have the right to claim damages and recover from the MSI all losses/ or other damages that may have resulted from such failure.

iv. Terminate the Contract in full or in part.

v. Retain such amounts from the payment due and payable by the designated authority to the MSI as may be required to offset any losses caused to the designated authority as a result of such event of default and the MSI shall compensate the designated authority for any such loss, damages or other costs, incurred by the designated authority in this regard. Nothing herein shall effect the continued obligation of the subcontractor / other members of its Team to perform all their obligations and responsibilities under the Contract in an identical manner as were being performed before the occurrence of the default.

vi. Invoke the Performance Bank Guarantee and other Guarantees furnished hereunder, enforce indemnity provisions, recover such other costs/losses and other amounts from the MSI which may have resulted from such default and pursue such other rights and/or remedies that may be available to the designated authority under law.

41 Termination

41.1 The designated authority may, terminate this Contract in whole or in part by giving MSI a prior and written notice indicating its intention to terminate the Contract under the following circumstances:

i. Where the designated authority is of the opinion that there has been such Event of Default on the part of MSI / MSI's Team which would make it proper and necessary to terminate the Contract and may include failure on the part of MSI to respect any of its commitments with regard to any part of its obligations under its Bid, the RFP or under the Contract.

ii. Where it comes to the designated authority's attention that MSI (or MSI's Team) is in a position of actual conflict of interest with the interests of the designated authority, in relation to any of terms of MSI's Bid, the RFP or this Contract.

iii. Where MSI's ability to survive as an independent corporate entity is threatened or is lost owing to any reason whatsoever, including inter-alia the filing of any bankruptcy proceedings against SI, any failure by MSI to pay any of its dues to its creditors, the institution of any winding up proceedings against MSI or the happening of any such events that are adverse to the commercial viability of MSI. In the event of the happening of any events of the above nature, the designated authority shall reserve the right to take any steps as are necessary, to ensure the effective transition of the sites pilot site to a successor agency, and to ensure business continuity

iv. The designated authority may terminate the Contract Agreement due to reason specified in clause 44;

v. The designated authority may terminate the Agreement if it comes to knowledge of the designated authority that the MSI or any of the MSI's personnel or the MSI's Sub-Contractors or such Sub-contractor's personnel have been involved in any fraudulent or corrupt practices or any other practice of similar nature.

41.2 Termination for Insolvency: The designated authority may at any time terminate the Contract by giving written notice to SI, without compensation to SI, if MSI becomes bankrupt or otherwise insolvent, provided that such termination shall not prejudice or affect any right of action or remedy which has accrued or shall accrue thereafter to the designated authority.

41.3 MSI may, subject to approval by the designated authority, terminate this Contract before the expiry of the Term by giving the designated authority a prior and written notice at least 3 months in advance indicating its intention to terminate the Contract.

42 Consequence of Termination

42.1 In the event of termination of the Contract due to any cause whatsoever, whether consequent to the stipulated Term of the Contract or otherwise the designated authority shall be entitled to impose any such obligations and conditions and issue any clarifications as may be necessary to ensure an efficient transition and effective business continuity of the project which MSI shall be obliged to comply with and take all available steps to minimize loss resulting from that termination/breach, and further allow and provide all such assistance to the designated authority and/ or the successor agency/ service provider, as may be required, to take over the obligations of MSI in relation to the execution/continued execution of the requirements of the Contract.

42.2 Where the termination of the Contract is prior to its stipulated Term on account of a Default on the part of MSI or due to the fact that the survival of MSI as an independent corporate entity is threatened/has ceased, or for any other reason, whatsoever, the designated authority, through unilateral re-determination of the consideration payable to MSI, shall pay MSI for that part of the Services which have been authorized by the designated authority and satisfactorily performed by MSI up to the date of termination. Without prejudice to any other rights, the designated authority may retain such amounts from the payment due and payable by the designated authority to MSI as may be required to offset any losses caused to the designated authority as a result of any act/omissions of MSI. In case of any loss or damage due to default on the part of MSI in performing any of its obligations with regard to executing the Schedule of Requirements under the contract, MSI shall compensate the designated authority for any such loss, damages or other costs, incurred by the designated authority. Additionally, members of its team shall perform all its obligations and responsibilities under the Contract in an identical manner as were being performed before the collapse of MSI as described above in order to execute an effective transition and to maintain business continuity. All third parties shall continue to perform all/any functions as stipulated by the designated authority and as may be proper and necessary to execute the Schedule of Requirements under the Contract in terms of MSI's Bid, the Bid Document and the Contract

42.3 Nothing herein shall restrict the right of the designated authority to invoke the Bank Guarantee and other Guarantees furnished hereunder and pursue such other rights and/or remedies that may be available to the designated authority under law.

42.4 The termination hereof shall not affect any accrued right or liability of either Party nor affect the operation of the provisions of the Contract that are expressly or by implication intended to come into or continue in force on or after such termination.

42.5 Any and all payments under this clause shall be payable only after the MSI has complied with and completed the transition and exit management as per the Exit Management Plan to the satisfaction of the designated authority. In case of expiry of the Agreement, the last due payment shall be payable to the MSI after the MSI has complied with and completed the transition and exit management as per the Exit Management Plan to the satisfaction of the designated authority.

44. Change Control Note (CCN)

44.1 This applies to and describes the procedure to be followed in the event of any proposed change to contract, site Implementation, and Service levels. Such change shall include, but shall not be limited to, changes in the scope of services provided by MSI and changes to the terms of payment.

44.2 Change requests in respect of the contract, the site implementation, or the Service levels shall emanate from the Parties' representative who shall be responsible for obtaining approval for the change and who shall act as its sponsor throughout the Change Control Process and shall complete Part A of the CCN (Annexure 13 of the RFP). CCNs shall be

presented to the other Party's representative who shall acknowledge receipt by signature of the authorized representative of the City SPV Authority.

44.3 MSI and the Authority while preparing the CCN, shall consider the change in the context of whether the change is beyond the scope of Services including ancillary and concomitant services required The CCN shall be applicable for the items which are beyond the stated/implied scope of work as per the RFP document.

44.4 MSI shall assess the CCN and complete Part B of the CCN. In completing Part B of the CCN MSI/Lead Bidder shall provide as a minimum:

- a description of the change;
- a list of deliverables required for implementing the change;
- a timetable for implementation;
- an estimate of any proposed change; o any relevant acceptance criteria;
- an assessment of the value of the proposed change;
- Material evidence to prove that the proposed change is not already covered within the scope of the RFP, Agreement and Service Levels.

44.5 Prior to submission of the completed CCN to the City SPV or its nominated agencies, MSI shall undertake its own internal review of the proposal and obtain all necessary internal approvals. As a part of this internal review process, MSI shall consider the materiality of the proposed change in the context of the Agreement, the sites, Service levels affected by the change and the total effect that may arise from implementation of the change.

44.6 Each Party shall be responsible for its own costs incurred in the quotation, preparation of CCNs and in the completion of its obligations described in this process provided MSI meets the obligations as set in the CCN. In the event MSI is unable to meet the obligations as defined in the CCN then the cost of getting it done by third party shall be borne by MSI. Change requests and CCNs shall be reported monthly to each Party's representative who shall prioritize and review progress.

44.7 City SPV Authority after approving change request will submit the approved Change request to BSCDCL for consideration of the payment in next payment cycle.

45. Quotation

a. MSI shall assess the CCN and complete Part B of the CCN. In completing

Part B of the CCN SI/Lead Bidder shall provide as a minimum: o a description of the change;

- a list of deliverables required for implementing the change; o a timetable for implementation;
- an estimate of any proposed change; o any relevant acceptance criteria;
- an assessment of the value of the proposed change;
- Material evidence to prove that the proposed change is not already covered within the scope of the RFP, Agreement and Service Levels.

b. Cost for the change request in CCN will be included in the subsequent invoice of the next month.

c. Prior to submission of the completed CCN to the designated City SPV authority or its nominated agencies, MSI shall undertake its own internal review of the proposal and obtain all necessary internal approvals. As a part of this internal review process, MSI shall consider the materiality of the proposed change in the context of the Agreement, the sites, Service Levels affected by the change and the total effect that may arise from implementation of the change.

Each Party shall be responsible for its own costs incurred in the quotation, preparation of CCNs and in the completion of its obligations described in this process provided MSI meets the obligations as set in the CCN. In the event MSI is unable to meet the obligations as defined in the CCN then the cost of getting it done by third party shall be borne by MSI. Change requests and CCNs shall be reported monthly to each Party's representative who shall prioritize and review progress.

B. SERVICE LEVELS

46. Purpose

46.1 The purpose is to define the levels of service provided by MSI to the designated authority for the duration of the contract. The benefits of this are:

46.2 Start a process that applies to the designated authority and MSI attention to some aspect of performance, only when that aspect drops below the threshold defined by the designated authority

46.3 Help the designated authority control the levels and performance of MSI's services

46.4 The Service Levels are between the BSCDCL and MSI

47. Service Level Agreements & Targets

47.1 This section is agreed to by the designated authority and MSI as the key performance indicator for the project. This may be reviewed and revised according to the procedures detailed in Clause 45 SLA Change Control.

47.2 The following section reflects the measurements to be used to track and report system's performance on a regular basis. The targets shown in the following tables are for the period of contact.

47.3 The procedures in Clause 49 shall be used if there is a dispute between the designated authority and MSI on what the permanent targets should be.

48. General principles of Service Level Agreements

The Service Level agreements have been logically segregated in the following categories:

48.1 Liquidated Damages

The liquidated damages shall come into effect once the notification of Award has been issued by the designated authority. It would be mainly applicable on the implementation phase of the project.

48.2 Service Level Agreement

SLA would be applicable in operations and maintenance phase of the project. The penalties shall be applicable on Operations & Maintenance cost of the project calculated quarterly. Majorly SLAs would be applicable on 1) CSP, the cloud service provider for hosting data center and disaster recovery on cloud based platform and 2) each city ICCC through which all the service integrated in city.

49. Service Levels Agreement (SLA) and Monitoring

i. Service Level Agreement (SLA) shall become the part of contract between the designated authority and the Successful bidder. SLA defines the terms of the successful Bidder's responsibility in ensuring the timely delivery of the deliverables and the correctness of the same based on the agreed Performance Indicators as detailed in this section.

ii. The successful bidder has to comply with Service Levels requirements to ensure adherence to project timelines, quality and availability of services, throughout the period of this contract i.e. during implementation phase and for a period of five (5) years. The successful bidder has to supply appropriate software/hardware/ automated tools as may be required to monitor and submit reports of all the SLAs mentioned in this section.

iii. The Service Level parameters defined in Clause 42 shall be monitored on a periodic basis, as per the individual parameter requirements. MSI shall be responsible for providing appropriate web based online SLA measurement and monitoring tools for the same. MSI shall be expected to take immediate corrective action for any breach in SLA. In case issues are not rectified to the complete satisfaction of the designated authority, within a reasonable period of time defined in this RFP, then the BSCDCL shall have the right to take appropriate penalizing actions, or termination of the contract.

iv. For purposes of the SLA, the definitions and terms as specified in the document along with the following terms shall have the meanings set forth below:

a) **"Total Time"** - Total number of hours in the quarter (or the concerned period) being considered for evaluation of SLA performance.

b) **"Uptime"** – Time period for which the specified services/ outcomes are available in the period being considered for evaluation of SLA. Formulae for calculation of Uptime: *Uptime (%) = {1-[(Downtime)/(Total time- scheduled maintenance time)]}*100*

c) **"Downtime"-** Time period for which the specified services/ components/ outcomes are not available in the concerned period, being considered for evaluation of SLA, which would exclude downtime owing to Force Majeure & Reasons beyond control of the successful bidder.

d) **"Scheduled Maintenance Time" -** Time period for which the specified services/ components with specified technical and service standards are not available due to scheduled maintenance activity. The successful bidder is required to take at least 10 days prior approval from the designated authority for any such activity. The scheduled maintenance should be

carried out during non-peak hours (like post mid-night, and should not be for more than 4 hours. Such planned downtime would be granted max 4 times a year.

e) **"Incident" -** Any event / abnormalities in the service being rendered, that may lead to disruption in normal operations and services to the end user.

f) **"Response Time" -** Time elapsed from the moment an incident is reported in the Helpdesk over phone or by any applicable mode of communication, to the time when a resource is assigned for the resolution of the same.

g) **"Resolution Time" -** Time elapsed from the moment incident is reported to Helpdesk either in person or automatically through system, to the time by which the incident is resolved completely and services as promised are restored.

50. Penalties

- A maximum level of performance penalties is established and described in the section
- Performance Penalty for not meeting a measurement parameter for any two months in consecutive quarters shall result in twice the penalty percentage of that respective measurement parameter in the third quarter for all the three months

- Maximum Penalty applicable for any quarter shall not exceed 30% of the 'applicable fees' for the respective quarter.

- Three consecutive quarterly deductions of 30 % of the applicable fee on account of any reasons shall be deemed to be an event of default and termination as per Clause 35 of this Section of RFP respectively and the consequences as provided in Clause 36 of this section of RFP shall follow.

- The payment to the agency shall be on Quarterly basis however the penalty shall be calculated on monthly basis as per the SLAs stated in the RFP.

51. Measurement of SLA

The SLA metrics provided specifies performance parameters as baseline performance, lower performance and breach. All SLA calculations will be done on quarterly basis. The SLA also specifies the liquidated damages for lower performance and breach conditions.
Payment to the MSI is linked to the compliance with the SLA metrics. The matrix specifies three levels of performance, namely,

a. The MSI will get 100% of the Contracted value if all the baseline performance metrics are compiled and the cumulative credit points are 100
b. The MSI will get lesser payment in case of the lower performance. (For e.g. if SLA point score is 80 then the MSI will get 20% less on the quarterly payment – The formula calculating the deductions is "(100 – SLA Point Score)%")
c. If the performance of the Agency in respect of any parameter falls below the prescribed lower performance limit, debit points are imposed for the breach.

The credit (+) points earned during the quarter will be considered for computing penalty. The quarterly payment shall be made after deducting the liquidated damages as mentioned above.

The aforementioned SLA parameters shall be measured as per the individual SLA parameter requirements and measurement methods, through appropriate SLA Measurement tools to be provided by the MSI and approved and audited by the designated authority or its appointed Consultant for accuracy and reliability.

BSCDCL shall also have the right to conduct, either itself or through any other agency as it may deem fit, an audit / revision of the SLA parameters. The SLAs defined, shall be reviewed by the designated authority on an annual basis after consulting the SI, Project Management Consultants and other experts. All the changes would be made by the designated authority after consultation with the MSI and might include some corrections to reduce undue relaxation in Service levels or some corrections to avoid unrealistic imposition of liquidated damages, which are noticed after project has gone live.

Total liquidated damages to be levied on the MSI shall be capped at 10% of the total contract value. However, the designated authority would have right to invoke termination of the contract in case the overall liquidated damages equals 10% of total contract value. Liquidated damages to be levied during Post Implementation period shall be capped at 10% of the OPEX value. The designated authority would also have right to invoke termination of contract in case cumulative debit point (breach points) are above 30 in 2 consecutive quarters.

51.1 Pre Implementation SLA

Timely delivery of the Scope of Work

Definition	**Timely delivery of deliverables would comprise entire bill of material and the application systems, and as per successful UAT of the same.**
Service Level Requirement	All the deliverables defined in the contract has to be submitted On-time on the date as mentioned in the contract with no delay.
Measurement of Service Level Parameter	To be measured in Number of weeks of delay from the timelines mentioned in the section “Project Timelines”
Penalty for non-achievement of SLA Requirement	Any delay in the delivery of the project deliverables (solely attributable to vendor) would attract a liquidated damage per week of 0.2% of the Total CAPEX of Request Order value per week for first 8 weeks and 0.3% per week for every subsequent week. If the liquidated damage reaches 10% of the total contract value, Authority may invoke termination clause. Liquidated damage will be computed on Total Capex value of contract/ Request order value of the particular phase

51.2 SLA Matrix for Post Implementation SLAs (City ICCC)

#	Performance Area	Baseline		Lower Performance		Breach	
		Metric	Points	Metric	Points	Metric	Points
1. Application Performance (includes any user/system application related to the project)							
1	Overall application(s) availability – Command & Control Center	99%	20	>= 96.5 % to <99%	10	< 96.5 %	0
2	Reports Generation Response Time (Alerts/MIS/Logs etc.)	Simple query - < 5secs Medium complexity query - <30 secs High Complexity query - < 1min	5	Simple complexity Query = 5.01 – 10 secs Medium complexity query = 30.01 – 60 secs High Complexity query = < 60.1 sec – 2 min	2.5	Simple complexity Query = > 10 secs Medium complexity query = > 60 secs High Complexity query = > 2 min	0
3	Maximum time for successful settings modification of field devices	< 4 secs	5	4.01 – 6.0 secs	2.5	>6 secs	0
2. End-User Equipment Uptime							
1	Monitoring workstations at Command Centers	99%	5	>= 96 % to <99%	2.5	< 96 %	0
2	IP Phones	98%	5	>= 96 % to <98%	2.5	< 96 %	0

#	Performance Area	Baseline		Lower Performance		Breach	
		Metric	Points	Metric	Points	Metric	Points
	3. Underlying IT Infrastructure Uptime/Availability at Data Centers						
1	Production Servers Uptime	99.98%	20	>= 99.5 % to <99.97%	10	< 99.5%	0
2	Storage System Uptime	99.98%	20	>= 99.5 % to <99.97%	10	< 99.5%	0
	4. Security /Patch Services for IT Infrastructure						
1	Firewall and any other security appliance Uptime	100%	15	97 % to 99.99%	7.5	< 97%	0
2	Security rules update within 2 hours of approved change management request	0 violations of service parameters	1	1 – 4 violations	0.5	> 4 violations	0
3	Anti-virus, Anti-spyware, Anti-spam updates within 24 hrs. of request	0 violations of service parameters	1	1 – 4 violations	0.5	> 4 violations	0
4	Critical Patches – within 48 hours of patch release.	0 violations of service parameters	1	1 – 4 violations	0.5	> 4 violations	0
5	Non Critical Patches – within 15 days of patch release.	Up-to 1 violations of service parameters	1	2 – 5 violations	0.5	> 5 violations	0
6	Resolution of Issue	<8 Hrs (for Critical issue) <16 Hrs (for Medium issue) <4 days (for Low issue)	1	<12 Hrs and >=8 hrs(for Critical issue) <24 Hrs and >=16 (for Medium issue) <8 days and >=4 (for Low issue)	0.5	>12 Hrs (for Critical issue) >24 Hrs (for Medium issue) >8 days (for Low issue)	0
	Total Score		**100**		**50**		**0**

51.3 Service Level Agreement for Cloud Service Provider for cloud based common data center:

Uptime Measurement

Sr. No	Parameter	Target	Measurement Method
1.	Overall Cloud Solution Availability	>=99.95%	Overall Cloud Solution Availability will be measured by following formula: Availability %age = {(Agreed Service Time – Subsystem Down Time)/ (Agreed Service time)*(100%). ** Scheduled downtime will be excluded
2.	Cloud Network Availability	>=99.95%	The component availability will be measured by following formula: Component Availability %age = {(Agreed Service Time for the component– Down Time of the component)/ (Agreed Service time for the component)*(100%)
3.	Cloud Virtualization Layer Availability	>=99.95%	<<same as above>>
4.	Cloud Storage Availability	>=99.95%	<<same as above>>
5.	Virtual Operating System Availability	>=99.95%	<<same as above>>
6.	Cloud Orchestration layer Availability	>=99.95%	<<same as above>>
7.	Cloud Security Layer Availability	>=99.95%	<<same as above>>

Cloud Service Provisioning:

Sr. No	Parameter	Target	Basis	Penalty
1.	Provisioning and De-provisioning of Virtual Machines	Within 15 minutes	Per occurrence. This will be calculated monthly	0.5% of the QP for every 1 hours of delay beyond the target time. To the maximum capping of 5 hrs. Beyond 5 hours, 1% of the QP for every 1 hour.
2.	Uptime of Cloud Resource supplied (all IT infrastructure provisioned – server, VM and other networking and security equipment) (including the Hypervisor, VM and OS running on it)	>= 99.95%	Per occurrence. This will be calculated monthly	a) <99.95% to >= 99.90% - 1% of QP b) <99.90% to >= 99.75% - 2% of QP c) <99.75% to >= 99.25% - 3% of QP d) Subsequently, for every 0.5% drop in SLA criteria - 2% of QP
3.	Uptime of Cloud Solution (including all modules specified in FRS and all network connectivity)	>= 99.95%	Per occurrence. This will be calculated monthly	a) <99.95% to >= 99.90% - 1% of QP b) <99.90% to >= 99.75% - 2% of QP c) <99.75% to >= 99.25% - 3% of QP d) Subsequently, for every 0.5% drop in SLA criteria - 2% of QP
4.	Uptime of Cloud Solution (Storage Area Network and NAS)	>= 99.95%	Per occurrence. This will be calculated monthly	a) <99.95% to >= 99.90% - 1% of QP b) <99.90% to >= 99.75% - 2% of QP c) <99.75% to >= 99.25% - 3% of QP d) Subsequently, for every 0.5% drop in SLA criteria - 2% of QP

Sr. No	Parameter	Target	Basis	Penalty
5.	Adherence to RTO	RTO is 2 Hours	Per occurrence. This will be calculated monthly	a)<=2 Hours – Nil b)>2 Hours to <=2.5 Hours – 0.5 of QP c)>2.5 Hours to <=3 Hours – 1% of QP d)>3 Hours to <=4 Hours – 2%of QP e) Subsequently, for every Hour - 2% of QP
6.	Adherence to RPO	RTO is 30 minutes	Per occurrence. This will be calculated monthly	a)<=30 Minutes – Nil b)>30 Minutes to <=45 Minutes – 0.5% of QP c)>45 Minutes to <=60 Minutes – 1% of QP d)>60 Minutes to <=75 Minutes – 2%of QP e) Subsequently, for every 30 Minutes - 2% of QP
7.	Peak CPU Utilization for Production servers	<=60%	Per occurrence. This will be calculated monthly	a) Each occurrence in servers (either same or different) that are operational at the active site and cross the peak CPU utilization of 60% for a sustained period 30 minutes each b) Each occurrence in servers (either same or different) that are operational at the active site and cross the peak CPU

Sr. No	Parameter	Target	Basis	Penalty
				utilization of 60% for a sustained period >30 minutes to <=45 minutes – 0.5% of QP c) Each occurrence in servers (either same or different) that are operational at the active site and cross the peak CPU utilization of 60% for a sustained period >=45 minutes to <=60 minutes – 1% of QP d) c) Each occurrence in servers (either same or different) that are operational at the active site and cross the peak CPU utilization of 60% for a sustained period >60 minutes – 2% of QP
8.	Peak CPU Utilization for Testing environment	<=60%	Per occurrence. This will be calculated monthly	a) Each occurrence in servers (either same or different) that are operational at the active site and cross the peak CPU utilization of 60% for a sustained period 30 minutes each b) Each occurrence in servers (either same or different) that are operational at the

Sr. No	Parameter	Target	Basis	Penalty
				active site and cross the peak CPU utilization of 60% for a sustained period >30 minutes to <=45 minutes – 0.1% of QP c) Each occurrence in servers (either same or different) that are operational at the active site and cross the peak CPU utilization of 60% for a sustained period >=45 minutes to <=60 minutes – 0.2% of QP d) Each occurrence in servers (either same or different) that are operational at the active site and cross the peak CPU utilization of 60% for a sustained period >60 minutes – 0.3% of QP
9.	Peak I/O Utilization for Production servers	<=60%	Per occurrence. This will be calculated monthly	a) Each occurrence in servers (either same or different) that are operational at the active site and cross the peak I/O utilization of 60% for a sustained period 30 minutes each

Sr. No	Parameter	Target	Basis	Penalty
				b) Each occurrence in servers (either same or different) that are operational at the active site and cross the peak I/O utilization of 60% for a sustained period >30 minutes to <=45 minutes – 0.5% of QP c) Each occurrence in servers (either same or different) that are operational at the active site and cross the peak I/O utilization of 60% for a sustained period >=45 minutes to <=60 minutes – 1% of QP d) Each occurrence in servers (either same or different) that are operational at the active site and cross the peak I/O utilization of 60% for a sustained period >60 minutes – 2% of QP
10.	Peak I/O Utilization for Testing environment	<=60%	Per occurrence. This will be calculated monthly	a) Each occurrence in servers (either same or different) that are operational at the active site and cross the peak I/O utilization of 60% for a sustained period 30 minutes each

Sr. No	Parameter	Target	Basis	Penalty
				b) Each occurrence in servers (either same or different) that are operational at the active site and cross the peak I/O utilization of 60% for a sustained period >30 minutes to <=45 minutes – 0.1% of QP c) Each occurrence in servers (either same or different) that are operational at the active site and cross the peak I/O utilization of 60% for a sustained period >=45 minutes to <=60 minutes – 0.2% of QP d) Each occurrence in servers (either same or different) that are operational at the active site and cross the peak I/O utilization of 60% for a sustained period >60 minutes – 0.3% of QP
11.	Peak Memory Utilization for Production servers	<=60%	Per occurrence. This will be calculated monthly	a) Each occurrence in servers (either same or different) that are operational at the active site and cross the peak memory utilization of 60% for a sustained period 30 minutes each

Sr. No	Parameter	Target	Basis	Penalty
				b) Each occurrence in servers (either same or different) that are operational at the active site and cross the peak memory utilization of 60% for a sustained period >30 minutes to <=45 minutes – 0.5% of QP c) Each occurrence in servers (either same or different) that are operational at the active site and cross the peak memory utilization of 60% for a sustained period >=45 minutes to <=60 minutes – 1% of QP d) Each occurrence in servers (either same or different) that are operational at the active site and cross the peak memory utilization of 60% for a sustained period >60 minutes – 2% of QP
12.	Peak Memory Utilization for Testing environment	<=60%	Per occurrence. This will be calculated monthly	a) Each occurrence in servers (either same or different) that are operational at the active site and cross the peak memory utilization of 60% for a sustained period 30 minutes each

Sr. No	Parameter	Target	Basis	Penalty
				b) Each occurrence in servers (either same or different) that are operational at the active site and cross the peak memory utilization of 60% for a sustained period >30 minutes to <=45 minutes – 0.1% of QP c) Each occurrence in servers (either same or different) that are operational at the active site and cross the peak memory utilization of 60% for a sustained period >=45 minutes to <=60 minutes – 0.2% of QP d) Each occurrence in servers (either same or different) that are operational at the active site and cross the peak memory utilization of 60% for a sustained period >60 minutes – 0.3% of QP
13.	Response time for uploading and downloading of document	95% requests within 6 seconds	Per occurrence. This will be calculated monthly	0.3% of QP

MIS Reporting:

Sr. No	Definition	Target	Penalties
1.	The bidder shall submit the MIS reports as requested by the city SPV, broadly classified below but not limited to: - IMAC (Install, Move, Add, Change) Report -Exception report indicating calls completed beyond SLA, with calculation of non-performance Deduction.	Report for the previous quarter shall be submitted to the BSCDCL within 7 working days of the beginning of new quarter	a) Up to 7 working days - No penalty b) 8 to 15 working days - 0.5 % of QP c) 16 working days to 30 days - 1 % of QP d) >30 days - 2 % of QP

The severity would be defined as follows:

a. **Critical**: In case more than 1 physical servers are down threatening business continuity (VMs on the physical server are not accessible and not working and Multiple Clients are affected) which is attributable to the Cloud Solution implemented by the SI, it shall be considered as a Critical incident.
b. **High**: In case 1 physical server is down causing high impact on business operations (VMs on physical server are not accessible/not working (few clients are affected) which is attributable to the cloud solution implemented MSI.
c. **Medium**: In case an essential functionality of the Cloud solution (like VM availability) becomes unavailable in the Live Cloud environment which is not actually hampering the live services of the Cloud but may impact the services if not attended immediately will be termed as medium.
d. **Low**: The incidents would be termed as low, which does not have any significant impact on the Cloud service delivery (little or no impact on business entity), eg:

i. A minor problem or question that does not affect the software function,

ii. An error in software product Documentation that has no significant effect on operations; or

iii. A suggestion for new features or software product enhancement.

Response Time : The response time for CSP Help Desk services incidents shall be less than 15 min.

Helpdesk Support/Issue Response and Resolution				
Sr. No	**Severity**	**Resolution Time**	**Basis**	**Penalty**
1.	Critical	<1 hour	Per Incident	No Penalty
2.	Critical	Between 1 hour and 2 hours	Per Incident unresolved	0.5% of the QP for every unresolved call
3.	Critical	Between 2 hour and 3 hours	Per Incident unresolved	1% of the QP for every unresolved call, up to 10% of QP
4.	Critical	>3 hours	Per Incident unresolved	2% of the QP for every unresolved call, up to 10% of QP
5.	High	<1.5 hour	Per Incident	No Penalty
6.	High	Between 1.5 hour and 2.5 hours	Per Incident unresolved	0.5% of the QP for every unresolved call
7.	High	Between 2.5 hour and 3.5 hours	Per Incident unresolved	1% of the QP for every unresolved call, upto 10% of QP
8.	High	>3.5 hours	Per Incident unresolved	2% of the QP for every

				unresolved call, upto 10% of QP
9.	Medium	<2 hours	Per Incident	No Penalty
10.	Medium	> 2 Hours and ≤ 4 Hours	Per Incident unresolved	0.1% of the QP for every unresolved call, up to 10% of QP
11.	Medium	>4 hours		0.5% of the QP for every unresolved call, up to 10% of QP
12.	Low	1 day from the time of incident logged at the help desk	Per Incident	No Penalty
13.	Low	> 1 day and ≤5 days	Per Incident	0.5% of the QP for every unresolved call, up to 10% of QP
14.	Low	>5 days		1% of the QP for every unresolved call, up to 10% of QP
15.	Average Call Lost Rate (Total No. Of calls lost because they were not attended by an operator /	<=1%	Per Month	0.1% of the QP for every <> 1% call lost subject to a maximum of 10% of QP

	Total incoming calls)*100			

Training

Sr. No	Parameter	Metric	Frequency/basis	Penalty
1.	Adherence to training timetable	95% of the batches at individual city to be conducted as per planned schedule.	Batches planned per department	0.1% of the QP per breach per batch.
2.	Training Feedback from Participants and training completion certification	75% of the participants in a batch to offer a feedback rating of 3 or above on a scale of 1 to 5.	Feedback Per batch	0.1% of the QP per breach per batch.

Note:

1. The Agency has to submit all the reports pertaining to SLA Review process within 2 weeks after the end of the quarter.
2. All the reports must be made available to BSCDCL, as and when the report is generated or as and when asked by the competent authority.
3. The down time will be calculated on monthly basis. Non-adherence to any of the services as mentioned below will lead to penalty as per the SLA clause and will be used to calculate downtime. The downtime calculated shall not include the following
   a. Down time due to hardware/software and application which is owned by BSCDCL at their premises

b. Negligence or other conduct of BSCDCL or its agents, including a failure or malfunction resulting from applications or services provided by BSCDCL or its vendors.

c. Failure or malfunction of any equipment or services not provided by the Bidder.

4. However, it is the responsibility/ onus of the selected Bidder to prove that the outage is attributable to BSCDCL. The selected Bidder shall obtain the proof authenticated by the BSCDCL's official that the outage is attributable to the BSCDCL.
5. The total deduction per quarter shall not exceed 20% of the total QP value
6. Two consecutive quarterly deductions amounting to more than 20% of the QPs on account of any reasons will be deemed to be an event of default and termination
7. It is the right of the BSCDCL to bring/deploy any external resources / agencies at any time for SLA review
8. No Carry forward of any penalties of SLA calculations can be done from any of the preceding quarters
9. The Agency shall deploy sufficient manpower suitably qualified and experienced in shifts to meet the SLA. Agency shall appoint as many team members as deemed fit by them, to meet the time Schedule and SLA requirements.

51.3.1 General Instructions related to SLAs mentioned above

a. Theft cases by default would not be considered as "beyond the control of Bidder". However, certain cases, based on circumstances & certain locations, the designated authority /End user department may agree to qualify as "beyond the control of Bidder".
b. Power shut down would not be considered as "beyond the control of Bidder".
c. Damages due to Road Accident / Mishap shall be considered as "beyond the control of Bidder".
d. Deliberate damage to field devices: camera, Pole etc. would not be considered as "beyond the control of Bidder"
e. Bidder is advised to have stronger poles & proper housing to protect from such damages.
f. Bidder is also required to note that in case of SLAs not being made applicable for cases considered as "beyond the control of bidders", Bidder would still need to replace the component (if it is not functional as per SLA) within the SLA defined for Resolution of Critical Level / Medium Level / Low level issues. In case bidder doesn't adhere to the Issue Resolution SLA timelines, the original SLA shall be made applicable.

51.3.2 Security Breach SLA

Note – This SLA for Security Breach is applicable over and above the SLAs mentioned in above table.

Definition	Security of the video feeds and the overall system is quite important and Successful Bidder shall be required to ensure no compromise is done on the same. Security Breach types considered for this SLA are– • Availability of Video feeds to any other user than those authorized by the designated authority /End user department and provided passwords • Availability of any report / data to any other user than those authorized by the designated authority /End user department, and provided passwords • Successful hacking of any active component on the network by any unauthorized user Or any other privacy rule is broken as per Govt. of India guidelines
Service Level Requirement	Security compliance of the system should be 100%
Measurement of Level Service Para Meter	Any reported security breach shall be logged into the SLA Management solution as a security breach
Penalty for non-achievement of SLA Requirement	For every security breach reported and proved, there shall be a penalty of 20% of the annual project billing- or lead to termination of contract

51.3.3 Breach in supply of Technical Manpower

Note – This SLA for supply of Technical Manpower is applicable over and above the SLAs mentioned in the above table.

<table>
<tr><td>Definition</td><td>Bidder is required to propose the CVs of the required technical manpower (as mentioned in Vol 2). It is vital that such manpower is available to the designated authority /End user department and performs to the expected levels. The current SLA breach shall specify penalty amount for non-availability of these man-power.</td></tr>
<tr><td>Service Level Requirement</td><td>Availability of the required man-power should be 100%. MSI to implement the biometric attendance system and share the attendance report of each person proposed as part of team on monthly basis with the designated authority.</td></tr>
<tr><td>Measurement of Service Level Parameter</td><td>Following instances would be considered as SLA non-compliances:
Replacement of a profile by the Bidder (only one replacement per profile – with equal or higher qualification and experience – would be permitted per year)
Non-deployment of the profile for more than 1 month. Authority reserves the right to ask MSI to replace (with equal or higher qualification and experience) the profile if the performance / commitment are not up to the mark
Note: Replacement due to reasons not in control of MSI (like resignation of the resource, accident, etc.) would not be counted in the permissible 1 replacement.</td></tr>
<tr><td>Penalty for non-achievement of SLA Requirement</td><td>For every SLA non-compliance reported and proved, there shall be a penalty as given below:
<table>
<tr><th>Team Member</th><th>Penalty</th></tr>
<tr><td>Project Manager</td><td>Penalty of Rs 25,000 in 1st week of non-availability
Penalty of Rs. 50,000 in 2nd week of non-availability and thereafter</td></tr>
<tr><td>For Technical Experts</td><td>Penalty of Rs 25,00 per day of non-availability for 7 days
Penalty of Rs. 5,000 per day of non-availability after 7 days</td></tr>
<tr><td>For all other team members</td><td>Penalty of Rs 1,000 per day of non-availability</td></tr>
</table></td></tr>
</table>

51.3.4 Explanation Notes for SLA Matrix

A) Application Availability

Definition	Application availability refers to the total time when the Application is available to the users for performing all activities and tasks.
Measurement of Service level Parameter	[(Total Uptime of the Application in a quarter) / (Total Time in a quarter)]*100

B) Issue Resolution

Explanation	Issue Resolution SLA shall monitor the time taken to resolve a complaint / query after it has been reported by the designated authority /End user department to the Successful Bidder.
Service Level Requirement	Different Issues/Queries shall be classified as in following three categories as defined above. **Critical** : Issue that impacts more than one production services / is raised by higher management / is impacting high importance areas **Medium**: Issue that doesn't impact more than one production services but has a potential to impact or may get escalated to top management if not resolved quickly **Low**: Upgrades, shifting, preventive maintenance. Issues which don't have impact on services.

43. Reporting Procedures

43.1. SI representative shall prepare and distribute Service level performance reports in a mutually agreed format by the **5th working day of subsequent month**. The reports shall include **"actual versus target"** Service Level Performance, a variance analysis and discussion of appropriate issues or significant events. Performance reports shall be distributed to City SPV Authority or personnel as directed by the designated authority along with monthly invoice.

43.2. Also, MSI may be required to get the Service Level performance report audited by a third-party Auditor appointed by the designated authority.

44. Issue Management Procedures

44.1. General

This process provides an appropriate management structure for the orderly consideration and resolution of business and operational issues in the event that quick consensus is not reached between the designated authority and Bidder.

Implementing such a process at the beginning of the outsourcing engagement significantly improves the probability of successful issue resolution. It is expected that this pre-defined process shall only be used on an exception basis if issues are not resolved at lower management levels.

44.2. Issue Management Process

44.2.1. Either the designated authority or MSI may raise an issue by documenting the business or technical problem, which presents a reasonably objective summary of both points of view and identifies specific points of disagreement with possible solutions.

44.2.2. Any unresolved issues/disputes concerning the Project/Contract between the Parties shall first be referred in writing to the Project Manager for his consideration and resolution. If the Project Manager is unable to resolve any issue/dispute within 5 days of reference to them, the Project Manager shall refer the matter to the Program

Management Committee. If the Program Management Committee is unable to resolve the issues/disputes referred to them within 15 days the unresolved issue/dispute shall be referred to Steering Committee / high powered committee/Project Implementation Committee for resolution. The Steering Committee within 30 days of reference to them shall try to resolve the issue/dispute.

44.2.3. If the Steering Committee fails to resolve a dispute as per the above clause, the same shall be referred to arbitration. The arbitration proceedings shall be carried out as per the Arbitration procedures mentioned in Clause 18 of this section of RFP.

52. Service Level Change Control

52.1 General

It is acknowledged that this **Service levels may change as the designated authority's business needs of all smart cities within the state of MP will evolve over the course of the contract period**. As such, this document also defines the following management procedures:

a. A process for negotiating changes to the Service Levels
b. An issue management process for documenting and resolving particularly difficult issues.
c. The designated authority and Bidder management escalation process to be used in the event that an issue is not being resolved in a timely manner by the lowest possible level of management.

Any changes to the levels of service provided during the term of this Agreement shall be requested, documented and negotiated in good faith by both parties. Either party can request a change.

52.2 Service Level Change Process: The parties may amend Service Level by mutual agreement in accordance. Changes can be proposed by either party .Unresolved issues shall also be addressed. MSI's representative shall maintain and distribute current copies of the Service Level document as directed by the designated authority. Additional copies of the current Service Levels shall be available at all times to authorized parties.

52.3 Version Control / Release Management: All negotiated changes shall require changing the version control number. As appropriate, minor changes may be accumulated for periodic release or for release when a critical threshold of change has occurred.

Schedule 4 – Annexures

1 Functional Requirements

Functional Requirements provided under are indicative, bidder carefully examine the requirements and may propose technical specification / design as per their solution to meet the objective of RFP. Below are minimum functional requirements, to be considered for this project. Bidder is free to offer better product with more functionalities.

1.1 Cloud Service Specification

i. Compute

	Requirement	Description
3.	Compute instances – ☒General Purpose ☒Memory optimized ☒Compute optimized ☒Storage optimized ☒GPU instances	Cloud provider should offer the following instance types – • General Purpose – optimized for generic applications and provides a balance of compute, memory, and network resources. • Memory optimized – optimized for memory applications • Compute optimized – optimized for compute applications • Storage optimized – include very fast/large amount of local storage for NoSQL databases and Hadoop • GPU – intended for graphics and general purpose GPU compute applications
4.	Compute instances – Burstable performance	Cloud provider should offer instances that provide a baseline level of CPU performance with the ability to burst above the baseline.
5.	Compute instances – Dedicated	Cloud provider should offer instances that run on hardware dedicated to a single customer.
6.	OS Support – Linux	Cloud provider should be able to support following Linux distributions - (Red Hat, SUSE, Ubuntu, CentOS, and Debian)
7.	OS Support – Windows	Cloud provider should be able to support the last two major Windows Server versions (Windows Server 2012, Windows Server 2008)
8.	Resize virtual cores, memory, storage seamlessly	Customer must be able to specify and modify server configuration (CPU, memory, storage) parameters seamlessly and without outage.
9.	Local disk/Instance store	Cloud service should support local storage for compute instances to be used for temporary storage of information that changes frequently.
10.	Provision multiple concurrent instances	Cloud service must offer self-service provisioning of multiple instances concurrently either through a programmatic interface (API/CLI) or through a management console.
11.	Instance affinity - logical grouping of instances within a single data center	Customer should be able to logically group instances together for applications that require low network latency and/or high network throughput.

12.	Instance anti-affinity -two or more instances hosted in different data centers	Customer should be able to split and host instances across different physical data centers to ensure that a single physical failure event does not take all instances offline.
13.	Auto Scaling support	Cloud service should be able to automatically increase the number of instances during demand spikes to maintain performance and decrease capacity during lulls to reduce costs.
14.	Bring your own image/Instance Import	Customer should be able to import their existing image and save it as a new, privately available image that can then be used to provision instances in the future.
15.	Export Instance Image	Cloud service must support the ability to take an existing running instance or a copy of an instance and export the instance into a VMDK or VHD image format.
16.	Instance maintenance mitigation	Cloud service must be architected in such a way to avoid instance outages or downtime when the provider is performing any kind of hardware or service maintenance.
17.	Instance failure recovery	Cloud service must be architected in such a way to automatically restart instances on a healthy host if the original physical host fails.
18.	Instance restart flexibility	Cloud provider must be able to schedule events for customer's instances, such as a reboot, stop/start, or retirement. Depending on the event, customer might be able to take action to control the timing of the event.
19.	Support for Docker containers	Cloud service should support containers, including Docker and/or other containerization platforms.
20.	Highly scalable, high performance container management service	Cloud provider should offer a highly scalable, high performance container management service.
21.	Event-driven computing that runs code in response to events	Cloud service should be able to run customer code in response to events and automatically manage the compute resources.
22.	License portability and support – Microsoft	Cloud provider should offer license portability and support for Microsoft apps like SQL Server and SharePoint Server.
23.	License portability and support – Oracle	Cloud provider should offer license portability and support for Oracle apps like Oracle Database 11g.
24.	License portability and support – SAP	Cloud provider should offer license portability and support for SAP apps like HANA.
25.	License portability and support – IBM	Cloud provider should offer license portability and support for IBM apps like DB2 and Websphere.
26.	Pay-as-you-go pricing	Cloud provider should offer a simple pay-as-you-go pricing where customers can pay for compute capacity by the hour with no long-term commitments.

ii. Networking

	Requirement	**Description**
27.	Multiple network interface/instance	Cloud service should be able to support multiple (primary and additional) network interfaces.
28.	Multiple IP addresses/instance	Cloud service should be able to support multiple IP addresses per instance. Use cases include hosting multiple websites on a single server and network appliances (such as load balancers) that have multiple private IP addresses for each network interface.
29.	Ability to move network interfaces and IPs between instances	Cloud service should support the ability to create a network interface, attach it to an instance, detach it from an instance, and attach it to another instance.

30.	Enhanced networking support	Cloud service should support capabilities such as single root I/O virtualization for higher performance (packets per second), lower latency, and lower jitter.
31.	Network traffic logging - Log traffic flows at network interfaces	Cloud service should support capturing information about the IP traffic going to and from network interfaces.
32.	Auto-assigned public IP addresses	Cloud service should be able to automatically assign a public IP to the instances.
33.	IP Protocol support	Cloud service should be able to support multiple IP protocols, including TCP, UDP, and ICMP protocols.
34.	Use any network CIDR, including RFC 1918	Cloud service should be able to support IP address ranges specified in RFC 1918 as well as publicly routable CIDR blocks.
35.	Static public IP addresses	Cloud provider must support IP addresses associated with a customer account, not a particular instance. The IP address should remain associated with the account until released explicitly.
36.	Auto-created default virtual private network	Cloud service should be able to create a default private network and subnet with instances launching into a default subnet receiving a public IP address and a private IP address.
37.	Subnets within private network	Customer should be able to create one or more subnets within private network with a single Classless Inter-Domain Routing (CIDR) block.
38.	Subnet level filtering (Network ACLs)	Cloud service should support subnet level filtering – Network ACLs that act as a firewall for associated subnets, controlling both inbound and outbound traffic at the subnet level.
39.	Ingress filtering	Cloud service should support adding or removing rules applicable to inbound traffic (ingress) to instances.
40.	Egress filtering	Cloud service should support adding or removing rules applicable to outbound traffic (egress) originating from instances.
41.	Disable source/destination checks on interfaces	Cloud service should support the ability to disable source/destination check on network interfaces. By default, compute instances perform source/destination checks.
42.	Configure proxy server (NAT instance) at network level	Cloud service should support NAT instances that can route traffic from internal-only instances to the Internet.
43.	Site-to-site managed VPN service	Cloud service should support a hardware based VPN connection between the cloud provider and customer data center.
44.	Virtual Network Peering	Cloud service should support connecting two virtual networks to route traffic between them using private IP addresses.
45.	Multiple VPN Connections per Virtual Network	Cloud service should support creating multiple VPN connections per virtual network
46.	BGP for high availability and reliable failover	Cloud provider should support Border Gateway Protocol. BGP performs a robust liveness check on the IPSec tunnel and simplifies the failover procedure that is invoked when one VPN tunnel goes down.
47.	Private connection to customer data centers	Cloud provider should support direct leased-line connections between cloud provider and a customer datacenter, office, or colocation environment, which in many cases can reduce network costs, increase bandwidth throughput, and provide a more consistent network experience than Internet-based connections.
48.	DNS based global load balancing	Cloud service should support Load balancing of instances across multiple host servers.

49.	Load balancing supports multiple routing methods	Cloud service should support multiple routing mechanism including round-robin, failover, sticky session etc.
50.	Front-end Load Balancer	Cloud service should support a front-end load balancer that takes requests from clients over the Internet and distributes them across the instances that are registered with the load balancer.
51.	Back-end Load Balancer	Cloud service should support an internal load balancer that routes traffic to instances within private subnets.
52.	Health checks - monitor the health and performance of application	Cloud service should support health checks to monitor the health and performance of resources.
53.	Integration with Load Balancer	Cloud service should support integration with load balancer.
54.	Low Latency	The CSP should be able to provide a 10GB network connectivity between the servers if required.

iii. Storage – Block Storage

	Requirement	**Description**
55.	Support for storage allocated as local disk to a single VM	Cloud provider should offer persistent block level storage volumes for use with compute instances.
56.	Storage volumes > 1 TB	Cloud provider should offer block storage volumes greater than 1 TB in size.
57.	SSD backed storage media	Cloud service should support solid state drive (SSD) backed storage media that offer single digit millisecond latencies.
58.	Provisioned I/O support	Cloud service should support the needs of I/O-intensive workloads, particularly database workloads that are sensitive to storage performance and consistency in random access I/O throughput.
59.	Encryption using provider managed keys	Cloud service should support encryption of data on volumes, disk I/O, and snapshots using industry standard AES-256 cryptographic algorithm.
60.	Encryption using customer managed keys	Cloud service should support encryption using customer managed keys.
61.	Durable snapshots	Cloud service should support point-in-time snapshots. These snapshots should be incremental in nature.
62.	Ability to easily share snapshots globally	Cloud Service should support sharing of snapshots across regions making it easier to leverage multiple regions for geographical expansion, data center migration, and disaster recovery.
63.	Consistent Input Output per second (IOPS)	Cloud service should support a baseline IOPS/GB and maintain it consistently at scale
64.	Annual Failure Rates <1%	Cloud service should be durable and support annual failure rates of less than 1%

iv. Storage – Object Storage

	Requirement	**Description**
65.	Scalable object storage service	Cloud provider should offer secure, durable, highly-scalable object storage for storing and retrieving any amount of data from the web.
66.	Low cost archival storage with policy support	Cloud provider should support an extremely low-cost storage service that provides durable storage with security features for data archiving and backup.

67.	Support for Server-side Encryption	Cloud service should support encryption for data at rest using 256-bit Advanced Encryption Standard (AES-256) encryption to encrypt your data.
68.	Support for Server Side Encryption with Customer-Provided Keys	Cloud service should support encryption using customer-provided keys. These keys should be used to manage both the encryption, as data is written to disks, and decryption, when data is accessed.
69.	Support for Server Side Encryption with a Key Management Service	Cloud service should support encryption using a Key Management Service that creates encryption keys, defines the policies that control how keys can be used, and audits key usage to prove they are being used correctly.
70.	Object lifecycle management	Cloud Service should support managing an object's lifecycle by using a lifecycle configuration, which defines how objects are managed during their lifetime, from creation/initial storage to deletion.
71.	Data Locality	Cloud provider should provide a strong regional isolation, so that objects stored in a region never leave the region unless customer explicitly transfers them to another region.
72.	Object change notification	Cloud service should be able to send notifications when certain events happen at the object level (addition/deletion).
73.	High-scale static web site hosting	Cloud service should be able to host a website that uses client-side technologies (such as HTML, CSS, and JavaScript) and does not require server-side technologies (such as PHP and ASP.NET).
74.	Object Versioning	Cloud Service should support versioning, where multiple versions of an object can be kept in one bucket. Versioning protects against unintended overwrites and deletions.
75.	Flexible access-control mechanisms	Cloud service should support flexible access-control policies to manage permissions for objects.
76.	Audit logs	Cloud service should be able to provide audit logs on storage buckets including details about a single access request, such as the requester, bucket name, request time, request action, response status, and error code.
77.	Multi-factor delete	Cloud service should support multi-factor delete as an additional security option for storage buckets
78.	Lower Durability offering	Cloud service should support a lower cost option for noncritical, reproducible data at lower levels of redundancy.
79.	Parallel, multipart upload	Cloud service should allow uploading a single object as a set of parts where each part is a contiguous portion of the object's data and these object parts can be uploaded independently and in any order.
80.	CDN option for users	Cloud provider should offer a service to speed up distribution of static and dynamic web content.
81.	Strong Consistency	Cloud service should support read-after-write consistency for PUT operations for new objects.
82.	Storage gateway appliance for automated enterprise backups	Cloud provider should offer a storage gateway appliance for seamlessly storing on-premises data to the cloud.
83.	Accept large data loads through shipped physical media	Cloud provider should support moving large amounts of data into the cloud by bypassing the internet.
84.	Deliver large data exports through shipped physical media	Cloud provider should support moving large amounts of data out of the cloud by bypassing the internet.

v. Storage – File Storage

	Requirement	Description
85.	Simple, scalable file storage service	Cloud provider should offer a simple scalable file storage service to use with compute instances in the cloud.
86.	SSD backed storage media	Cloud service should offer SSD backed storage media to provide the throughput, IOPS, and low latency needed for a broad range of workloads.
87.	Grow file systems to petabyte scale	Cloud service should support petabyte-scale file systems and allow thousands of concurrent NFS connections.
88.	Consistent low latency performance (T50-T99)	Cloud service should support consistent low latency performance between 5-15 ms at any scale.
89.	Scalable IOPS and throughput performance (/TB)	Cloud service should support scalable IOPS and throughput performance at any scale.
90.	Sharable across thousands of instances	Cloud service should support thousands of instances so that many users can access and share a common data source.
91.	Fully elastic capacity (no need to provision)	Cloud service should automatically scale up or down as files are added or removed without disrupting applications.
92.	Highly durable	Cloud service should be highly durable - file system object (i.e. directory, file, and link) should be redundantly stored across multiple data centers.
93.	Read-after-write consistency	Cloud service should support read after write consistency (each read and write operation is guaranteed to return the most recent version of the data).

vi. Relational Database

	Requirement	Description
94.	Managed relational database service	Cloud provider should offer a service that makes it easy to set up, operate, and scale a relational database in the cloud.
95.	Support for MySQL	Cloud service should support the last two major releases of MySQL (versions 5.6, 5.5) as a database engine.
96.	Support for Oracle	Cloud service should support the last two major releases of Oracle (11g and 12c) as a database engine.
97.	Support for Microsoft SQL Server	Cloud service should support all the editions (Express, Web, Standard, Enterprise) of SQL Server 2012 as a database engine.
98.	Support for PostgreSQL	Cloud service should support the last two major releases of PostgreSQL (9.4.x, 9.3.x)
99.	Low latency, synchronous replication across multiple data centers in a region	Cloud service should support synchronous replication of a primary database to a standby replica in a separate physical datacenter to provide data redundancy, eliminate I/O freezes, and minimize latency spikes during system backups.
100.	Read Replica support	Cloud service should support read replicas that make it easy to elastically scale out beyond the capacity constraints of a single DB Instance for read-heavy database workloads.
101.	Manual Failover	Cloud service should support a manual failover of the DB instance from primary to a standby replica.
102.	Provisioned IO support	Cloud service should support the needs of database workloads that are sensitive to storage performance and consistency in random access I/O throughput.
103.	Bring your own SQL, Oracle licenses	Cloud service should support customers who prefer to use their existing Oracle and SQL Server database licenses in the cloud.

104.	Cross region Snapshots	Cloud service should support copying snapshots of any size between different cloud provider regions for disaster recovery purposes.
105.	Cross region Read Replica	Cloud service should support creating multiple in-region and cross-region replicas per database instance for scalability or disaster recovery purposes.
106.	High Availability	Cloud Service should support enhanced availability and durability for database instances for production workloads.
107.	Point in time restore	Cloud service should support restoring a DB instance to a specific date and time.
108.	User snapshots and restore	Cloud service should support creating a DB snapshot and restoring a DB instance from a snapshot.
109.	Modifiable DB parameters	Cloud service should allow the DB parameter to be modified.
110.	Monitoring	Cloud service should allow monitoring of performance and health of a database or a DB instance.
111.	Encryption at rest	Cloud service should support encryption using the industry standard AES-256 encryption algorithm to encrypt data.

vii. Non-Relational Database

	Requirement	**Description**
112.	Scalable, fast and flexible NoSQL database service	Cloud provider should offer a fast and flexible NoSQL database service for applications that need consistent, single-digit millisecond latency at any scale.
113.	Replication	Cloud service should support automatic replication of data across multiple physical datacenters in a region to provide high availability and data durability.
114.	Performance/ Latency	Cloud service should support single-digit milliseconds (TP99) latencies at any scale.
115.	Key-value Data Model support	Cloud service should support key value data structure where the primary key is the only required attribute for items in a table and uniquely identifies each item.
116.	Document Data Model with JSON support	Cloud service should support storing, querying, and updating JSON documents.
117.	Tunable scaling	Cloud service should support seamless throughput and storage scaling.
118.	Secondary Indexes	Cloud service should support secondary indexes. Secondary indexes are indexes that contain hash or hash-and-range keys that can be different from the keys in the table on which the index is based.
119.	Streams	Cloud service should support streams. Stream is an ordered flow of information about changes to items.
120.	Cross region replication	Cloud Service should support cross-region replication to automatically replication data across multiple regions.
121.	Database triggers	Cloud Service should support database triggers - pieces of code that quickly and automatically respond to data modification in the tables.
122.	Strong consistency, Atomic counters	Cloud service should support strong consistency for read operations to make sure users are always reading the latest values.
123.	Integrated Monitoring	Cloud service should support monitoring of request throughput and latency for database tables, among other metrics.
124.	Integration with data warehouse	Cloud service should support integration with a data warehouse for advanced business intelligence capabilities.

125.	Hadoop Integration	Cloud service should support integration with a Hadoop framework to perform complex analytics on large datasets.

viii. Security and administration

	Requirement	Description
126.	Control access to your cloud resources at a granular level	Cloud provider should offer fine-grained access controls including, conditions like time of the day, originating IP address, use of SSL certificates, or authentication with a multi-factor authentication device.
127.	Utilize multi-factor authentication when accessing cloud resources	Cloud service should support multi-factor authentication. MFA requires users to prove physical possession of a hardware or virtual MFA device by providing a valid MFA code.
128.	Identify when an access key was last used to rotate old keys and remove inactive users	Cloud service should support reporting a user's access keys last use details.
129.	Policy Simulator to test policies before committing to production	Cloud service should provide a mechanism to test the effects of access control policies that are attached to users, groups, and roles before committing the policies into production.
130.	Policy validation to ensure policies match intentions	Cloud service should support a policy validator to automatically examine non-compliant access control policies.
131.	User and Group management	Cloud service should support features such as user and group management.
132.	Integration with your existing on-premises Active Directory	Cloud service should integrate with existing on-premise Active Directory.
133.	Self-service password reset for cloud users	Cloud service should allow users to reset their password in a self-service manner.
134.	Managed service to create and control the encryption keys used to encrypt your data	Cloud provider should offer a service to create and control the encryption keys used to encrypt user data.
135.	Audit of all action on keys	Cloud service should support auditing with features such as what request was made, the source IP address from which the request was made, who made the request, when it was made, and so on.
136.	Key Durability	Cloud service should support durability of keys, including storing multiple copies to ensure keys are available when needed.
137.	Web service to record API calls and deliver log files	Cloud provider should offer a service to record history of API calls and related events for a user account.
138.	Receive notification of API activity	Cloud service should support notifications when new log files are available.
139.	Durable and inexpensive log file storage	Cloud service should support storing log files in a durable and inexpensive storage solution.
140.	Choice of partner solution	Cloud service should support a variety of 3rd party solutions.
141.	Latency to deliver API activity history to a storage bucket	Cloud service should deliver API activity history within a reasonable timeframe (<30 minutes) from the time API call is made.
142.	Aggregation across multiple accounts and multiple Regions for ease of use	Cloud service should support receiving log files from multiple regions and accounts to a single location for ease of use.
143.	Managed service for resource inventory, configuration history & change notifications	Cloud provider should offer a service that provides resource inventory, configuration history, and configuration change notifications to enable security and governance.

144.	Automatically records a resource's configuration when it changes	Cloud service should automatically record a resource configuration when it changes and make this information available.
145.	Examine the configuration of your resources at any single point in the past	Customer should be able to obtain details of what a resource's configuration looked like at any point in the past using this cloud service.
146.	Receive notification of a configuration change	Cloud service should notify every configuration change so customers can process these notifications programmatically.
147.	Create and manage catalog of pre-approved services for use	Cloud provider should offer the ability to create and manage catalogs of IT services that are approved for use.

Security and administration – Independent 3rd party Assurance Programs

	Requirement	**Description**
148.	3rd party Assurance Programs ☒SOC1 / ISAE 3402 ☒SOC2 / SOC3 ☒ISO 27001 ☒ISO 9001 ☒PCI DSS Level 1 ☒FISMA ☒FIPS 140-2 ☒CSA	Cloud provider should meet a broad set of international and industry-specific compliance standards: ISO 27001, ISO 27017, ISO 27018, SOC 1, SOC 2, and SOC 3.

ix. Deployment and Management

	Requirement	**Description**
149.	Service to quickly deploy and manage applications in the cloud	Cloud provider should offer a service to quickly deploy and manage applications in the cloud by automatically handling the deployment, from capacity provisioning, load balancing, auto-scaling to application health monitoring.
150.	Supported Platforms ☒Java ☒Python ☒Ruby ☒Google Go ☒.NET ☒PHP ☒Node.js	Cloud service should support a wide variety of platforms from Java and .NET to Google Go.
151.	Supported OS ☒Windows ☒Linux ☒any OS in Docker	Cloud Service should support Windows, Linux, and Docker containers.
152.	Deployment Mechanism ☒Git ☒Visual Studio ☒Zip ☒Eclipse	Cloud service should support various deployment mechanisms, including a Git repository, or an integrated development environment (IDE) such as Eclipse or Visual Studio.
153.	Support for SSL connections	Cloud service should support SSL connections.
154.	Application source versioning	Cloud service should support application source versioning. This would be useful for applications that have been updated and need to be redeployed.
155.	Auto scaling	Cloud service should support automatically launching or terminating instances based on the parameters such as CPU utilization defined by users.
156.	Swap virtual IP between staging and production environments	Cloud service should support swapping IP addresses between staging and production environments so that a new application version can be deployed with zero downtime.

157.	Integration with caching solution	Cloud service should be integrated with a caching solution such as Redis cache.
158.	Service to create a collection of related resources and provision them using a template	Cloud provider should offer a service to create a collection of related resources and provision them in an orderly and predictable fashion using a template.
159.	Single JSON based template to declare your stack	Cloud service should use a template, a JSON-format, text-based file that describes all the resources required for an application. The resources in the template should be managed as a single unit.
160.	Allow parametrization and specific configurations	Cloud service should support parameterization for specific configuration.

x. Application Services

	Requirement	**Description**
161.	Search service	Cloud provider should offer a search service in the Cloud that makes it simple and cost-effective to set up, manage, and scale a search solution for websites or applications.
162.	Queueing service	Cloud provider should offer a fast, reliable, scalable, fully managed message queuing service.
163.	Notification service	Cloud provider should offer a fast, flexible, fully managed push notification service that lets users send individual messages or to fan-out messages to large numbers of recipients.
164.	Media transcoding service	Cloud provider should offer a highly scalable, easy to use and a cost effective media transcoding service in the cloud.

xi. Hybrid Integration

	Requirement	**Description**
165.	Hardware-based virtual private networking connection to cloud resources	Cloud provider should be able to extend customer's data center to the cloud and enable communication with their own network over an IPsec VPN tunnel.
166.	High speed, low latency, dedicated connectivity between on-premises & cloud	Cloud provider should provide mechanisms to establish private connectivity between the cloud environment and a customer datacenter, office, or colocation environment.
167.	Automated VM import functionality	Cloud provider should allow customers to import VMs from a virtualization environment such as Citrix Xen, Microsoft Hyper-V, or VMware vSphere.
168.	Automated VM export functionality	Cloud provider should allow customers to export instances to their on-premises virtualization environments.
169.	Integrate with on-premises Active Directory	Cloud service should integrate with existing on-premise Active Directory.
170.	Use any IP address range, including RFC 1918	Cloud service should be able to support IP address ranges specified in RFC 1918 as well as publicly routable CIDR blocks.
171.	Highly durable, automatic data replication, and recovery service from on-premises	Cloud provider should offer a service to automatically replicate data from on-premises to cloud for disaster recovery purposes.
172.	Backup service to back up on-premises servers	Cloud provider should offer a service with ability to take regular and scheduled back of on-premises servers.
173.	Utilize multi-factor authentication when accessing cloud resources	Cloud service should support multi-factor authentication. MFA requires users to prove physical possession of a hardware or virtual MFA device by providing a valid MFA code.

174.	Support from 3rd party management and monitoring tools ☒Microsoft System Center ☒VMware vCenter ☒CA ☒BMC ☒RightScale ☒Eucalyptus ☒Symantec	Cloud provider should offer management and monitoring plugins for management solutions from multiple vendors.
175.	App management service to deploy and operate apps in the Cloud or own data center	Cloud provider should offer a service to automate operational tasks like software configurations, package installations, and database setups for servers running on-premises or in the cloud.
176.	Service to automate code deployments to cloud and on-premises	Cloud provider should offer a service that automates code deployments to servers running on-premises or in the cloud.

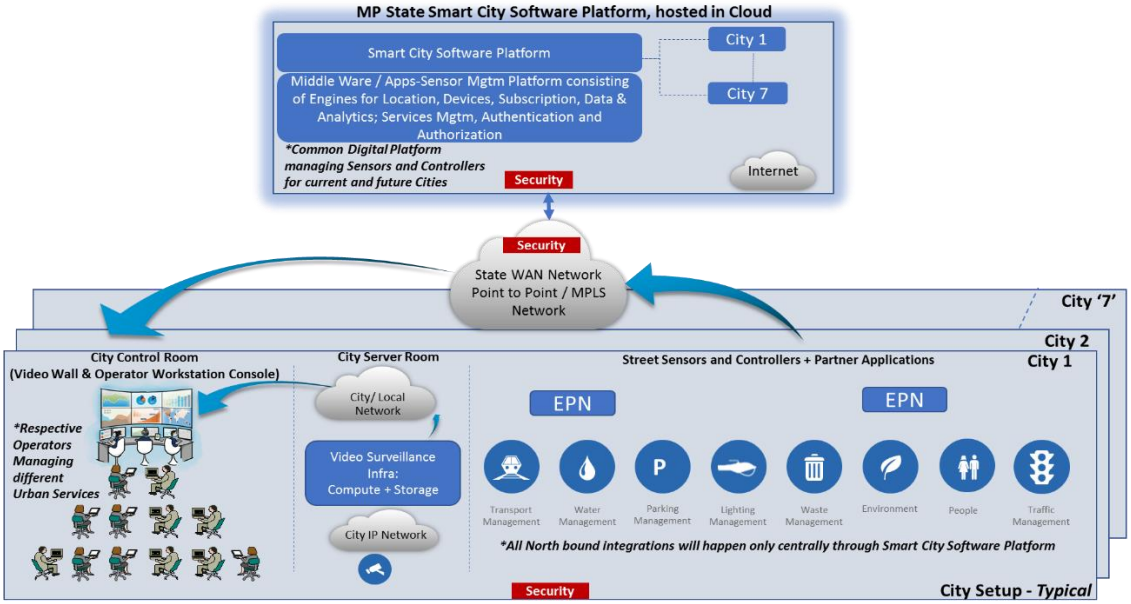
xii. Support

	Requirement	**Description**
177.	Service Health Dashboard	Cloud provider should offer a dashboard that displays up-to-the-minute information on service availability across multiple regions.
178.	365 day service health dashboard and SLA history	Cloud provider should offer 365 days' worth of Service Health Dashboard (SHD) history.
179.	Service to compare resource usage to best practices	Cloud provider should offer a service acts like a customized cloud expert and helps provision resources by following best practices.
180.	Monitoring Tools	Monitoring tools that will enable collection and tracking metrics, collection and monitoring log files, set alarms, and automatically react to changes in the provisioned resources. The monitoring tools should be able to monitor resources such as compute and other resources to gain system-wide visibility into resource utilization, application performance, and operational health.
181.	Governance and Compliance	Able to define guidelines for provisioning and configuring cloud resources and then continuously monitor compliance with those guidelines. Ability to choose from a set of pre-built rules based on common best practices or custom rules (e.g., ensure Storage volumes are encrypted, Compute instances are properly tagged, and Elastic IP addresses (EIPs) are attached to instances) and continuously monitor configuration changes to the cloud resources and provides a new dashboard to track compliance status.
182.	Audit Trail	Provide Audit Trail of the account activity to enable security analysis, resource change tracking, and compliance auditing

1.2 Functional Requirement of Command and Control Centre

The MSI has to provide, deploy and configured an integrated operations and dashboard application that integrated various Smart City use cases on this platform.

Cloud Based Architecture for Common Smart City Software Platform



Proposed Solution architecture should have combination of data normalization and City operation center software with below capabilities; data normalization software should support on-prem and cloud technology.

S.NO.	Functionality Description		Compliance (Yes/No)
1.	Data Aggregation, Normalization and Access	It is envisaged that the city will implement multiple Smart City use cases over a period of time. The potential example Smart City use cases are- • Smart Outdoor Lighting • Smart Parking • Smart Traffic Management • Smart Energy Metering • Smart Water Metering • Public Safety and Safe City Operations • Connected Public Transport • Public Wi-Fi and Urban Service Delivery over Public Wi-Fi • Kiosks for Citizen Information • Citizen Interactive Kiosks for Urban Service Delivery	

S.NO.	Functionality Description		Compliance (Yes/No)
		• Environmental Monitoring • Smart Waste Management	
2.		• Normalizes the data coming from different devices of same type (i.e. Different lighting devices, different energy meters etc…) and provide secure access to that data using data API(s) to application developers • The City will be using various device vendors for various urban services. For example, in the Smart city journey of the city, various vendors of smart elements will be used for deployment and each will be generating data in their own format. This Smart City platform should be able to define its own data model for each urban service like parking, waste, lighting, transport etc and map data from different device vendors to the common data model. This way, application development and analytics applications do not need to worry about the complexity of various data formats. • This data must be exposed to application eco system using secure APIs using API keys • The attributes of the API key(s) must restrict / allow access to relevant data, i.e. (the attributes can be like: specific domain(either parking or lighting or waste etc or combination of these), RO / RW /, specific to tenant (city, street within city etc)). • Multitenant City operations Dashboard: City software platform Dashboard should display only relevant data (associated geographincal data) for the user who logs in.	
3.		The platform should be able to integrate with any type of sensor platform being used for the urban services irrespective of the technology used. Agnostics to sensor technologies such as LoRA, ZigBee, GPRS, WiFi, IP Camera	
4.		The platform should also allow the manufacturers of the sensors to develop	

S.NO.	Functionality Description		Compliance (Yes/No)
		integrations themselves using SDKs without affecting the northbound applications and existing integration The platform should have the ability and provision to write adaptors, which interface with the sensors or sensor management software	
5.		The platform should be able to normalize the data coming from different devices of same type (i.e. Different lighting sensor from different OEMs, different energy meters from different OEMs etc.) and provide secure access to that data using data API(s) to application developers.	
6.		The platform should support distributed deployment of functions (workflows & policies) across city's network and compute infrastructure with centralized management and control	
7.	Device Abstraction method	The platform should normalize individual device data into Things Query Language—the underlying language used to communicate among devices.	
8.	GIS Map Support	System should support Esri, map box, Open street etc.	
9.	Location engine	a) Map services and geospatial coordinates: provides the geographical coordinates of specific facilities, roads, and city infrastructure assets, as well as unmapped facilities b) Geospatial calculation: calculates distance between two, or more, locations on the map c) Location-based tracking: locates and traces devices on the map	
10.	Service management	a) Data brokerage, ID Management: Performs service management	
11.	Developer Program tools	Sensor platform OEM should provide online Developer Program tools that help City to produce new applications, and/or use solution APIs to enhance or manage existing solution free of cost. OEM should have technology labs via an online public facing web interface. These labs should be available 24X7.	
12.	Authentication, Authorization	System should support standard Authentication, Authorization Performs	

S.NO.	Functionality Description		Compliance (Yes/No)
13.	Data plan Functionalities	Live data and visual feed from diverse sensors connected to the platform	
14.	API Repository / API Guide	Normalized APIs should be available for the listed domains (Parking, Outdoor Lighting, Traffic, Environment, Urban mobility etc.) to monitor, control sensor and/or actuators functionality to enable app developers to develop apps on the platform. For example Lighting APIs: Vendor agnostic APIs to control Lighting functionality.	
15.		Platform OEM should have published the normalized APIs in their website for the listed domains ((Parking, Outdoor Lighting, Traffic, Environment, Urban mobility etc.) to allow sensor vendors and app developers to develop their connectors / adaptors to the platform	
16.		Cross collaboration APIs: Enabling contextual information and correlation across domains and verticals (Multiple vendor and Multi-sensor in future)	
17.	Platform upgrade and maintenance	The OEM should be able to securely access the platform remotely for platform updates / upgrades and maintenance for the given duration	
18.		Platform should be able to be deployed on a public cloud for disaster recovery	
19.	Platform functionality	API management and gateway: Provides secure API lifecycle, monitoring mechanism for available APIs	
20.		User and subscription management: Provides different tier of user categorization, authentication, authorization, and services based on the subscriptions	
21.		Application management: Provides role-based access view to applications	
22.		Enabling analytics: Time shifted and real-time data available for big data and analytics	
23.		The platform should also be able to bring in other e-governance data (SCADA sytems) as i-frames in the command and control centre dashboard	
24.		All of these data should be rendered / visualized on the command and control centre dashboard.	
25.	CCC Operations	• The solution should be implemented and compliant to industry open standard	

S.NO.	Functionality Description		Compliance (Yes/No)
		commercial-off-the-shelf (COTS) applications that are customizable. • The solution should have the capability to integrate with GIS viz ESRI, Bing • The solution shall integrate with GIS and map information and be able to dynamically update information on the GIS maps to show status of resources. • The solution shall also provide an integrated user interface for all the smart elements implemented • The solution should provide operators and managers with a management dashboard that provides a real time status and is automatically updated when certain actions, incidents and resources have been assigned, pending, acknowledged, dispatched, implemented, and completed. The above attributes shall be color coded. • The solution shall provide the "day to day operation", "Common Operating Picture" and situational awareness to the centre and participating agencies during these modes of operation • It shall improve scalability for large and geographically distributed environments • It shall provide complete view of sensors, facilities, e-governance/erp, video streams and alarms in an easy-to-use and intuitive GIS-enabled graphical interface with a powerful workflow and business logic engine • It shall provide a uniform, coherent, user-friendly and standardized interface • It shall provide possibility to connect to workstations and accessible via web browser • The dashboard content and layout shall be configurable and information displayed on these dashboards shall be filtered by the role of the person viewing dashboard • The solution should allow creation of hierarchy of incidents and be able to	

S.NO.	Functionality Description		Compliance (Yes/No)
		present the same in the form of a tree structure for analysis purposes • The solution shall be available via a VPN as a web-based interface or a thin-client interface • It shall be possible to combine the different views onto a single screen or a multi-monitor workstation • The solution should maintain a comprehensive and easy to understand audit trail of read and write actions performed on the system • The solution should provide ability to extract data in desired formats for publishing and interfacing purposes • The solution should provide ability to attach documents and other artifacts to incidents and other entities • The solution is required to issue, log, track, manage and report on all activities underway during these modes of operation: • anticipation of incident • incident or crisis • recovery • incident simulation	
26.	Integration capabilities	This platform is expected to integrate various urban services devices at the street layer so that urban services applications can be developed on top of this platform independent of the technology that is used in the devices.	
27.		Integrate devices using their APIs in to this platform. For example, if the City wants to deploy Smart Parking solution, this platform should have the ability and provision to write adaptors which interface with the parking sensors or management software of the parking sensors to collect parking events, data and alerts and notifications from the devices and their software managers.	
28.		Platform should support on the fly deployment of Sensors. Platform shall have the ability to add / remove sensors including new vendor types without a need for shutdown.	

S.NO.	Functionality Description		Compliance (Yes/No)
29.	Edge Computing	• Provides standard edge appliance to connect industrial protocol devices, provides secure connection to cloud infrastructure, provides remote lifecycle management including software/firmware downloads and upgrades, provides remote management, self registration, and local administrative interface. • Provides edge appliance to abstract downstream industrial protocols and upstream internet protocols. • Edge appliance is provided in three form factors → Over the Pole, in street Cabinet and street appliances. Should be light weight with no moving parts and small in size. Should not need more than 1 Ghz of dual core CPU and 1 GB of memory to run with reasonable load. • Edge appliance provides software modules to interact with control systems and SCADA systems. • Smart City platform should be functionally complete on the edge, providing local processing of events, contextualization, transformation, analytics, decisions and controls. Business relevant events only passed to cloud. • Provides runtime load of new functions on the edge from the cloud. • Smart City platform should allow to set or change the behavior on the edge through policies, which could be defined through cloud instance of Smart City Platform. • Edge provides inline actions with analytics in same time window as SCADA functions. • Edge should learn the behavior as analyzing the data to create better decisions with time. Share the outcomes with the cloud to impact other edges. • Provide centralized Device Management from sensor to cloud. • Provide management tools to view, analyze, report on and modify the edge configurations. • Edges and cloud instances of platform should create a logical cluster to distribute the workload dynamically between the nodes, if	

S.NO.	Functionality Description		Compliance (Yes/No)
		and when applicable. (Need to check, if too strong of the requirements) • Edge software should not be dependent on sensors and devices or protocols. Same software blueprint should be deployed and running on all edges. Data and Configurations can be different from edge to edge.	
30.	Resiliency	• This architecture provides the smart city use cases much needed resiliency while adapting cloud architecture • Provides ways to define policies that make applications or things respond to external environments • Schedule actions to happen at future time points • The smart city platform should have integrations with the network layer to proactively monitor any incidents on the network for active troubleshooting and triaging • The Smart city platform should be able to alert any incidents in the network proactively on command and control center • The Smart City platform should have demonstrated integration to collaboration tools to bring multiple stake holders and responders to respond an emergency or an urban services event.	
31.	API Based Open Platform	• Provides urban services' API(s) to develop operation applications for each of the Urban Services domains. For example, the lighting operator of the City should be able to develop a City Lighting management application based on the API(s) provided by the platform. This lighting application should also have the ability to access data from other domains like environment based on the access control configured in the system. • The smart city platform should have API Management capabilities like API Security, API Metering, API Monetization • The smart city platform is should be able to provide API access based on roles and access control policies defined for each user and the key issued to that user	

S.NO.	Functionality Description		Compliance (Yes/No)
		• The vendor should have already documented different Urban Services APIs using which applications can be developed • The vendor should be able to demonstrate existing applications that are developed using these urabn services APIs	
32.		Enables the City and its partners to define a standard data model for each of the urban services domains (i.e. Parking, lighting, kiosks etc.…)	
33.		Enables City and/or its partners to write software adaptors based on the API(s) provided by device vendors and have the ability to control, monitor and collect the data from these street devices	
34.		Provides urban services API(s) to develop operation applications for each of the Urban Services domains. For example, the lighting operator of the City should be able to develop a City Lighting management application based on the API(s) provided by the platform. This lighting application should also have the ability to access data from other domains like environment based on the access control configured in the system.	
35.	Trending Service	System should provide trends in graphical representation from data sources over a period of time. Trends should allow to monitor and analyze device performance over time.	
36.	Policies and Events	System should allow policy creation to set of rules that control the behavior of infrastructure items. Each policy should a set of conditions that activate the behavior it provides. System should allow Default, Time-based, Event-based and Manual override polices creation. For example, an operator might enforce a "no parking zone" policy manually to facilitate road repairs.	
37.		System should provision to defines a set of conditions that can be used to trigger an event-based policy	
38.	Notifications, Alerts and Alarms	System should generate Notification, Alert and Alarm messages that should be visible within the Dashboard and the Enforcement Officer Mobile App if required.	

S.NO.	Functionality Description		Compliance (Yes/No)
39.		All system messages (notifications, alerts and alarms) should always visible from the Notifications view, which provides controls that operator can use to sort and filter the messages that it displays.	
40.		Systems should deliver message to a set of subscribers. The Notification service should support min two types of notification methods – Email notification and Short Messaging Service (SMS) notification.	
41.	Users and roles	Users access the perform various tasks, such as adding new locations, configuring new devices, managing adapters, and so on. However, not all users can perform all tasks. Each user should be associated with one or more roles and each role is assigned a certain set of permissions.	
42.		These roles and permissions define the tasks that a user can perform. Additionally, system should assign one or more locations to each role so that the user can perform tasks at the assigned locations only.	
43.		Roles and permissions define the tasks that a user can perform, such as adding users, viewing location details, exporting devices, generating reports, and so on. Each user should be associated with one or more roles and each role has an assigned set of permissions.	
44.		The platform should allow different roles to be created and assign those roles to different access control policies.	
45.		Since this platform is being used for managing Cities, the platform should also allow association of users and locations. For example, the platform should allow creation of locations in the system which correspond to various physical locations in the city and allow the admin to associate different users to different locations with the intent that each user can control only services for a location for which has been given access.	
46.		System should support LDAP to be used as an additional data store for user management and authentication.	

S.NO.	Functionality Description		Compliance (Yes/No)
47.	Service Catalog Management	The Service catalog management module should allow to categorize the externalized and non-externalized services into logical groups by creating the service catalogs. In addition, system should allow manage the service catalogs by adding, modifying, or deleting the catalog details.	
48.	Reports	The platform should have capability to provide access to real time data and historical data from various connected devices for reporting and analytics.	
49.		System should allow dashboard to generate reports and have provision to add reports in favorites list	
50.	Multi-tenancy	1. Single instance of SMART CITY PLATFORM can be logically partitioned to host multiple tenants. 2. Each tenant should have respective administrator users. 3. Role based access control: Allows to provision users with specific roles to delegate monitoring and management of city resources based on regions (sub-boundaries in the tenant/City geography). 4. Each Tenant (City) can be further partitioned (zones/streets etc) with access to users for the respective zones/streets.	
51.	Global Market Presence	Smart city suppliers should be adaptable to the emerging needs of cities. Suppliers should develop offerings that meet the growing interest in urban Internet of Things (IoT) applications, big data solutions, and the transformation in city approaches to energy policy, urban mobility, and city resilience.	
52.		The Smart City supplier should belong to league of registered organization	
53.	Standard Operating Procedure	Command & Control Center should provide for authoring and invoking un-limited number of configurable and customizable standard operating procedures through graphical, easy to use tooling interface.	
54.		Standard Operating Procedures should be established, approved sets of actions considered	

S.NO.	Functionality Description		Compliance (Yes/No)
		to be the best practices for responding to a situation or carrying out an operation.	
55.		The users should be able to edit the SOP, including adding, editing, or deleting the activities.	
56.		The users should be able to also add comments to or stop the SOP (prior to completion).	
57.		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.	
58.		The SOP Tool should have capability to define the following activity types: • Manual Activity - An activity that is done manually by the owner and provide details in the description field. • Automation Activity - An activity that initiates and tracks a particular work flow and select a predefined flow order from the list. • If-Then-Else Activity - A conditional activity that allows branching based on specific criteria. Either enter or select values for Then and Else. • 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. • SOP Activity - An activity that launches another standard operating procedure	
59.	Collaboration	• The CCC platform should provide an ability to bring multiple stake holders on to a common voice conference call as a standard operating procedure in response configured events • The stake holders can be on various types of devices like computer, smart phones, tablets or normal phones • The CCC platform should have the capability to bring in multiple stake holders automatically into a common collaboration platform like persistent chat	

S.NO.	Functionality Description		Compliance (Yes/No)
		rooms and virtual meeting rooms in response to a SOP defined to handle a particular event. • The operator should also have ability create these collaboration spaces like virtual meeting rooms or chat groups manually. • The platform should allow the stakeholders to be notified of the creation of collaboration spaces using SMSs and announcements over PSTN telephone calls. • The platform must allow configuration of the policy under which such collaboration spaces are created and stakeholders are invited and notified. • The platform should allow stakeholders to share content relevant to the issue in the collaboration space. This content may include text, pictures, video, PDF/DOC/DOCX documents etc. and stakeholders should be able to view the content directly from the collaboration space. • The platform should allow stakeholders to invoke a web conferencing session directly from the collaboration space. The web conferencing session should automatically include all stakeholders in the collaboration space. • The platform should allow stakeholders to participate in the web conferencing session using any means including smart phones, laptop computers, PSTN telephones, enterprise desk phones etc. • The platform should allow smart city devices (cameras, lights, various sensors etc.) to be added to the collaboration spaces. It should also allow the stakeholders to acquire data from such devices and to control such devices directly from the collaboration space, subject to access privileges for each user and device. • The platform should allow the stakeholders to access the collaboration	

S.NO.	Functionality Description		Compliance (Yes/No)
		spaces, participate in conversations, share content, create web conferences and control smart city devices from any endpoint (smart phones, laptops and other computers) and from any network location. • The platform should allow the stakeholders to be notified of the creation of collaboration spaces using SMSs and announcements over PSTN telephone calls. • The platform must allow configuration of the policy under which such collaboration spaces are created and stakeholders are invited and notified. • The platform should allow stakeholders to invoke a web conferencing session directly from the collaboration space. The web conferencing session should automatically include all stakeholders in the collaboration space. • The platform should allow stakeholders to participate in the web conferencing session using any means including smart phones, laptop computers, PSTN telephones, enterprise desk phones etc. • The platform should allow the stakeholders to access the collaboration spaces, participate in conversations, share content, create web conferences and control smart city devices from any endpoint (smart phones, laptops and other computers) and from any network location.	
60.	Enterprise resource planning (ERP) integration	System should allow integration of business process in ERP workflows like property tax collection etc.	
61.		System should allow ERP data visualization at city dashboard	
62.		The platform should have the capability to retrieve data directly from ERP systems. The	

S.NO.	Functionality Description		Compliance (Yes/No)
		APIs should be RESTful and return the data in JSON format.	
63.		The platform should also have the capability to read data directly from a set of databases (HBase, MongoDB, Oracle, Cassandra, MySQL, Impala). To connect to any of the databases information on how to connect should be provided.	
64.		System should be able to read data from flat CSV files.	
65.	Analytics Engine	Analytics Engine should be an artificial intelligence-based smart city analytics platform module to maximize business value through advanced machine learning capabilities. The machine learning capabilities aid in automating policies that result in better asset and infrastructure management.	
66.		The solution should be flexible to integrate with other city and government software applications.	
67.		Analytics Engine module should have below intelligence capabilities; a) Advanced Predictive Analytics should be part of the solution. b) The solution should be flexible to integrate with other city and government software applications c) The solution should be able to predict insights consuming data from city infrastructure viz., Traffic, Parking, Lighting etc. d) The solution should have predictions with measurable accuracy of at least > 70% e) The solution should be able to predict and integrate with Smart City solutions helping in driving operational policies creation. f) The solution should be robust, secure and scalable. g) The solution should have a visualization platform to view historic analytics	
68.		The application should enable the customers 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 application, system do the following tasks:	

S.NO.	Functionality Description		Compliance (Yes/No)
		a) Connect to a variety of data sources b) Analyze the result set c) Visualize the results d) Predict outcomes	
69.		Analytics Engine should support multiple Data Sources. Min below standard data sources should be supported from day 1 – CSV, TSV, MS Excel , NoSQL, RDBMS	
70.		Analytics Engine should provide analysis of data from a selected data source(s). Analysis enables to define arithmetic and aggregation operations that result in the desired output. Analytics engine should provide capability to check analysis with multiple predictive algorithms	
71.	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 party applications seamlessly	
72.	Export Formats	System should allow export the analysis into min following formats: g) XML/JSON h) Excel i) PDF j) CSV	

S.NO.	Functionality Description		Compliance (Yes/No)
73.	Cloud Infrastructure Operations	**Hardened components:** The OS instances are hardened as per the latest CIS-CAT benchmarks with target of 80 % compliance. All actions are audit-logged. Hardened OS shall have only required applications, process and permissions. All components are hardened as per industry standards	
74.		**Infrastructure components security:** Platform should support user encrypted storage volumes. Restrict inbound access from public network only on secure ports via DMZ proxy instances. SSH access is restricted with secure keypair and from designated jump hosts alone. User management and authentication is tied to Corporate SSO.	
75.		**VM Infrastructure security:** Platform should have appropriate technical controls in place to prevent attacks that target virtual infrastructure	
76.	Infrastructure as a Service support	System should provider should support following security features • User encrypted storage volumes. • Restrict inbound access from public network only on secure ports via DMZ proxy instances • SSH access is restricted with secure keypair and from designated jumphosts alone. • User management and authentication is tied to Corporate SSO. • Platform should have appropriate technical controls in place to prevent attacks that target virtual infrastructure • Platform should have appropriate controls in place to detect source code security defects, functionalities for any outsourced software development activities from suppliers, open source libraries	
77.	API & Interface Security	• The access to data should be highly secure and efficient.	
78.		• Access to the platform API(s) should be	

S.NO.	Functionality Description		Compliance (Yes/No)
		secured using API keys.	
79.		• Software should support security standards: OAuth 2.0, HTTPS over SSL, and key management help protect the data across all domains.	
80.		• Should support security features built for many of its components by using HTTPS, TLS for all its public facing API implementations. For deployment where CCC Software API(s) exposed to application eco system, API Management, API security features and API Key management functions are required.	
81.	Data Security & Integrity	• **Data Governance / RBAC:** Platform should support data governance & stewardship model, in which roles, responsibilities are clearly defined, assigned, implemented, documented and communicated • **Data Governance/ Resilient hosting:** Platform should have capability to restrict the storage of customer data to specific countries or geographic locations with resilient hosting options • **Data Protection / Production Data integrity:** Platform should support procedure in place to ensure production data shall not be replicated or used in non-production environment • **Data Protection / Data at rest:** Platform should support encryption for tenent data at rest (on disk/storage) • **Data Retention:** Platform should have capabilities to enforce tenent data retention policies • **Data recover & restore:** Platform should have capability to recover and restore data for a specific customer in the case of a failure or data loss. • **Data disclosure & privacy :** Platform should disclose data attributes, elements collected from source . All the attributes should be disclosed & appraised to data owner. With appropriate approval from City authority, Platform should have ability to	

S.NO.	Functionality Description		Compliance (Yes/No)
		encrypt sensitive data element at rest.	
82.	Release Operations	**Critical production assets:** Platform vendor should maintain complete inventory of critical production assets. Asset could be defined as source code, documents, binaries, configuration data, scripts, supplier agreements, SW Licenses	
83.		**Patch Management:** Platform should have capabilities to patch vulnerabilities across VM infrastructure, applications and systems	
84.		**Patch timeline / notifications:** Platform vendor should provide risk-based systems patching time frames to tenants based on request	
85.		**Secure SDLC:** Platform should support automated source code analysis tool to detect security anamolies / defects in code prior to production	
86.	Scaling, Capacity Provisioning parameters	• Platform should be scalable and should support capacity provisioning additional CPU, RAM to existing VM, Cloud infrastructure • Platform should have tools to monitors the healthiness of the individual tenants and status of CPU, Memory performance • The platform shall send alerts to the user once it exceeds certain limits in terms of CPU and Memory performance	
87.	Business Operations	**Audit & logging:** Platform should support centralized logging & auditing framework. Physical and logical user access to audit logs restricted to authorized personnel only.	
88.		**Legal / Supplier chain agreements:** Platform provider vendor should have policies and procedures established, and supporting business processes and technical measures implemented, for mainitaining complete, accurate and relevant agreeements (e.g. SLAs) between providers and customers	
89.		**Critical production assets:** Platform vendor should maintain complete inventory of critical production assets. Asset could be defined as	

S.NO.	Functionality Description		Compliance (Yes/No)
		source code, documents, binaries, configuration data, scripts, supplier agreements, SW Licenses	
90.		**Outsourced SW Development:** Platform should have appropriate controls in place to detect source code security defects, functionalities for any outsourced software development activities from suppliers, open source libraries	
91.	Field Responder Mobile Apps	Provide integrated Mobile Application for Android and Windows for capturing real-time information from the field response team using Mobile- Standard Operating Procedure.	
92.	High Availability	• Platform shall meet availability level of 95.0 % for testing & development environment • Platform shall meet availability level of 99.0 % for Production environment	
93.		Platform shall have no single point of failure. Software & hardware fault shall not result total system failure.	
94.		All failure must report relevant error messages to the user	
95.		Platform vendor shall provide supporting infrastructure, appropriate tools to measure & monitor system availability and automated notification for system failure and unavailability	
96.		System response Time Measured as the elapsed time between the moment a user initiates a process using input device to last display of first screen • System response time should not exceed 3 seconds for 2 concurrent users • System response time for any web services shall not exceed 3 seconds for 60 concurrent users	
97.	Logging	Platform should have logging frame with following functionalities • Logs shall readable in ASCII plaintext or UTF-8 format • All logs shall be timestamped • Log events shall capture user activities, applications, system & network IDPS	

S.NO.	Functionality Description		Compliance (Yes/No)
		messages • Centralized & secure log repositories to all log events • System logging shall be provided for all successful and unsuccessful login attempts and for all super user activities • Platform should implement mechanisms to trigger alerts and facilitate users to analyze and review logs efficiently • All critical logs are secured and sent to archive • Centralized logging shall be configurable to report for exceptions and generate reports based on desired filters • Logging framework shall be integrated with SIEM framework • Any anomalies shall be promptly identified & investigated through SIEM(Security Incident Management Framework) • Appropriate controls shall be put in place to ensure outage of the central log repository does not result in any loss of logs • The central syslog shall be able to normalize logs from wide variety of platforms / components to Common Event Format (CEF) to ease of use for monitoring and analysis and support logical data segregation so that the different user groups can only view their own managed equipment logs • Central syslog system shall have sufficient disk storage to keep the logs for 1 year to facilitate incident response investigation • Logging should have following retrieval time o Timeline : Log Duration o 6 Hrs : 0 – 30 days o 1 day : 30 – 90 days o 5 days : Older than 90 days	

S.NO.	Functionality Description		Compliance (Yes/No)
98.	Performance Monitoring Tool	Performance monitoring tool shall include following functionalities • Identify infra and/or application components between the user and backend servers that is causing the problems • Providing key performance indicators • Identify the inter-dependencies between application & infra components • Able to provide network/ system node causing the problem • Provide email, SMS and/or mobile alert mechanism if performances falls below predefined thresholds • Performance monitoring shall not adversely affect the performance of the platform	
99.	Database monitoring	• Platform should provide database monitoring tool for DB health checks to monitor o Memory allocation, usage and contention o Disk I/O usage o CPU usage for a particular transition o Number of buffers, buffer size and usage o Active locks and locks contention, including waiting time o Active users and status of their operations o List of users (complete or selected) with their access rights	
100.	Platform Environment	• Platform provider shall have 3 environments 1. Development environment 2. QA environment 3. Production environment • All 3 environments shall be physically / logically separated • All should have same system & application software versions	

S.NO.	Functionality Description		Compliance (Yes/No)
101.	Platform Software	• Platform provider shall provide complete information on all platform software deployed indicating clearly the software versions, quantity of licenses, functions, type of license (one time or annual recurring) • Platform provider shall transfer all licenses with maintenance service supports to authority • There shall be no use of freeware, shareware and proprietary software	
102.	Backup and Recovery	• Platform backup and recovery solution functionality shall meet following requirements o Perform online database backup and recovery o Support full, incremental, scheduled and on-demand backups o Provide additional programs and utilities for the purpose of backup and recovery and administration o Perform backup verification to ensure integrity of backup o Perform automatic drive cleaning using pre-mounted cleaning tape o Support the backup of all files including open files within servers including operating systems, database o Be carefully administered and monitored o Provide comprehensive reporting and analysis functions	
103.	Archival and Retrieval	• Platform vendor shall propose a detailed housekeeping and archival strategy that meet the Authority's housekeeping policy and business requirements • The strategy shall enable the Authority to access historical data on an ad hoc basis for audit, verification and investigation purposes • Ease of restoration of archived data from online achieves or offline storage and it	

S.NO.	Functionality Description		Compliance (Yes/No)
		shall be able to keep track of all archival activities performed • Overall platform performance shall not be compromised during the archival process	
104.	Documentation	• All application software developed shall be properly documented with header indicating title, author, date of creation/update, update description, abstract of program/ module, interfaces, description of variables and data structures • Platform provider shall maintain traceability matrices for all requirements, system design and testing. • The traceability matrices shall trace all requirements throughout all stages of development life-cycle • Full documentation and source codes of all the software programs, modules, algorithms, software engines, link interfaces, GUI that are designed, developed and/or customized by the contractor for the Platform shall be submitted to Customer	

1.3 Backup / Achieved / Replication Software

Backup Solution

#	Description
1.	The proposed backup solution shall have same GUI across heterogeneous platform to ensure easy administration and available on various OS platforms such as Windows, Linux and UNIX platforms and be capable of supporting backup/ restores from various supported platforms.
2.	Backup Solution should have ability to backup data from one server platform and restore it to another server platform to eliminate dependence on a particular machine and for disaster recovery purposes.
3.	Backup Solution should support various level of backups including full, incremental, and user driven backup along with various retention period.
4.	Backup clients should be updated automatically using the client push feature
5.	Backup should support agentless backup for virtualization platform with non-staged granular recovery.
6.	Backup Software should support intelligent policy for virtualization.

7.	Backup Software must provide Source (Client & Media Server) & Target base data Deduplication capabilities.
8.	Backup Solution should Integrate with third party VTL, NAS, SAN which has data deduplication capabilities
9.	Backup Solution must have Wizard-driven configuration and modifications for backup, restoration and devices.
10.	The proposed backup solution shall have in-built frequency and calendar based scheduling system.
11.	Backup Solution must have Optimized way for data movement from client to disk target.
12.	Backup Solution should support (inflight & at rest) encryption.
13.	The proposed backup solution shall support tape mirroring of the same job running concurrently with primary backup.
14.	The proposed backup solution shall allow creating tape clone facility after the backup process.
15.	Backup Solution should have Capability to do trend analysis for capacity planning of backup environment.
16.	The proposed Backup Solution must offer capacity-based licensing. The license should be for the front-end capacity rather than back-end. There should be no incremental cost associated with longer retention periods.
17.	The solution should not require purchase of additional licenses for DR sites (copies of original data), also should not require purchase of additional licenses for replication to DR sites.
18.	The proposed backup dedupe license should be independent of hardware so replacing hardware should not incur new software license cost.
19	The proposed backup solution must include Agent/Modules for online backup of files, applications and databases such as MS SQL, Oracle, DB2, Sybase, Exchange, Sharepoint and File share backup(SMB)
20	The proposed backup solution should provide recovery from physical servers to Virtual and image level recovery.
21	The proposed backup solution should have Cloud plug-ins for backup data replication.
22	Backup Solution should have Inbuilt feature for extensive alerting and reporting with pre-configured and customizable formats.
23	Backup Replication at DR site, Cloud. Replication license should be included as part of solutions.
24	Backup software should support multiplexing and multistreaming and shall support the capability to write up to Min 32 data streams.
25	Backup Solutions should have capabilities to disk out backup catalog and deduplication catalog.
26	Backup solution should have integrated data de-duplication engine with multi-vendor storage support to save de-duplication data. The de-duplication engine should also facilitate IP base replication of de-dupe data; without any extra charge.
27	The Proposed Backup solution must restore files, emails and other granular items from Microsoft Exchange, SharePoint, and Active Directory and for hypervisors such as VMware and Microsoft Hyper-V from a single-pass backup.
28	Backup solution must Support Backups/Restores for 1) Clustered servers (Industry popular clusters). 2) Virtual platform. 3) RAW SCSI volumes. 4) Block based backup & restore simultaneously.

Archival Solution

#	Description
1.	The solution must be capable of archiving content from multiple sources like messaging including MS Exchange, Domino File Servers , MS Sharepoint, VOIP etc

2.	The proposed solution must have integration with Email solution through SMTP archiving without the need of any additional hardware.
3.	The solution should have the capability to archive data from multiple electronic repository to single repository to achieve best single instance across multiple frontend source data.
4.	The solution must support a Single unified console to manage archiving from different sources like File server, sharepoint, Mailing solution etc
5.	The solution should provision a web based discovery mechanism to search relevant data across archives from multiple sources like file server, messaging, Sharepoint etc. The discovery mechanism should support a guided, hierarchal review of searched data with capability to filter, marking and legal hold to prevent deletion/expiry.
6.	The solution should facilitate a supervision mechanism for emails to ensure compliance of messaging content. The supervision mechanism should facilitate sampling of messages and subsequent review by authorized personnel
7.	The solution should support tagging of messages by message security solutions like anti-spam/anti-virus for efficient retention
8.	Proposed solution must support outlook on Windows & MAC machines.
9.	Archival solution must have support with IMAP compliant devices to access the emails.
10.	Proposed solution should support archiving both at premises and cloud.
11.	Proposed solution must have monitoring integration with messaging solution vendor.
12.	The solution should support Message Journaling as well as Envelope Journaling, capture BCC data and expansion of distribution lists
13.	The solution must support "Agentless" archiving of messages. There should be no need to deploy any agent on the messaging server.
14.	The solution must support search for mails based on undisclosed recipients criteria
15.	The solution should support seamless access using shortcuts from the native email client as well as browser based client. The solution should support all archiving actions like manually archive, search, restore, retrieve, delete from the native email client and browser based client
16.	The solution should support archiving based on either any or a combination of the following criteria: - Item Type (message, calendar etc.) - Date - Size - Email Attachment only - User - Organizational Unit
17.	Proposed solution must have advance way of archive disk/partition data backup to avoid backup of old partitions which must be possible with or without WORM devices.
18.	The solution must allow the administrators to configure the following in shortcuts: - Include recipient information in the shortcuts. - Include nothing / original message body / custom message body in shortcuts. - Include "X" number of characters in the shortcut. - Include a custom body defined from a configuration file in the shortcut etc.
19	The solution should leave a shortcut at either the time of archiving or later as well.
20	The solution should allow users to view archived items directly without having the need to restore them to the messaging server to avoid delays and impact on messaging solution. No network connections should be established between archiving server and messaging server at the time of retrieving archived items
21	The solution must support indexing and archiving of minimum 500+ commonly used file types.
22	The solution should support archiving of entire email folders and application of selective archiving policies based upon folders.

23	The solution must support dynamic retention period of archived items i.e. retention of archived items can be increased or decreased on fly.
24	The solution should facilitate "future proofing" of content by facilitating an HTML copy for long term retention and search
25	The solution should support "safety copies" of items to be kept on the mail server. The "safety copy" allows the archiving software to wait for the archived item to be backed up or replicated before the original item is removed from the mail server.
26	Archival solution must have option to set or configure disk property read and read-write access
27	Archival solution must have disk configurable option with High & Low watermark. In case, High watermark reaches, disk should automatically become Read only and other pre-configured disk should get read-write access to store fresh archived items.
28	The solution must have OWA integration in such a fashion that archived item can be browsed directly through archived browser tab instead of browsing through internet explorer (IE). IE can be additional feature.
29	The archival solution must have an integrated e-discovery solution which allows guided Discovery, review and analysis of data from the archives and non-archived data like desktop, sharepoint, file server, Documentum etc. It's required for future proofing.
30	Proposed Archival solution must have seamless and consistent end user search experience across multiple interface like Desktop/Laptop, mobile, tablets etc.

Replication Solution

#	Description
1	The proposed architecture should ensure that in event of Disaster at Primary Site, applications can be restarted at DR Site without any data loss.
2	The proposed architecture should focus on not only the data replication, but ensuring application availability with zero data loss at DR site.
3	The proposed solution must optimize additional infrastructure and storage resources in the architecture.
4	The proposed solution should be a storage agnostic solution. The solution should not only seamlessly integrate with current infrastructure, but also not impose any restriction on storage or platform technology that BSCDCL may deploy in future.
5	The proposed software must provide comprehensive hardware and platform support. Support for physical and virtual platforms, including Solaris, AIX, HP-UX, Linux, Windows, VMware, and KVM.
6	The proposed software should provide application level availability by ensuring that it not only replicates data within database but also structural changes to databases, application and database binaries etc. without any manual intervention.
7	Application high availability at primary & DR site should not be dependent on Operating system event logs. Solution should be capable to integrate directly with application start, stop and monitor service to avoid outage remedy solution because of Operating system log.
8	The proposed software should support real time tracking of configuration changes being done to Operating system, application binaries, any tunable added/modified etc. and alert administrators in case of configuration drift between primary and DR site.
9	Shall be able to handle long outages of network without affecting the consistency of data at secondary site. The replication solution should be provisioned for storing data for at least 4 days in case network is down for extended period.
10	The proposed software should provide for an automated fire-drill for testing of DR site. The testing mechanism should automatically validate the application startup at DR site at a pre-defined schedule defined.
11	The proposed software should provide availability across any distance—Builds local metropolitan and wide-area clusters for disaster recovery and local availability.

12	The proposed software should ensure no single point of failure. It has the ability to gracefully move an application to an available server in the event of a failure and coordinate the movement with storage ownership.
13	The proposed software should provide Multi-cluster management and reporting, including applications composed of multiple components running on different physical and virtual tiers, adding resilience to business services. Manages and reports on multiple local and remote clusters from a single unified web-based console.
14	The proposed software should provide seamless integration with Oracle, Exchange, SQL, SharePoint, and major applications/databases for increased application performance and availability.
15	It should also have the integration with replication technologies such as EMC SRDF/Mirrorview, Hitachi TrueCopy, IBM MetroMirror, Oracle DataGuard, Veritas Replicator, etc.
16	The proposed software should provide advanced application failover logic to ensure that application uptime is maximized, server resources are efficiently utilized, and detect failures faster than traditional clustering solutions and requires almost no CPU overhead
17	The proposed software should provide advanced clustering support for virtual machine architectures.
18	The proposed software should be simple to install, configure, and maintain. It should provide powerful wizards that enable simple, quick, and error-free setup of advanced, high availability, disaster recovery, and Fire Drill configurations.
19	The proposed software must be able to provide comprehensive insight into the storage environment, enabling improved usage and efficiency across all major operating systems, including Oracle Solaris, HP-UX, IBM AIX, Red Hat Enterprise Linux, SUSE Linux, Oracle Enterprise Linux (RHEL compatible mode), and Microsoft Windows, and storage hardware, including EMC, HDS, IBM, NetApp, HP, Dell Compellant, and more.
20	The proposed software should have deduplication and compression to reduce the primary storage footprint.
21	The proposed software should support automated storage tiering to seamlessly and transparently move data based on business value
22	The proposed software should have the ability to make data compatible between operating systems for simplified OS migration.
23	The proposed software should be able to support physical environment. It should support virtual disks in VMDK/VMFS format, and as well as RDM.
24	The proposed solution should have multi-pathing feature for I/O path availability and performance to efficiently spread I/Os across multiple paths for maximum performance, path failure protection, and fast failover.
25	Host Replication should be certified for performing replication to heterogeneous storage models from different OEMs (HP, IBM, EMC, SUN and Netapp)
26	The Host Replication technology should support different types of data whether structured or unstructured.
27	The proposed host base replication solution should be capable of maintaining data consistency at all times.

1.4 EMS (Enterprise Monitoring 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 specified users (minimum 10 users) of City SPV.

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 BSCDCL in data driven decision making. In case the MSI uses any OEM product(s), the implementation should be as per best practices of the OEM. City SPV may engage STQC/other independent auditors for validating the deployment of EMS facilities as per RFP requirements, specially their capabilities for measuring

and reporting SLAs & KPIs as defined in RFP. The entire EMS implementation shall be certified by the MSI also for its correctness, adequacy to meet RFP requirements and measurement of SLAs & KPIs etc. Various key components of the EMS are:

- SLA & Contract management System
- Network Monitoring System
- Server Monitoring System
- Helpdesk System
- Application Performance Management

Proposed EMS Solution shall be based on industry standard best practice framework such as ITIL etc.

1.4.1 SLA & Contract management System

The SLA & Contract Management solution should enable the City SPVs 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 ICCC 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 -

- It must be a centralized monitoring solution for all IT assets (including servers, network equipment etc.)
- The solution must have integrated dashboard providing view of non performing components / issues with related to service on any active components
- The solution must follow governance, compliance and content validations to improve standardisation of service level contracts
- Application should be pre-configured so as to allow the users to generate timely reports on the SLAs on various parameters.
- The solution must support Service Level Agreements & Lifecycle Management including Version Control, Status Control, Effectively and audit Trail to ensure accountability for the project.
- The solution must have the ability to define and calculate key performance indicators from an End to End Business Service delivery perspective related to ICCC Project under discussion.
- The solution should support requirements of the auditors requiring technical audit of the whole system which MSI should allow the auditors to access the system.
- The solution most have an integrated dashboard, view of Contract Parties & current SLA delivery levels and view of Services & current SLA performance
- The solution should support SLA Alerts escalation and approval process.

- Solution should support effective root-cause analysis, support capabilities for investigating the root causes of failed service levels and must make it possible to find the underlying events that cause the service level contract to fail.

- Accept Data from a variety of formats.

- Support for Defining and Calculating service Credit and Penalty based on clauses in SLAs.

1.4.2 Reporting

- Ability to generate reports on penalty and credit due, to check on non-compliance of SLAs for the CCDCSC and each city ICCC.

- 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.

- The solution should provide 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 Microsoft Word, Adobe PDF etc.

- The solution must support Templates for report generation, Report Filtering and Consolidation and Context sensitive Drill-down on specific report data to drive standardisation and governance of the CCDCSC and each city ICCC

- The solution must support security for drill-down capabilities in dashboard reports ensuring visibility for only relevant personnel of the CCDCSC and each city ICCC.

- Support real-time reports (like at-a-glance status) as well as historical analysis reports (like Trend, Capacity planning reports etc.)

    - Resource utilisation exceeding or below customer-defined limits

    - Resource utilisation exceeding or below predefined threshold limits

An indicative List of SLAs that need to be measured centrally by SLA contract management system are given in the Tender Document. These SLAs must be represented using appropriate customisable reports to ensure overall service delivery.

- The ICCC should allow users to define benchmarks against performance parameters. Performance reports shall have the option to generate reports with or without benchmark comparison.

- The ICCC should provide facility to trigger a corrective action workflow and define the stakeholders for the same.

- The platform should have tightly integrated Asset Management System to have all the relevant information of all assets in Smart City Area of respective cities to give real time status of assets and update automatically in case of failure. It should also be possible to have procurement plan of similar product in past, check inventory & issue work order accordingly.

- The ICCC platform should include a broad range of device integration servers for establishing the I/O interface to filed devices such as RTU's, PLCs and DCS systems.

- The ICCC platform software provided shall consist of a human machine interface (HMI) system with support for supervisory and process control, real time data acquisition, alarm and event management, historical data collection, report generation, local or remote telemetry communications to PLCs/RTUs and internet / internet access.

1.4.3 Network Management System

- The Solution should provide capability to monitor any device based on SNMP v1, v2c & 3
- The Solution should monitor bandwidth utilization.
- The solution should monitor utilization based on bandwidth.
- The Solution must be capable of monitoring the availability, health, and performance of core networking devices including but not limited to CPU, memory, temperature.
- The Solution should have the ability to issues pings to check on availability of ports, devices.
- The Ping Monitoring should also support collection of packet loss, Latency and Jitters during ICMP Ping Checks
- The Port Check for IP Services monitoring should also provide mechanism to define new services and ability to send custom commands during port check mechanism.
- The Solution should have the ability to receive SNMP traps and syslog.
- The Solution should automatically collect and store historical data so users can view and understand network performance trends.
- The solution should be capable of monitoring network delay/latency.
- The solution should be capable of monitoring delay variation
- The solution should be capable of monitoring packet loss, Packet QOS, Packet Errors on one or more ports
- The solution should allow users to access network availability and performance reports via the web or have those delivered via e-mail.
- The solution should support auto-discovery of network devices
- The solution should have the ability to schedule regular rediscovery of subnets.
- The solution should provide the ability to visually represent LAN/WAN links) with displays of related real-time performance data including utilizations.
- The system should provide discovery of heterogeneous physical network devices like Layer-2 & Layer-3 switches, Routers and other IP devices and do mapping of LAN & WAN connectivity.
- The solution should provide capability to mask the default port speed for accurate % port utilization reporting
- The System shall support monitoring of Syslog

- The solution should provide capability to add an IP device or IP Range or IP subnet with functionality supporting multiple SNMP strings.
- The solution should provide capability to add devices from word or excel file by drag and drop functionality and auto configure based on pre-defined settings.
- The solution should allow easy configuration of polling frequency till per minimum 30 second scenario.
- The solutions should have real time, detect configuration and asset information changes made across a multi-vendor device network, regardless of how each change is made and also support configuration deployment/rollback and configuration templates.

1.4.4 Server Performance Monitoring System

- The proposed tool should integrate with network performance management system and support operating system monitoring for various platforms supplied as part of the Surveillance Project.
- The proposed tool must provide information about availability and performance for target server nodes.
- The proposed tool should be able to monitor various operating system parameters such as processors, memory, files, processes, file systems, etc. where applicable.
- The solution should provide a unified web based console, which consolidates all aspects of role based access under a single console.
- Proposed Network Management 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.

1.4.5 City ICCC Helpdesk System

- The proposed helpdesk solution must provide flexibility of logging, viewing, updating and closing incident manually via web interface for issues related to surveillance project.
- 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.
- 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.
- Centralized Helpdesk System should have integration with Network/Server Monitoring Systems so that the Helpdesk Operators can to associate alarms with Service Desk tickets to help surveillance operators that for what particular alarms corresponding helpdesk tickets got logged.
- Surveillance Network admin should be able to manually create tickets through Fault Management GUI.
- System should also automatically create tickets based on alarm type

System should provide a link to directly launch a Service Desk view of a particular ticket created by alarm from within the Network Operation console.

Centralized helpdesk for DC and DR is defined in cloud specifications.

1.4.6 Application Performance Management

- The solution should measure the end users' experiences based on transactions without the need to install agents on user desktops
- The solution must be able to provide user usage analysis and show how user's success rate, average time and transaction count has changed over a specific period of time such as current week versus previous week.
- The solution must be able to provide the ability to detect and alert when users experience HTTP error codes such as 404 errors or errors coming from the web application.
- Solution shall be able to monitor customer transaction by end-user name, and thus able to understand exactly which customers were impacted, their location, type of browser used etc.
- The solution must simplify complex app topologies through task–relevant views based on attributes such as location, business unit, application component etc.
- The solution must speed up the process of triage by showing the impact of change, thus enabling to easily locate where performance problems originate.
- The solution should provide the flexibility of collecting deep-dive diagnostics data for the transactions that matter for triage as opposed to collecting deep-dive data for every transaction.
- The solution must proactively monitor 100% of real user transactions; detect failed transactions; gather evidence necessary for triage and diagnosis of problems that affect user experiences and prevent completion of critical business processes.
- The solution must determine if the root cause of performance issues is inside the monitored application, in connected back-end systems or at the network layer from a single console view.
- The solution must provide proactive real-time insights into real user behaviour, trends, log analytics and performance to enhance customer experience across various channels
- The solution must provide rapid analysis where crash analytics and video session playback allows for rapid analysis and repair to deliver seamless user interactions
- The solution must provide operational efficiency capabilities that provide insight of app performance by version, carrier, geo, OS, network, real-time alerts on threshold violations impacting SLAs and prioritize alerts based on impact to business, revenue and gain end-to-end visibility into the mobile infrastructure.
- The solution must provide complete Insights into Application Flows, Heat Maps & Crash to enable improving the UI design, understand user interactions, build functionality based on real user data and create product & services differentiation.

1.5 Software Defined Security (SDS) for Applications /Services

#	Parameter and Minimum Specifications
1	The Proposed solution should have the ability to provide native application isolation and on-demand creation of security groups based on existing security policies.
2	The proposed Solution Architecture should Firewall any inter VM communication / Traffic. This Inter VM Firewalling within the same VLAN / Application Tier should not burden the Intranet Firewall but should be done closer to the Application inside the Host.
3	The proposed Firewall should be in Software Form factor and can be either present in the Virtualization/ Hypervisor layer or as a Virtual Machine in every Physical Host as agentless mode. It should preferably offer throughput of over 10Gbps Per Physical Host/Server/Blade.
4	The proposed solution should get managed from a centralized console and should be integrated with the Centralized Virtualization console for an easy and common Operational mode with that of the Virtual Machine.
5	Automated Security Policy Management - The Security Policy should be tied with each Virtual Machine and the Policy should automatically move with the movement of the Virtual Machine, thus bring Security Policy Portability along with the VM motion.
6	The solution shall provide inspection firewall that can be applied at the virtual network interface card level directly in front of specific workloads thus creating capability of Application isolation for Risk/Breach containment.
7	The solution should offer to Integrate with industry-leading solutions for antivirus, malware, intrusion prevention, and next-gen security services through Security Service Chaining
8	The solution should have the capability of creating unique Security Groups of the VMs based on Operating Systems, Workload Type (Web, App or DB), Machine Name, Services running, Regulatory requirement etc. and apply Automated and Centralized Security Policy based on this context or grouping.

1.6 Virtualization Software

#	Parameter	Minimum Specification
1.	Solution	Sits directly on the server hardware with no dependence on a general purpose OS for greater reliability and security.
2.	Guest OS Support	Windows client, Windows Server, Linux (at least Red Hat, SUSE, Ubuntu and CentOS, Solaris x86) etc.
3.	VM Capability	Create Virtual machines with up to 128 virtual processors, 6 TB virtual RAM and 2GB Video memory in virtual machines for all the guest operating system supported by the hypervisor.
4.	VM Live Migration	Live Virtual Machine migration between different generations of CPUs in the same cluster and without the need for shared storage option and between servers in a cluster, across clusters as well as long distances from one site to another (up to 150 milliseconds round trip time) with no disruption to users or loss of services, eliminating the need to schedule application downtime or business downtime.
5.	Storage Live Migration	Live migration of VM disk from one storage array to another without any VM downtime. Support this migration from one storage protocol to another eg: FC, NFS, iSCSI, DAS.
6.	High Availability	Proactive High availability capability that utilizes server health information and migrates VMs from degraded hosts before problem occurs.
7.	Always Available	Zero downtime, Zero data loss and continuous availability for the applications running in virtual machines in the event of physical host failure, without the cost and complexity of traditional hardware or software clustering solutions.
8.	Resource Addition	Add CPU, Memory & devices to virtual machines on the fly when needed, without disruption or downtime of working VMs for both windows and Linux based VMs.
9.	Resource Scheduler	Dynamically allocate and balance computing capacity across collections of hardware resources aggregated into one unified resource pool with optional control over movement of virtual machines like restricting VMs to run on selected physical hosts. Create a cluster out of multiple storage data stores and automate load balancing by using storage characteristics to determine the best place for a virtual machine's data to reside, both when it is created and when it is used over time.
10.	Security	VM-level encryption with no modifications in guest OS to protects unauthorized data access both at-rest and in-motion and also provides secure boot for protection for both the hypervisor and guest operating system by ensuring images have not been tampered with and preventing loading of unauthorized components. Integration of 3rd party endpoint security to secure the virtual machines with offloaded Firewall and HIPS solutions without the need for agents inside the virtual machines from day 1.

11.	Storage support	Support boot from iSCSI, FCoE, and Fiber Channel SAN. Integrate with NAS, FC, FCoE and iSCSI SAN and infrastructure from leading vendors leveraging high performance shared storage to centralize virtual machine file storage for greater manageability, flexibility and availability. Virtual Volumes which enables abstraction for external storage (SAN and NAS) devices making them Virtualization aware. Integration with Storage API's providing integration with supported third-party data protection, multi-pathing and disk array solutions.
12.	Virtual Switch	Span across a virtual datacenter and multiple hosts should be able to connect to it. This will simplify and enhance virtual-machine networking in virtualized environments and enables those environments to use third-party distributed virtual switches. In-built enhanced host-level packet capture tool which will provide functionalities like SPAN, RSPAN, ERSPAN and will capture traffic at uplink, virtual switch port and virtual NIC level. It should also be able to capture dropped packets and trace the path of a packet with time stamp details. “Latency Sensitivity” setting in a VM that can be tuned to help reduce virtual machine latency. Link aggregation feature in the virtual switch which will provide choice in hashing algorithms on which link aggregation in decided and this should also provide multiple link aggregation groups to be provided in a single host.
13.	VM based Replication	Efficient array-agnostic replication of virtual machine data over the LAN or WAN. This Replication should simplify management enabling replication at the virtual machine level and enabling RPOs as low as 15 minutes.
14.	VM Backup	Simple and cost effective backup and recovery for virtual machines which should allow admins to back up virtual machine data to disk without the need of agents and this backup solution should have built-in variable length de-duplication capability.
15.	I/O Control	Prioritize storage access by continuously monitoring I/O load of storage volume and dynamically allocate available I/O resources to virtual machines according to needs. Prioritize network access by continuously monitoring I/O load over network and dynamically allocate available I/O resources to virtual machines according to needs.
16.	OEM Support	Direct OEM 24x7x365 days with unlimited incident support and 30mins or less response time including the unlimited upgrades and updates.

2. Annexure 2-Technical Specifications

Technical Specification provided under are indicative, bidder carefully examine the requirements and may propose technical specification / design as per their solution to meet the objective of RFP. Below are minimum technical requirements, to be considered for this project. Bidder is free to offer better product with more functionalities.

2.1 Multi-Function Laser Printer

#	Parameter	Minimum Specifications
1.	Technology	Laser
2.	Monthly duty cycle/RMPV (pages)	200,000/5K-20K
3.	Print speed – simplex (A4)	Up to 41 ppm
4.	Scan speed – Black/Color simplex	Up to 50/30 ipm
5.	Scan speed – Black/Color duplex	Up to19/14 ipm
6.	Scan-to destinations	Email, Network folder, USB
7.	Processor (MHz)	600
8.	Memory (MB)	1,024
9.	Hard disk drive (HDD)/Capacity (GB)	Yes/240
10.	Connectivity	2 Hi-Speed USB 2.0; 1 Gigabit Ethernet 10/100/1000T network
11.	Print resolution – Max/Best print quality (dpi)	Up to 1200x1200
12.	Input capacity – Std/Max (sheets)	600/4,600
13.	Output size – Min/ Max (mm)	76.2 x127/312x469.9
14.	Automatic duplex	Yes
15.	Energy Efficiency	BEE or Energy Star certified
16.	Control panel display	21 m touchscreen

2.2 Laser Printer

#	Parameter	Minimum Specifications
1.	Print speed black (normal, A4)	Up to 25 ppm
2.	Print quality black (best):	Up to 1200 x 1200 dpi
3.	Print technology :	Monochrome Laser
4.	Duty cycle (monthly, A4)	Up to 15,000 pages
5.	Recommended monthly page	volume 250 to 2000
6.	Standard memory:	Minimum 128 MB
7.	Processor speed:	Minimum 700 MHz
8.	Paper handling standard/input	Up to 250-sheet input tray

#	Parameter	Minimum Specifications
9.	Paper handling standard/output	Up to 150-sheet output bin
10.	Media sizes supported	A4, A5, A6, B5, postcard
11.	Media types supported	Paper, transparencies, postcards, envelopes, labels
12.	Standard connectivity	Hi-Speed USB 2.0 port with USB data cable, Ethernet with RJ45 connectivity
13.	Duplex printing	Automatic (standard)
14.	Compatible operating systems	Microsoft Windows 7 Professional(64bit), Windows 8 Pro(64 bit), Windows 8.1, Windows 10, Server 2008 R2, Server 2012 R2, MAC OS 9.0, MAC OS X, Linux
15.	Power requirements:	Input voltage 220 to 240 VAC (+/- 10%), 50 Hz (+/- 2 Hz);
16.	Power consumption during printing	Less than 500W
17.	Energy Efficiency	BEE or Energy Star certified
18.	Front operating Panel	Graphical LCD display

b. Video Wall

The minimal specifications of video wall cubes are as below -

- Video wall: 70" inches diagonal, 6X3 arrangement, Laser illumination based
- The native resolution of each Visual Display Unit / Rear Projection Module should be 1920 X 1080 pixels (Full HD) and should offer min 16.7 million colors.
- The Light source lifetime of 70" DLP Laser lit cubes should be >80,000 hrs. The brightness uniformity should be > 95%.
- The contrast shall be 1500:1 or higher.
- The Aspect Ratio of each of projection module should be 16:9.
- The screen should have front accessibility and adjustable low inter screen gap < 1 mm to give seamless viewing experience.
- Video Wall Controller:
    - Should be based on server architecture, operating system should be windows 7 or higher, 64 bit
    - RAM 16GB, HDD 500 GB, Dual redundant power supply,
    - 24 DP/ DVI outputs to the cube
    - 6 DVI Input , Dual LAN
    - 19 Inch rack mountable
    - Capable to display image from UNIX, LINUX system
    - Software should be provided to manage video wall content

c. Workstations (Desktop Computer)

#	Parameter	Minimum Specifications
1.	Processor	Latest generation 64bit X86 Quad core processor(3Ghz) or better
2.	Chipset	Latest series 64bit Chipset

#	Parameter	Minimum Specifications
3.	Motherboard	OEM Motherboard
4.	RAM	Minimum 8 GB DDR3 Memory @ 1600 Mhz. Slots should be free for future upgrade
5.	Graphics card	Minimum Graphics card with 2 GB video memory (non-shared)
6.	HDD	2 TB SATA-3 Hard drive @7200 rpm
7.	Media Drive	NO CD / DVD Drive
8.	Network interface	10/100/1000 Mbps autosensing on board integrated RJ-45 Ethernet port.
9.	Audio	Line/Mic IN, Line-out/Spr Out (3.5 mm)
10.	Ports	Minimum 6 USB ports (out of that 2 in front)
11.	Keyboard	104 keys minimum OEM keyboard
12.	Mouse	2 button optical scroll mouse (USB)
13.	Monitor	Min. 22" (*or 21.5"*) TFT LED monitor, Minimum 1920 x1080 resolution, 5 ms or better response time, TCO 05 (or higher) certified For Command Control Centers : 2 LED Monitors *attached to the same workstation (multi monitor)*
14.	Certification	Energy star 5.0/BEE star certified
15.	Operating System	64 bit pre-loaded OS with recovery disc
16.	Security	BIOS controlled electro-mechanical internal chassis lock for the system.
17.	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)
18.	Power supply	SMPS;. Power supply should be 90% efficient with EPEAT Gold certification for the system.

d. Television Set (Meeting room)

- 46 Inch Full HD LED

e. Projector

#	Item	Minimum Specifications
1.	Display Technology	Poly-silicon TFT LCD
2.	Resolution	HD 1080p
3.	Colours	16.7 million Colours
4.	Brightness	2500 or more ANSI lumens (in Normal Mode)

5.	Contrast Ratio	2000:1 or more
6.	Video Input	One computer (D-Sub, Standard 15 pin VGA connector) One S-Video One HDMI
7.	Audio	Internal speaker
8.	Output ports	External Computer Monitor port, audio ports
9.	Remote Operations	Full function Infrared Remote Control
10.	Other features	Auto source detect, Auto-synchronisation, Keystone Correction

f. IP PABX System

#	Description	Parameter
1.	Technology	PCM-TDM , IP, Non-blocking
2.	Interface	Should support all telecom interfaces in Indian Telecom Service provider offerings
3.	Type of Interface	ISDN interface for digital, basic interface for Analog lines
4.	No. of lines - ,ISDN PRI lines & Analog / Digital Extensions	1 PRI from BSNL, 32 Extensions (IP / Analog / Digital)
5.	Type of Extension Support	Analog , Digital and IP
6.	Expansion of Extensions	Multiples of 8 / 16
7.	Run Distance	Not less than 800 mtrs. on 0.5mm dia. Cable
8.	Max. Loop resistance for analog trunk lines Extensions	2500 ohms including telephone
9.	Requirement at the time of supply	01 ISDN PRI, 24 Analog Ports & 8 Digital extension ports.. Expected to handle at least 30 external lines.
10.	Contact center Expansion available (Max. capacity)	It must support at least 16 Call center Agents
11.	Max. loop resistance for analog trunk lines	1200 ohms at –48 Volts DC

#	Description	Parameter
12.	Other	• ISDN supplementary services for Digital phone • Support for digital trunk lines • Working on 230v AC mains and DC voltage • Support for ACD call center with CTI and advanced call routing
13.	Design of EPABX System	Modular with universal slots, wall mountable
14.	Conferencing	5 party conferencing to be provided (to be configurable dynamically)
15.	Digital / IP Extension telephone instrument with programmable one touch keys	

g. Civil Work, Safety Instrumentation and Furniture (at command center)

a. False Ceiling

- Providing and fixing metal false ceiling with powder coated 0.5mm thick hot dipped galvanized steel tiles 595 x 595 mm with regular edge (10mm) suitable for 25mm grid supported on suitable powder coated galvanized steel grid as per manufacturer specification. The same shall be inclusive of cut outs for lighting, AC grills, Fire detectors, nozzles, etc.
- 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

- 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.
- Providing & making of storage unit with 18 mm thick MDF board along with 1.5 mm approved laminate color 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

- 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.
- 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 low height partition, brick wall, partition wall, cladding etc. complete with French polish in all respect.
- 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 color 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)

- 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 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.
- With glazing including the framework of 4" x 2" powder coated aluminum section complete (in areas like partition between server room & other auxiliary areas).
- Providing & fixing Fire Rated Wire Glass minimum 6 mm thick for all glazing in the partition wall complete. (External windows not included in this).
- All doors should be minimum 1200 mm (4 ft.) wide.

d. Painting

- 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.
- For all vertical Plain surface.
- For fire line gyp-board ceiling.
- 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.
- Applying approved fire retardant coating on all vertical surfaces, furniture etc. as per manufacturer's specification.

e. Steel Conduit

- All sections of conduit and relevant boxes shall be properly cleaned and glued using appropriate epoxy resin glue and the proper connecting pieces, like conduit fittings such

as Mild Steel and should be so installed that they can remain accessible for existing cable or the installing of the additional cables.

- No conduit less than 20mm external diameter shall be used. Conduit runs shall be so arranged that the cables connected to separate main circuits shall be enclosed in separate conduits, and that all lead and return wire of each circuit shall be run to the same circuit.
- All conduits shall be smooth in bore, true in size and all ends where conduits are cut shall be carefully made true and all sharp edges trimmed. All joints between lengths of conduit or between conduit and fittings boxes shall be pushed firmly together and glued properly.
- All electrical wiring should be done as per CPWD specifications.

- 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 center 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.

f. Wiring

- PVC insulated copper conductor cable shall be used for sub circuit runs from the distribution boards to the points and shall be pulled into conduits. They shall be stranded copper conductors with thermoplastic insulation of 650 / 1100 volts grade. Color code for wiring shall be followed.
- Looping system of wring shall be used, wires shall not be jointed. No reduction of strands is permitted at terminations.
- Wherever wiring is run through trunking or raceways, the wires emerging from individual distributions shall be bunched together with cable straps at required regular intervals. Identification ferrules indication the circuit and D.B. number shall be used for sub main, sub circuit wiring the ferrules shall be provided at both end of each sub main and sub-circuit.
- Where, single phase circuits are supplied from a three phase and a neutral distribution board, no conduit shall contain wiring fed from more than one phase in any one room in the premises, where all or part of the electrical load consists of lights, fans and/or other single phase current consuming devices, all shall be connected to the same phase of the supply.
- Circuits fed from distinct sources of supply or from different distribution boards or M.C.B.s shall not be bunched in one conduit. In large areas and other situations where the load is divided between two or three phases, no two single-phase switches connected to difference phase shall be mounted within two meters of each other.
- All splicing shall be done by means of terminal blocks or connectors and no twisting connection between conductors shall be allowed.
- Metal clad sockets shall be of die cast non-corroding zinc alloy and deeply recessed contact tubes. Visible scraping type earth terminal shall be provided. Socket shall have push on protective cap.
- 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.

- 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.

g. Earthing

- 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. Earthling shall be in conformity with provision of rules 32, 61, 62, 67 & 68 of Indian Electricity rules 1956 and as per IS-3043. The entire applicable IT infrastructure in the Control Rooms shall be earthed.

- Earthing should be done for the entire power system and provisioning should be there to earth UPS systems, Power distribution units, and AC units etc. so as to avoid a ground differential. State shall provide the necessary space required to prepare the earthing pits.
- All metallic objects on the premises that are likely to be energized by electric currents should be effectively grounded.
- The connection to the earth or the electrode system should have sufficient low resistance in the range of 0 to 25 ohm to ensure prompt operation of respective protective devices in event of a ground fault, to provide the required safety from an electric shock to personnel & protect the equipment from voltage gradients which are likely to damage the equipment.
- Recommended levels for equipment grounding conductors should have very low impedance level less than 0.25 ohm.
- In case of a UPS and Transformer equipment, the Earth resistance shall be automatically measured on an online basis at a pre-configured interval and corrective action should be initiated based on the observation. The automatic Earthing measurements should be available on the UPS panel itself
- 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.
- The earth connections shall be properly made.
- 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.
- Provide separate earthing pits for servers, UPS & generators as per the standards.
- Expectation is to have maintenance free chemical earthing.

h. Cable Work

- Cable ducts should be of such dimension that the cables laid in it do not touch one another. If found necessary the cable shall be fixed with clamps on the walls of the duct. Cables shall be laid on the walls/on the trays as required using suitable clamping/ fixing arrangement as required. Cables shall be neatly arranged on the trays in such manner that a criss-crossing is avoided and final take off to switch gear is easily facilitated.
- 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 aluminum 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.
- Each section of the rising mains shall be provided with suitable wall straps so that same the can be mounted on the wall.
- Whenever the rising mains pass through the floor they shall be provided with a built-in fire proof barrier so that this barrier restricts the spread of fire through the rising mains from one section to the other adjacent section.
- Neoprene rubber gaskets shall be provided between the covers and channel to satisfy the operating conditions imposed by temperature weathering, durability etc.
- Necessary earthling arrangement shall be made alongside the rising mains enclosure by Mean of a GI strip of adequate size bolted to each section and shall be earthed at both ends. The rising mains enclosure shall be bolted type.
- The space between data and power cabling should be as per standards and there should not be any criss-cross wiring of the two, in order to avoid any interference, or corruption of data.

i. Fire Detection and alarm System

- 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.

i. System Description

- 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.
- 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.

ii. Control and Indicating Component

- 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.
- All controls of the system shall be via the control panel only.
- The system status shall be made available via panel mounted LEDs and a backlit 8 line x 40-character alphanumeric liquid crystal display.

- 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.
- 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.

iii. Manual Controls

- Start sounders
- Silence sounders
- Reset system
- Cancel fault buzzer
- Display test
- Delay sounder operation
- Verify fire condition
- Disable loop

iv. Smoke detectors:

Smoke detectors shall be of the optical or ionisation type. Devices shall be compatible with the CIE conforming to the requirements of EN54 Part 7 and be LPCB approved. The detectors shall have twin LEDs to indicate the device has operated and shall fit a common addressable base.

v. Heat detectors

- Heat detectors shall be of the fixed temperature (58° C) or rate of temperature rise type with a fixed temperature operating point.
- Devices shall be compatible with the CIE conforming to the requirements of EN54 Part 5 and be LPCB approved.
- The detectors shall have a single LED to indicate the device has operated and shall fit a common addressable base.

vi. Addressable detector bases

- All bases shall be compatible with the type of detector heads fitted and the control system component used. Each base shall comprise all necessary electronics including a short circuit isolator.
- The device shall be automatically addressed by the CIE on power up of the loop without the need of the insertion of a pre-programmed EPROM or setting of DIL switches.
- Detector bases shall fit onto an industry standard conduit box.

vii. Audible Alarms

- Electronic sounders shall be coloured red with adjustable sound outputs and at least 3 sound signals. The sounders should be suitable for operation with a 24V

DC supply providing a sound output of at least 100dBA at 1 meter and 75 dBA min, for a bed head or sounder base type device. The sounder frequency shall be in the range of 500Hz to 1000Hz.

viii. Commissioning

- The fire detection and alarm system will be programmable and configurable via an alpha numeric keypad on the control panel.

ix. High Sensitivity Smoke Detection System

- General – The HSSD system shall provide an early warning of fire in its incipient stage, analyse the risk and provide alarm and actions appropriate to the risk. The system shall include, but not be limited to, a Display Control Panel, Detector Assembly and the properly designed sampling pipe network. The system component shall be supplied by the manufacturer or by its authorized distributor.

x. Regulatory Requirements

- National Electrical Code (NEC)
- Factory Mutual
- Local Authority having Jurisdiction

j. Water leak detection System

- Water leak detection System should be designed to protect the Air-conditioned premises and to alert the personnel about the leak in the AC systems. The system should be capable of interfacing to Water leak detection sensors, condensation sensors & I/O modules.
- Events should be clearly reported on LCD/LED display with full English language description of the nature of the fault in the panel. The successful bidder should make detailed working drawings and coordinate them with other agencies at site. Water Leak Detection systems should be integrated with BAS.

i. EQUIPMENT

The Water leak detection system should comprise of Tape Sensors, Water Leak detection modules, Condensation detectors, I/O modules and sounders all connected to a Control Panel.

ii. CONTROL PANEL

- The control panel should be computerized 4/8/12 zone multiplex controller with a facility to add on dialer and speech processor. The system should be programmed, armed or disarmed through a control key pad. The control key pad should have a 16 character LCD display for viewing various events. The code to arm or disarm the system should be changed only by entering a master code.
- The system should have 4/8/12 zones and all the detectors should be connected through a 2 core cable. Each area of the premises should be divided into specific zones such that any zone should be isolated by the user if required.
- The entire system should be backed up by a maintenance free rechargeable battery to take care of system's power requirements whenever power fails.
- The system should be totally tamper proof and should activate an alarm if the control panel is opened, the sensors tampered with or if the system cables are cut even in the disarmed state.
- The system should log 500 events and optionally printer should be connected for generating reports.
- The Detectors, I/O Modules, Remote Keypads and other Devices should be connected to a system on a single 2/4/6 Core Cable Bus to avoid individual cabling of zones.
- The system should have a Buffer memory of minimum 250 events and log each event with exact date and time.
- The controller should have a Serial Port for connecting to a computer.
- The controller should work on 220/240V AC power supply and it should also have a built in battery backup.
- The memory inside the controller should be backed up by a lithium battery. The controller should work effectively over a temperature range of -10 Deg. C to + 55 Deg. C. and 0 to 90% of Humidity.

iii. WATER LEAK DETECTION SENSOR

Water Leak Detection sensors should be able to mount in DIN rails, inside AHU's, power distribution units or other equipment where localized leak detection is required.

The detectors should be resistant to oxidation and erosion. The detector should have relay output for connection to the controller. LED alarm indication should also be provided. The detectors should operate in AC or DC supply.

iv. TAPE SENSORS

Tape sensors are used to detect water leaks usually under floors. Tape sensors for use with water leak detectors should be covered with plastic netting to prevent short circuits when used in metal trays or conduits, and enables the tape to be folded at right angles to allow easy routing.

v. HOOTER / SOUNDER

The hooter / sounder should give audible alarm when any sensor operates. It should be complete with electronic oscillations, magnetic coil (sound coil) and accessories ready for mounting (fixing). The sound output from the Hooter should not be less than 85 decibels at the source point.

k. 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:

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

l. Rodent Repellent system:

The entry of Rodents and other unwanted pests shall be controlled using non-chemical, non-toxic devices. Ultrasonic pest repellents shall be provided in the false flooring and ceiling to repel the pests without killing them. However periodic pest control using Chemical spray can be done once in 3 months as a contingency measure to effectively fight the pest menace.

- Configuration : Master console with necessary transducer

- Operating Frequency : Above 20 KHz (Variable)
- Sound Output : 50 dB to 110 dB (at 1 meter)
- Power output : 800 mW per transducer
- Power consumption : 15 W approximately
- Power Supply : 230 V AC 50 Hz
- Mounting : Wall / Table Mounting

m. Instruction about Civil Work

a. Building design must be in accordance with international standards.
b. MSI has to provide the Building Design Parameters which are essential for building State of the Art Building of ICCC
    i. Layout Design
    ii. Cabling
c. Layout
    i. Type of cable (Fire resistant etc.)
d. Ducting
e. MSI should define the standard of on building construction.
f. It is expected that design of CCC building is demonstrated through 3D video.
g. MSI should recommend the international standards and suggest what specific requirement of building design are required for building a state of the art Integrated Command and Control Center.
h. Building design must be futuristic, using 3D modelling, which can be refined and revise the final view of the actual ICCC.
i. The ICCC physical building design should also be modular and able to accommodate other Municipal Corporations systems within ICCC premises.
j. MSI will be required to get approval on engineering drawings of ICCC from BSCDCL.
k. During the review of design documents, BSCDCL may suggest some changes or provide feedback on design parameters. MSI will be required to incorporate such inputs.
l. BSCDCL may authorize any third party do to review of design documents.
m. After final approval of BSCDCL on design documents, building work will be initiated by BSCDCL.

h. DG Set

#	Item	Minimum Specifications
1	General Specifications	• Auto Starting DG Set mounted on a common base frame with AVM (Anti-Vibration) pads, residential silencer with exhaust piping, complete conforming to ISO 8528 specifications and CPCB certified for emissions. • KVA rating as per the requirement to provide the supply for CCC
2	Engine	Radiator cooled, multi cylinder, 1500 RPM diesel engine, with electronic/manual governor and electrical starting arrangement complete with battery, conforming to BS 5514/ ISO 3046/ IS 10002
3	Fuel	High Speed Diesel (HSD)

5	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.
6	AMF (Auto Main Failure) Panel	AMF Panel fitted inside the enclosure, with the following: It should have 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 fuel tank, low fuel indication • Emergency Stop button • Auto/Manual/Test selector switch • MCCB/Circuit breaker for short-circuit and overload protection • Control Fuses • Earth Terminal • Any other switch, instrument, relay etc. essential for Automatic functioning of DG set with AMF panel
7	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 must be weather resistant powder coated, with insulation designed to meet latest MOEF/CPCB norms for DG sets, capable to withstand climate. The enclosure must have ventilation system, doors for easy access for maintenance, secure locking arrangement, complete and
8	Fuel Tank Capacity	It should be sufficient and suitable for containing fuel for minimum 12 hours continuous operation, Complete with level indicator, fuel inlet and outlet, air vent, drain plug, inlet arrangement for direct filling and set of fuel hoses for inlet and return.

i. Server (Application / Database or Other)

#	Parameter	Minimum Specifications
1.	Make And Model	To be specified by the bidder
2.	Processor	Latest generation x86 processor with highest cache and highest frequency (on processor with highest cache), within the selected category of cores, should be provided, e.g. while selecting 8 core processor, bidder

#	Parameter	Minimum Specifications
		needs to select the processor in 8 core category with highest frequency in the highest cache
3.		Min. 2 Physical sockets or higher
4.	Main Memory	Min. 8GB per core expandable to 196 GB
5.	RAS Features	Hot Pluggable Disk Drives
6.		Redundant Power Supply at server / chassis level
7.		Redundant hot swappable fans at server / chassis level
8.	Hard Disks	2 Nos. Hot-swap 146 GB or higher SAS/SCSI Disk Drives.
9.	RAID	Integrated RAID offering Striping, Mirroring (RAID 0, 1)
10.	Network Interface	Minimum 2Nos. 10/100/1000 Mbps Ethernet ports
11.		Minimum 2Nos. 8Gbps FC HBA ports or FCOE ports (wherever connectivity to Storage)
12.		Both Ethernet / FC ports should be in redundant mode
13.	USB	Minimum 1 USB 2.0 ports or an option for connecting USB devices
14.	Virtualization	The server should support virtualization technology and a software defined datacenter network infrastructure

j. Blade Chassis

#	Item	Minimum Requirement Description
1.	Blade Chassis	Blade chassis shall be 19" standard Width rack mountable and provide appropriate rack mount kit.
2.	Blade Chassis	The power supply modules should be hot pluggable and should be able to support fully populated chassis with all the servers with highest CPU and memory configuration in the offered series

#	Item	Minimum Requirement Description
3.	Blade Chassis (Redundancy)	The power subsystem should support all of the following modes of power redundancy (No redundancy, N+1 , N+N or grid)
4.	Blade Chassis (Redundancy)	The power subsystem should be support N + N power redundancy for a fully populated chassis with the 2 socket (CPU) servers
5.	Blade Chassis (Redundancy)	Should be configured to provide full redundant cooling to all blade slots
6.	Fabric Channel & Ethernet Interconnects	Bidder should provide converged fabric (FCOE) based modules in redundancy to provide 10 Gbps of uplink aggregated bandwidth per server
7.	Management	It should support remote KVM / virtual KVM capability for management and administration.
8.	Blade Chassis (DVD)	Should support virtual DVD and virtual floppy internally / externally
9.	Interface	The Fabric switches should support the direct connection to FCoE enabled storage arrays
10.	Management	Supports a stateless environment where server identity is created by the administrator who defines the server BIOS version, MAC ID, NIC firmware version, WWPN , FC-HBA firmware version , Adapter QoS , Management module firmware version, UUIDs , Server Boot Policies, KVM IP etc
11.	Blade Chassis	Servers can be automatically assigned to the resource pools based on qualification criteria
12.	Management	Firmware upgrade / rollback should be possible for all the components in the infrastructure including the server, chassis management modules , Ethernet switch modules, SAN switch modules, Other IO modules from the same console that is used to manage the individual blades
13.	Management	Role Based Access Control so that the resources can be managed by respective resource administrator.
14.	Server Management	Movement of server identity from one slot to another in the event of server failure. The failover can be movement within a single chassis or across multiple chassis
15.	Power Management	Administrators have the flexibility to define power policies so that the power can be limited to a specific server
16.	Power Management	Administrators should be able to decide the threshold / cap on the maximum power that the chassis can draw.
17.		The system should not be an end of life / end of service product.
18.	Support	The system should not be an end of life / end of service product.

k. Storage Specification

#	Parameter	Minimum Specifications
1.	Solution/Type	• The Solution should be using NL-SAS/SAS Disks for Video camera storage purpose and SSDs/Flash for all other applications. • Solution proposed should yield low cost per TB, while meeting the performance parameters

#	Parameter	Minimum Specifications
		• Licenses for the actual protocols used in the storage solution must be provided from day 1.
2.	Storage	• The SSD storage should provide inline deduplication and inline compression to reduce the capacity requirement and the solution can factor upto 2x capacity efficiency for this purpose. If storage OEMs do not support inline deduplication and inline compression, then they cannot assume any storage efficiency and should provide the required usable capacity to compensate for lack of benefits of these features
3.	Hardware Platform	• Rack mounted form-factor • Modular design to support controllers and disk drives expansion
4.	Connectivity	• The storage system shall be capable of providing host connectivity as per solution offered (Unified/SAN/NAS/Scale out NAS) as to meet operational SLA requirements.
5.	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.
6.	RAID support	• Should support various RAID levels (Minimum RAID6 or equivalent)
7.	Cache	• Minimum 128 GB of useable cache spread across all controllers of the storage system. This should be scalable to 256GB in a scale-up or scale-out fashion. If cache is provided in additional hardware for unified storage solution, then cache must be over and above 128 GB.
8.	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
9.	Storage 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 disk capacity/count of the complete solution and any additional disks to be plugged-in in the future, up to the max disk capacity of the existing controllers/units. • A single command console for entire storage solution. • 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

#	Parameter	Minimum Specifications
		• Should be able to take "snapshots" (or equivalent feature) of the stored data to another logical drive for backup purposes
10.	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
11.	IOPS	Offered Primary Storage shall support up for the operation. Please suggest how we reached this value
12.	Operating system support	The storage system should support latest versions of operating systems like Linux, RHEL, SUSE, Windows, Apple, etc.
13.	File system	The File system managing the SAN Storage should support the management of Secondary Storage to move the data from Primary to Secondary Storage.
14.	Firmware	The storage system should support non-disruptive updation/upgrade of firmware for controllers and disks.
15.	Diagnostic	The storage system should have facility to report any failures & errors through Intranet for diagnosis and quick resolution of problems.
16.	Interface	The storage management software should come with web-based/CLI interface for configuring the SAN system from anywhere using TCP/IP network.
17.	Cloud Integration	The proposed solution must provide flexibility to move the application and its associated data from private cloud to MEITY empaneled public cloud, across two different MEITY empaneled public cloud providers and from MEITY empaneled Public Cloud to Private Cloud depending on requirements of various departments. This movement of data should be carried out with minimal downtime, over the Network in an encrypted form. The proposed solution should allow flexibility to allow Primary Site to be on private cloud and its DR to be hosted on MEITY empaneled public cloud without any limitations. The proposed solution should provide for a cloud backup gateway which provides flexibility to backup/archive applications and data from public/private cloud to another public/private cloud.

l. Core Switch

#	Minimum Specifications
1.	Should be a chassis based switch and have minimum 32 x 40G QSFP+ or more ports distributed across minimum two or more interface line-cards fully populated with Mode Fiber Transceiver. In addition, it must have 48x 10G BaseT ports and 48x 1/10G SFP+ ports fully populated with multi-mode fiber transceiver.
2.	There should not be any single point of failure in the switch. All the main components like CPU module, switching fabric, power supplies and fans etc. should be in redundant configuration.
3.	It must have minimum five or more vacant interface payload slots (after populating all the required above interfaces).
4.	Chassis must support 40G and 100G interface line cards.
5	Should have minimum of 3.84 Tbps full duplex or more per interface slot throughput.

6	All the interfaces / line-cards should be non-blocking and wire-speed for 64 bytes of packet size and have distributed forwarding architecture.
7	Should have 128K IPv4 Routes, 32K IPv6 Routes, 12K ACL's, 160K MAC Address, 4K active VLAN's and 8 hardware queues per port.
8	Should support minimum of 32 no of ports per LAG / vLAG / Ether channel.
9	Should have IPv6 Static routes, OSPFv3, PIM Sparse / Dense mode (SM /DM), Policy-based routing (PBR), Virtual routing and forwarding (VRF), BGP and Netflow/ Jflow/ Sflow.
10	Should have minimum of 64MB or more of packet buffer size for traffic to support huge file transfers on all the proposed line-cards.
11	Should support the separation of data and control plane, to be controlled by SDN Controller, utilizing ACI / openflow or equivalent protocol.
12	It is preferred that Switch & transceiver to be from same OEM.

m. Core Router

#	Minimum Specifications
1.	Chassis should have a minimum 16 x 1/10G SFP+ or more ports populated with Multi-mode 10G SR transceivers from day 1. In addition, it must have an additional 16 x 10/100/1000 BaseT RJ45 ports.
2.	There should not be any single point of failure in the Router. All the main components like Supervisor / CPU module, management module, power supplies and fans etc should be in redundant configuration. It should have distributed forwarding and there should not be any performance degradation in case of any switching/routing engine failure.
3.	It must have minimum two or more vacant interface payload slots from day 1 (after populating all the required above interfaces).
4.	Should have minimum of 400 Gbps or more per interface slot throughput from day 1 with all the above asked redundancy.
5	All the interfaces / line-cards should be non-blocking and wire-speed for 64 bytes of packet size and have distributed forwarding architecture.
6	Should have 1M IPv4 Routes, 200K IPv6 Routes, 32K IPv6 Multicast routes, 1M MAC Address and 4K active VLAN's.
7	Chassis must support 40G and 100G interface line cards
8	Should have IPv6 Static routes, OSPFv3, PIM Sparse / Dense mode (SM /DM), Policy-based routing (PBR), Virtual routing and forwarding (VRF), BGP, BFD, MPLS and Netflow/Jflow/Sflow.
9	It is preferred that Router & transceiver should be from same OEM.

n. Internet Router

#	Minimum Specifications
1.	Chassis should have a minimum 8 x 10G SFP+ or more ports populated with Multi-mode 10G SR transceivers from day 1. In addition, it must have an additional 8 x 10/100/1000 BaseT RJ45 ports from day 1.

2.	There should not be any single point of failure in the Router. All the main components like Supervisor / CPU module, management module, power supplies and fans etc should be in redundant configuration. It should have distributed forwarding and there should not be any performance degradation in case of any switching/routing engine failure.
3.	It must have minimum two or more vacant interface payload slots (after populating all the required above interfaces).
4.	Should have minimum of 400 Gbps or more per interface slot throughput with all the above asked redundancy.
5	All the interfaces / line-cards should be non-blocking and wire-speed for 64 bytes of packet size and have distributed forwarding architecture.
6	Should have 1M IPv4 Routes, 200K IPv6 Routes, 32K IPv6 Multicast routes, 1M MAC Address and 4K active VLAN's .
7	Chassis must support 40G and 100G interface line cards from day 1
8	Should have IPv6 Static routes, OSPFv3, PIM Sparse / Dense mode (SM /DM), Policy-based routing (PBR), Virtual routing and forwarding (VRF), BGP, BFD, MPLS and Netflow/Jflow/Sflow.
9	It is preferred that Router & transceiver should be from same OEM.

o. SAN Switch

#	Parameter	Minimum Specifications
1.	Power Specification	200-240V, 50-60 Hz
2.	Operating temperature range	0° to 40° C
3.	Operating Relative Humidity range (non-condensing)	10 to 90% relative humidity
4.	Total no. of ports on the proposed switch	24
5.	Throughput of each FC port	8/16Gbps
6.	Support for 4/8/16 Gb/s HBAs	YES
Protocol Supported		
7.	FC	Yes
8.	FCP	Yes
9.	FC-AL	Yes
10.	Designed for high availability with no Single Point of Failure	Yes
Power Supply		
11.	Hot Swappable Power supply proposed	Yes
12.	(N+1) redundant power supply proposed	Yes
Cooling Fans		
13.	Hot Swappable Cooling Fans proposed	Yes

#	Parameter	Minimum Specifications
14.	(N+1) redundant Cooling Fans proposed	Yes
15.	Capability for streaming the data in multiple paths with Optimization algorithms for streaming data through shortest available path.	Yes
16.	Capabilities for cascading of switches	Yes
17.	Non-disruptive firmware update	Yes
18.	End to end performance monitoring	Yes
19.	Capability to interface with host based adapters (HBA) of multiple OEM, supporting multiple Operating System including but not limited to AIX, HP-UX, Linux, Solaris, Windows, etc.	Yes
Zoning And Security		
20.	The switch must support hardware ACL-based Port Security, Virtual SANs (VSANs), and Port Zoning.	Yes
21.	Policy based security and centralised fabric management	Yes
22.	Support for Encrypted password	Yes
23.	Support for PKI Digital certificates	Yes
24.	Support for FCAP or FC-SP authentication	Yes
25.	Support for RADIUS, SSL / HTTPS, SSH, SNMP V3	Yes
26.	Support for LUN masking	Yes
Support For Hardware Based Trunking		
27.	Compatibility with proposed network devices	Yes
28.	Compatibility with proposed servers	Yes
29.	The system should not be an end of life / end of service product.	Yes

p. Aggregation/ Data center Switches (L3 Manageable)

#	Parameter	Minimum Specifications
1.	Ports	• 10/100/1000 Base-TX Ethernet ports/FX and extra 2 numbers of Base-SX/LX ports should be one either 24 or 48 • FX/TX Splits for a switch as per location requirement All ports can auto-negotiate between 10Mbps/ 100Mbps/ 1000Mbps, half-duplex or full duplex and flow control for half-duplex ports.
2.	Switch type	Layer 3

3.	MAC	Support 8K or 16K MAC address. (as per solution offered)
4.	Forwarding rate	Packet Forwarding Rate should be 70.0 Mbps or better
5.	Port Features	Must support Port Mirroring, Port Trunking and 802.3ad LACP Link Aggregation port trunks
6.	Flow Control	Support IEEE 802.3x flow control for full-duplex mode ports.
7.	Protocols	• 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 • 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 IPV6 ready features with dual stack • Support up to 255 VLANs and up to 4K VLAN IDs • Support IGMP Snooping, IGMP Querying and Multicasting Should support Loop protection and Loop detection, Should support Ring protection (when used in aggregation location)
8.	Access Control	• Support port security • Support 802.1x (Port based network access control). • Support for MAC filtering. Should support TACACS+ and RADIUS authentication
9.	VLAN	• Support 802.1Q Tagged VLAN and port based VLANs and Private VLAN • The switch must support dynamic VLAN Registration or equivalent Dynamic Trunking protocol or equivalent
10.	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
11.	Management	• Switch needs to have RS-232/USB console port for management via a console terminal/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

q. KVM Module

#	Item	Minimum Specifications
1.	KVM Requirement	Keyboard, Video Display Unit and Mouse Unit (KVM) for the IT Infrastructure Management at Data Center
2.	Form Factor	19” rack mountable
3.	Ports	minimum 8 ports
4.	Server Connections	It should support both USB and PS/2 connections.
5.	Auto-Scan	It should be capable to auto scan servers
6.	Rack Access	It should support local user port for rack access
7.	SNMP	The KVM switch should be SNMP enabled. It should be operable from remote locations
8.	OS Support	It should support multiple operating system
9.	Power Supply	It should have dual power with failover and built-in surge protection
10.	Multi-User support	It should support multi-user access and collaboration

r. Rack with KVM over IP

#	Parameter	Minimum Specifications
1.	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
2.	Wire managers	Two vertical and four horizontal
3.	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
4.	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.
5.	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
6.	Metal	Aluminium extruded profile
7.	Side Panel	Detachable side panels (set of 2 per Rack)

s. Load Balancer

- **Server Load Balancer**

#	Parameter & minimum specification
	Server Load Balancing Mechanism
1	Cyclic, Hash, Least numbers of users
2	Weighted Cyclic, Least Amount of Traffic
3	NT Algorithm / Private Algorithm / Customizable Algorithm / Response Time
	Redundancy Features
1	Supports Active-Active and Active-Standby Redundancy
2	Segmentation / Virtualization support along with resource allocation per segment, dedicated access control for each segment
	Routing Features
1	Routing protocols RIPv1/RIPv2/OSPF
2	Static Routing policy support
	Server Load Balancing Features
1	Server and Client process coexist
2	UDP Stateless
3	Service Failover
4	Backup/Overflow

5	Direct Server Return
6	Client NAT
7	Port Multiplexing-Virtual Ports to Real Ports Mapping
8	DNS Load Balancing
	Load Balancing Applications
1	Application/ Web Server, MMS, RTSP, Streaming Media
2	DNS, FTP- ACTIVE & PASSIVE, REXEC, RSH,
3	LDAP, RADIUS
	Content Intelligent SLB
	HTTP Header Super Farm
	URL-Based SLB
	Browser Type Farm
1	Support for Global Server Load Balancing
2	Global Server Load Balancing Algorithms
3	HTTP Redirection,
4	HTTP
5	DNS Redirection, RTSP Redirection
6	DNS Fallback Redirection, HTTP Layer 7 Redirection
7	SLB should support below Management options
	Secure Web Based Management
1	SSH
2	TELNET
3	SNMP v1, 2, 3 Based GUI
4	Command Line

- **Application Load Balancer**

#	Parameter & minimum specification
	Application Load balancing features
1	Should able to load balancer both TCP and UDP based applications with layer 2 to layer 7 load balancing support
2	The appliance should support server load balancing algorithms i.e. round robin, weighted round robin, least connection, Persistent IP, Hash IP, Hash Cookie, consistent hash IP, shortest response, proximity, snmp, SIP session ID, hash header etc.
3	Should support Multi-level virtual service policy routing – Static, default and backup policies for intelligent traffic distribution to backend servers
4	Support for policy nesting at layer7 and layer4, solution should able to combine layer4 and layer7 policies to address the complex application integration.
5	Script based functions support for content inspection, traffic matching and monitoring of HTTP, SOAP, XML, diameter, generic TCP, TCPS. Load balancer should support ePolicies to customize new features in addition to existing feature/functions of load balancer
6	Traffic load balancing using ePolicies should support algorithms including round robin, least connections, shortest response, persistence ip, hash ip, hash ip and port, consistent hash ip and snmp

7	Should provide application & server health checks for well-known protocols such as ARP, ICMP, TCP, DNS, RADIUS, HTTP/HTTPS, RTSP etc.
8	IPv6 gateway and Application acceleration
9	Appliance should provide real time Dynamic Web Content Compression to reduce server load and solution should provide selective compression for Text, HTML, XML, DOC, Java Scripts, CSS, PDF, PPT, and XLS Mime types.
10	should provide advanced high performance memory/packet based reverse proxy Web cache; fully compliant with HTTP1.1 to enhance the speed and performance of web servers
11	Should provide support for cache rules/filters to define granular cache policies based on cache-control headers, host name, file type, max object size, TTL objects etc..
12	Should provide secure online application delivery using hardware-based high performance integrated SSL acceleration hardware. SSL hardware should support both 2048 and 4096 bit keys for encrypted application access.
	Clustering and failover
1	Should provide comprehensive and reliable support for high availability with Active-active & active standby unit redundancy mode. Should support both device level and VA level High availability
2	should support built in failover decision/health check conditions (both hardware and software based) including CPU overheated, SSL card, port health, CPU utilization, system memory, process health check and gateway health check to support the failover in complex application environment
3	Should have option to define customized rules for gateway health check - administrator should able to define a rule to inspect the status of the link between the unit and a gateway
4	Support for automated configuration synchronization support at boot time and during run time to keep consistence configuration on both units.
5	Support for multiple communication links for real-time configuration synchronizations including HA group, gateway health check, decision rules, SSF sessions etc. and heartbeat information
6	Clustering function should support IPv6 VIP's (virtual service) switchover
7	N+1 clustering support with active-active and active-standby configurations.
	Application firewall
1	The device should have abuse detection, tracking, Profiling and should support Abuse response and real time incident management
2	Device e should be able inspect HTTP and HTTPS traffic on TCP port 80 & 443
3	Should be able to detect attempts to abuse form inputs and establish vectors for injection and cross-site scripting attacks
4	Must protect web application against Cookie Poisoning, cookie injection command injection.
5	Must protect web application against buffer overflow and layer7 DDOS attacks.
6	Must protect web application against parameter tampering and must have inbuilt controls to block invalid files, filtering of sensitive words in HTTP request and response.
7	Should be able to detect suspicious application errors that indicate abuse including illegal and unexpected response codes.
8	Should be able to detect when an attacker is attempting to request files with suspicious extensions, prefixes, and tokens

9	Should support creation of the policies for HTTP/HTTPS headers to ensure critical infrastructure information is not exposed. Response and request headers can be stripped, mixed, or filtered
10	Should be able to detect and prevent attackers from finding hidden directories. inbuilt security control to limit the action of crawling and scanning
11	Should be able to detect attempts to abuse non-standard HTTP/HTTPS methods such as TRACE.
12	Should be able to detect attempts to manipulate application behavior through query parameter abuse. Solution must support behavior analysis to detect and prevent day 0n attacks
13	Should maintain a profile of known application abusers and all of their malicious activity against the application
14	Should support network based security controls including ACL's, IP blacklist/whitelist and URL blacklist/Whitelist
15	Anti-DDOS protection with syn flood, UDP flood, ICMP flooding, command and control protection
	Management , Logging & Monitoring
1	Should support simplified configuration with wizards
2	Should support web-based configuration.
3	Should support web-based monitoring and analysis interface
4	Solution Should Support Restful API
5	Should support role based access control with different privilege levels for configuration management and monitoring.
6	The appliance should provide detailed logs and graphs for real time and time based statistics
7	Should enable SNMP system logging and able to send alerts to a centralized EMS solution

- **Link Load Balancer**

#	Parameter & minimum specification
	Link Load balancing features
1	Support for multiple internet links in Active-Active load balancing and active-standby failover mode.
2	Should support Outbound load balancing algorithms like round robin, Weighted round robin, shortest response, hash ip, target proximity and dynamic detect
3	Should support inbound load balancing algorithms like round robin, Weighted round robin, target proximity & dynamic detect.
4	Should support Static NAT, Port based NAT and advanced NAT for transparent use of multiple WAN / Internet links.
5	IPV6 support with IPv6 to IP4 and IPv4 to IPv6 translation and full IPv6 support.
6	IPV6 support with DNS 6 to DNS 4 & DNS 4 to DNS 6 translation
7	Domain name support for outbound link selection for FQDN based load balancing.
8	Dynamic detect (DD) based health check for intelligent traffic routing and failover
9	In case of link failure, device should detect it in less than 30 seconds and divert the traffic to other available links.
10	Shall provide individual link health check based on physical port, ICMP Protocols, user defined l4 ports and destination path health checks.

11	Should provide mechanism to bind multiple health checks, support for Application specific VIP health check and next gateway health checks.
12	Should support persistency features including RTS (return to sender) and ip flow persistence.
	Application Performance
1	Should provide performance optimization using TCP connection multiplexing, TCP buffering and IEEE 802.3ad link aggregation.
2	Should support TCP optimization options including windows scaling, timestamp & Selective Acknowledgement for enhanced TCP transmission speed.
3	TCP optimization option configuration must be defined on per virtual service basis not globally.
4	Software based compression for HTTP based application, support and high speed HTTP processing on same appliance.
5	Should support QOS for traffic prioritization, CBQ, borrow and unborrow bandwidth from queues.
6	Should provide QOS filters based on port and protocols including TCP, UDP and ICMP Protocols.
7	Should support rate shaping for setting user defined rate limits on critical application.
	Remote access
1	SSL VPN solution should be 100% client less for web based applications
2	must support for CIFS file share and provision to browse, create and delete the directories through web browser
3	should maintain original server access control policies while accessing the file resources through VPN
4	must support Single Sign-On (SSO) for web based applications and web based file server access
5	Should have secure access solutions for mobile PDAs, Andriod smart phones, Ipad, Iphones.
6	Should Support IPV6
7	SSL VPN solution must provide machine authentication based on combination of HDD ID, CPU info and OS related parameters i.e. mac address to provide secure access to corporate resources.
8	Should support following Authentication methods: - LDAP, Active directory, Radius, secureID, local database, and certificate based authentication and anonymous access.
9	Management
10	Centralized management appliance should have extensive reporting and logging with inbuilt tcpdump like tool and log collecting functionality
11	Solution Should Support Restful API
12	The appliance should have SSH CLI, Direct Console, SNMP, Single Console per Cluster with inbuilt reporting.
13	Should support XML-RPC for integration with 3rd party management and monitoring
14	Should support role based access control with different privilege levels for configuration management and monitoring.
15	The appliance should provide detailed logs and graphs for real time and time based statistics

t. Firewall (Internal/ External)

#	Parameter & minimum specification
	General and Performance Specifications.
1.	The Firewall should have integrated Firewall and VPN functionality.
2.	Firewall packet handling performance should be adequate to deliver the required throughput.
3.	Firewall should have a redundant power supply.
	Operational Modes.
4.	The Firewall should support Layer 2 (Transparent) mode and Layer 3 mode.
5.	Firewall should support static NAT; Policy based NAT and PAT (Port Addressed Translation).
	Firewall.
6.	Firewall should provide TCP reassembly for fragmented packet protection.
7.	Firewall should support integration with URL/Content filtering systems.
	VPN.
8.	Firewall should be capable of dynamic routing on VPN.
9.	Firewall should support client based SSL/TLS as well as IPSec VPN Tunnels.
	High Availability.
10.	Firewall should support Active/Passive High Availability.
11.	Firewall should support Active/Active High Availability.
12.	Firewall should support Stateful failover of firewall sessions.
13.	Firewall should support device failure detection.
14.	Firewall should support link failure detection.
15.	Firewall should support authentication for all members.
16.	Firewall should support encryption of all traffic.
	Routing.
17.	Support for OSPF and BGP routing protocol
18.	Firewall should support static routes
19.	Should support Multicast with features like RPF, IGMP/ IGMP Proxy, and PIM.
	IPv6 Support
20.	Should support dual stack IPv4 / IPv6 Firewall and VPN.
21.	Support for IPv4 to/from IPv6 translations or tunneling.
22.	Should support Virtualization (Virtual Firewall, Security zones and VLAN).
	Firewall Management
23.	Firewall should support Web based (HTTP and HTTPS) configuration and management.
24.	Firewall should support Command Line Interface using console and SSH.
25.	Firewall should support management via VPN tunnel on any interface.
	Logging.
26.	Should support Syslog server logging.
27.	Should have support for SNMP V1 to V3.

#	Parameter & minimum specification
28.	Support for voice protocols: H.323, SIP, and NAT/ ALG for H.323/ SIP.
29.	Firewall should have Automated certificate enrolment (SCEP). PKI Support.
	Administration.
30.	Firewall should support multilevel administration privilege.
31.	Firewall should support software upgrades using secure web Interface
32.	Firewall should support Command Line Interface using console SSH.

u. Data Leakage Prevention

#	Parameter & minimum specification
	DLP design and architecture
1	The solution can be proposed as either hardware or software based. However For software based solution, Supplier has to provide appropriate hardware keeping overall design and functional requirement under consideration and must not affect overall application performance.
	The proposed solution should not require any third party proxy server (such as ICAP servers – Blue Coat or any other ICAP server) to provide Enforcement of Information Security
2	The proposed solution should cover both Active and passive FTP including fully correlating transferred file data with control information
3	The proposed solution Should have the ability to monitor popular IM protocols (AIM, Yahoo, MSN, IRC) and properly classify tunneled IM traffic (HTTP)
4	The proposed solution should be able to interface with an institution's employee or staff directories (e.g., Active Directory, LDAP)
5	The proposed solution must have Identity and Role Based policy capabilities that integrate with AD/LDAP/HR database.
6	The proposed solution should be capable of "Segmentation of Duty" (SoD) based Enforcement of Information Security
7	The proposed solution should enforce "Automatic Access Control" on Data and Information
8	The proposed solution must be able to apply different policies to different employee groups
9	The proposed solution should have ability to filter out network traffic for inspection based on protocol, IP range, or email sender/recipient email
10	The proposed solution should have various methods to monitor quarantine and block e-mails that violates the company's DLP policies (existing)
11	The proposed solution should provide encryption capabilities to protect data at risk
	Information Classification
1	The proposed solution should have a comprehensive Information Classification methodology that would be readily deployable
2	The proposed solution should have Resources Qualification and experience in Information Classification
	Policy Management
1	The proposed solution should have ability to create and manage policies that can be deployed across all components (Network and Endpoints)
2	The proposed solution MUST use automated policy mechanism
3	The proposed solution should have built-in Automated Policy Synthesis mechanism

4	The proposed solution should be able to monitor and prevent Advanced Persistent Threats (APT)
5	The proposed solution should have Built-in Ontologies on International PII and PCI-DSS capabilities and has the ability to add or customized new Ontologies to cater to specific Government or Defense parameters
6	The proposed solution should have rule or policy-based capabilities such as assigning access rights, restricting where users can store sensitive data, and so forth
	Detection and Enforcement
1	The proposed solution should have ability to Detect based on fully customizable regular expressions
2	The proposed solution should have Ability to detect and protect confidential unstructured data based on the data categorization that has been learnt
3	The proposed solution should have Ability to detect and protect new or unseen documents, which content is similar to the data categorization which has been taught via data categorization
4	The proposed solution should have Ability to detect scanned documents, which contains sensitive data in text form
5	The proposed solution should have Ability to detect screen captures or picture formats, which contain sensitive data in text form.
6	The proposed solution should have Ability to learn to categorize data via providing a set of sample documents to improve accuracy of detection.
7	The proposed solution should have Ability to detect new unstructured documents.
8	The proposed solution should have Redaction of certain data such as sender identity information (email address, username, file owner, etc.) that may need to be kept confidential from certain users to protect employee privacy.
9	The proposed solution should have Ability to configure and send multiple automated responses based on severity, match count, policy, etc.
10	The proposed solution should have Ability to release quarantined email from notification received.
	Incident Management
1	On-screen/ pop-up/ e-mail notification delivered to users during a rule/ policy violation and escalation workflow to ICT Security team or immediate manager.
2	User's ability to conduct self-remediation (such as on-screen/pop-up/e-mail notification prompting user to confirm whether to continue or cancel confidential data transfer). Ability to capture justification for DLP rule/policy violation as part of logs capturing.
3	All relevant incident details on a single screen/ page to allow quick user decision-making and immediate action.
4	Per-user ability to customize the layout and data of the incident snapshot.
5	Store and display in the user interface the original message or file that generated the incident.
6	Ability for an incident to be correlated to other incidents by subject, sender, recipient, filename, file owner, user name, and policy.
7	The proposed solution should support incident search functionality
	a. Time
	b. Keyword
	c. Employee Name/ Staff ID
	d. Department Unit
	e. Violated Policies

	f. Multiple parameters (example: by Time + Keyword + Staff ID)
	g. Others. Please state.
8	The proposed solution should have methods to ensure fast search response with large amount of data
9	The proposed solution should have ability to support real-time incident analysis
10	Limit access to incident details for a role-based by policy, by department or business unit, by severity or remediation status, or by any user-defined custom attribute.
11	The proposed solution should have Integration with external directory for incident workflow assignment
	a. Active Directory (AD)
	b. Others please state.
12	Ability to create/ update/ delete/ manages work flow processes such as changing severity, status, escalation, via e-mail notification response suitable for XXX BANK's environment.
	Administration and Management
1	Support centralized administration. Ability to support network, storage and endpoint DLP from single console.
2	Describe administration method supported by the proposed solution
	a. Client-Server
	b. Web based
3	Support for role-based access and delegated administration.
4	Integration with Active Directory or other directory
5	Support real-time dashboard display. Describe and attach screenshot:
	a. Type of display (e.g.. Chart type)
	b. Type of information
	c. Incident status
6	Provide detailed and summarized traffic statistics down to an hourly level for:
	a. overall data
	b. number of messages
	c. number of incidents on a per protocol basis
7	Should have customizable dashboard
8	Ability to support log integration with RSA Envision Security Information and Event Management system.
9	Ability to support automatic updates (signatures/ rules/ etc) and firmware upgrades
	Reporting
1	The proposed solution should have a list of pre-defined template reports
2	The proposed solution should Support ad-hoc and scheduled report generation
3	The proposed solution should Support report customization
4	The following reporting format must be supported but not limited to:
	a. CSV
	b. HTML
	c. PDF
	End point DLP
1	The end point solution should inspect data leaks from all portable storage and to keep track of what data users are taking from and to their work computers on any kind of portable storage device

2	the end point solution must monitor and control various storage devices including USB flash drives, CD/DVD, external HDD, card readers, Zip drives, digital cameras, smartphones, PDA, MP3 players, Bluetooth devices etc.,,
3	The endpoint solution should be able to monitor data copied to USB storage devices and should enforce trusted device policy
4	The endpoint solution should Blocking of non-Windows CD/DVD burners, it should also Inspect and optionally block Explorer writes to WPD class devices
5	End point DLP agent should support network offline mode to access a specific device when a client computer is disconnected from a network
6	The endpoint solution should encrypt information copied to removable media
7	end point DLP agent should support protection features such as client uninstall and client stop in order to ensure client is running all the time and user should not have authority to uninstall or stop the services
8	Endpoint solution should Keep a record of all clients, devices and actions producing history reports for future audits
9	Solution should be Equipped with a powerful reporting tool that makes auditing easy and straight forward.

v. Integrated Building management system

Sr #	Description
1.	A. The MSI shall supply, install and commission BAS, Access control and Physical security system for ICCC Building Office. MSI has to also provide all necessary hardware and all operating and applications software necessary to perform the control sequences of operation as called for in this specification B. The MSI shall Supply, install and commission a complete Building Automation System (BAS) including all necessary hardware and all operating and applications software necessary to perform the control sequences of operation as called for in this specification. All components of the system –, application controllers, unitary controllers, etc. shall communicate using the BACnet protocol, as defined by ASHRAE Standard 135-2007, or EIA standard 709.1, the LonTalk™ protocol, or Modbus protocol. At a minimum, provide controls for the following: 1. Air handling units 2. Return air fans 3. Exhaust and supply fans 4. Chilled water system including pumps, chillers, and cooling towers 5. Boilers including hot water pumps 6. Computer room air handling units 7. Refrigerant leak detection system 8. Smoke evacuation sequence of AHUs and return fans including smoke control dampers and fire command override panel. 9. Finned tube radiation control 10. Variable volume and constant volume box control including interlocks with finned tube radiation. 11. Cabinet unit heater controls 12. Monitoring points for packaged equipment such as emergency generators,

	13. Power wiring to DDC devices, smoke control dampers and BAS panels except as otherwise specified. C. Except as otherwise noted, the control system shall consist of all necessary Ethernet Network Controllers, Standalone Digital Control Units, workstations, software, sensors, transducers, relays, valves, dampers, damper operators, control panels, and other accessory equipment, along with a complete system of electrical interlocking wiring to fill the intent of the specification and provide for a complete and operable system. Except as otherwise specified, provide operators for equipment such as dampers if the equipment manufacturer does not provide these. Coordinate requirements with the various Contractors. D. The MSI shall review and study all HVAC drawings and the entire specification to familiarize themselves with the equipment and system operation and to verify the quantities and types of dampers, operators, alarms, etc. to be provided. E. All interlocking wiring, wiring and installation of control devices associated with the equipment listed below shall be provided. When the BAS system is fully installed and operational, the MSI and representatives of the Owner will review and check out the system. At that time, the MSI shall demonstrate the operation of the system and prove that it complies with the intent of the drawings and specifications. F. Provide services and manpower necessary for commissioning of the system in coordination with the existing HVAC Contractor, Balancing Contractor and Owner's representative. G.
2.	**BAS -System Description** H. In accordance to the scope of work, the system shall also provide a graphical, web-based, operator interface that allows for instant access to any system through a standard browser. The contractor must provide PC-based programming workstations, operator workstations and microcomputer controllers of modular design providing distributed processing capability, and allowing future expansion of both input/output points and processing/control functions. The system shall consist of the following components: • Administration and Programming Workstation(s) • Ethernet-based Network Router and/or Network Server Controller(s) These controllers will connect directly to the Operator Workstation over Ethernet at a minimum of 100mbps, and provide communication to the Standalone Digital Control Units and/or other Input/Output Modules. Network Server Controllers shall conform to BACnet device profile B-BC. Network controllers that utilize RS232 serial communications or ARCNET to communicate with the workstations will not be accpted. • Network Controllers shall be tested and certified by the BACnet Testing Laboratory (BTL) as Network Server Controllers (B-BC). • Standalone Digital Control Units (SDCUs): Provide the necessary quantity and types of SDCUs to meet the requirements of the project for mechanical equipment control including air handlers, central plant control, and terminal unit control. Each SDCU will operate completely standalone, containing all of the I/O and programs to control its associated equipment. Each BACnet protocol SDCU shall conform to the BACnet device profile B-AAC. • BACnet SDCUs shall be tested and certified by the BACnet Testing Laboratory (BTL) as Advanced Application Controllers (B-AAC). I. The Local Area Network (LAN) shall be either a 10 or 100 Mpbs Ethernet network supporting BACnet, Modbus, Java, XML, HTTP, and CORBA IIOP for maximum flexibility for integration of building data with enterprise information systems and providing support for multiple Network Server Controllers (NSCs), user workstations and a local host computer system.

J. The Enterprise Ethernet (IEEE 802.3) LAN shall utilize Carrier Sense Multiple/Access/Collision Detect (CSMA/CD), Address Resolution Protocol (ARP) and User Datagram Protocol (UDP) operating at 10 or 100 Mbps.

K. The system shall enable an open architecture that utilizes EIA standard 709.1, the LonTalk™ protocol and/or ANSI / ASHRAE™ Standard 135-2007, BACnet functionality to assure interoperability between all system components. Native support for the LonTalk™ protocol and the ANSI / ASHRAE™ Standard 135-2007, BACnet protocol are required to assure that the project is fully supported by the HVAC open protocols to reduce future building maintenance, upgrade, and expansion costs.

L. The system shall enable an architecture that utilizes a MS/TP selectable 9.6-76.8 KBaud protocol, as the common communication protocol between all controllers and integral ANSI / ASHRAE™ Standard 135-2008, BACnet functionality to assure interoperability between all system components. The AAC shall be capable of communicating as a MS/TP device or as a BACnet IP device communicating at 10/100 Mbps on a TCP/IP trunk. The ANSI / ASHRAE™ Standard 135-2008, BACnet protocol is required to assure that the project is fully supported by the leading HVAC open protocol to reduce future building maintenance, upgrade, and expansion costs.

M. LonTalk™ packets may be encapsulated into TCP/IP messages to take advantage of existing infrastructure or to increase network bandwidth where necessary or desired.
   - Any such encapsulation of the LonTalk™ protocol into IP datagrams shall conform to existing LonMark™ guide functionality lines for such encapsulation and shall be based on industry standard protocols.
   - The products used in constructing the BMS shall be LonMark™ compliant.
   - In those instances in which Lon-Mark™ devices are not available, the BMS contractor shall provide device resource files and external interface definitions for LonMark devices.

N. The software tools required for network management of the LonTalk™ protocol and the ANSI / ASHRAE™ Standard 135-2008, BACnet protocol must be provided with the system. Drawings are diagrammatic only. Equipment and labor not specifically referred to herein or on the plans and are required to meet the functional intent, shall be provided without additional cost to the Owner. Minimum BACnet compliance is Level 4; with the ability to support data read and write functionality. Physical connection of BACnet devices shall be via Ethernet IP or MS/TP. Physical connection of LonWorks devices shall be via Ethernet IP or FTT-10A.

O. The system shall support Modbus TCP and RTU protocols natively, and not require the use of gateways.

P. The field bus shall support the use of wireless communications.

Q. Complete temperature control system to be DDC with electronic sensors and electronic/electric actuation of Mechanical Equipment Room (MER) valves and dampers and electronic actuation of terminal equipment valves and actuators as specified herein. The BAS is intended to seamlessly connect devices throughout the building regardless of subsystem type, i.e. variable frequency drives, low voltage lighting systems, electrical circuit breakers, power metering and card access should easily coexist on the same network channel.
   - The supplied system must incorporate the ability to access all data using Java and HTML5 enabled browsers without requiring proprietary operator interface and configuration programs.
   - A hierarchical topology is required to assure reasonable system response times and to manage the flow and sharing of data without unduly burdening the customer's internal Intranet network.

R. Provide the Commissioning, configuration and diagnostic tool (CCDT), color display personnel computer, software, and interfaces to provide uploading/downloading of High Point Count Controllers (AAC), Unitary Equipment Controllers (UEC) and VAV controllers

	(VAVDDC) monitoring all BACnet objects, monitoring overrides of all controller physical input/output points, and editing of controller resident time schedules. S. Provide a Portable Operator's Terminal (POT) color display personnel computer, software, and interfaces to provide uploading/downloading of Custom Application Controller and Application Specific Controllers databases, monitoring of all LonMark™ Standard Network Variables Types (SNVTs) including display of all bound SNVTs, monitoring and overrides of all controller physical input/output points, and editing of controller resident time schedules. POT connectivity shall be via digital wall sensor connected to controller. T. Deployed system must satisfy system requirements to meet DIARMF (U.S. Department of Defense Information Assurance Risk Management Framework) compliance. Only exception is if system is employing a PEMS system such as described in subsection 1.6 Q. below. U. The system shall have the capability to provide a web-based AFDD (automated fault detection and diagnostic) system. The AFDD system shall be able to interface directly with the project BAS and energy/performance metering system to provide information on HVAC systems that are being controlled. Pricing is to be a separate line item from the BAS proposal. See specification section 25 08 01 for exact requirements. V. The system shall have the capability to provide a web-based APEO (automated predictive energy optimization) system and enable effective participation in local utility Demand Response (DR) programs. The vendor shall provide software and ongoing services that will identify actionable energy saving and peak reduction opportunities to assist the facility in achieving its energy and sustainability objectives, and automatically and continuously operate the systems necessary to achieve the targeted savings and reductions. W. The system shall have the capability to provide a web-enabled PEMS (power and energy management system) monitoring system intended to monitor an entire electrical distribution infrastructure, from incoming utility feeds down to low voltage distribution points. It shall be designed to monitor and manage energy consumption throughout an enterprise, whether within a single facility or across a network of facilities, to improve energy availability and reliability, and to measure and manage energy efficiency. It shall be a standard product offering with no custom programming required. It shall provide a seamless user experience ("Single pane of glass") for managing the mechanical systems (HVAC and lighting) and monitoring the power distribution system (transformers, breakers, relays, switches, capacitors, UPS, invertors, etc.)
	BAS -System Architecture X.General 1. The Building Automation System (BAS) shall consist of Network Server/Controllers (NSCs), a family of Standalone Digital Control Units (SDCUs), Administration and Programming Workstations (APWs), and Web-based Operator Workstations (WOWs). The BAS shall provide control, alarm detection, scheduling, reporting and information management for the entire facility, and Wide Area Network (WAN) if applicable. 2. An Enterprise Level BAS shall consist of an Enterprise Server, which enables multiple NSCs (including all graphics, alarms, schedules, trends, programming, and configuration) to be accessible from a single Workstation simultaneously for operations and engineering tasks. 3. The Enterprise Level BAS shall be able to host up to 250 servers, or NSCs, beneath it. 4. For Enterprise reporting capability and robust reporting capability outside of the trend chart and listing ability of the Workstation, a Reports Server shall be installed on a Microsoft Windows based computer. The Reports Server can be installed on the same computer as the Enterprise Server.

5. The system shall be designed with a top-level 10/100bT Ethernet network, using the BACnet/IP, LonWorks IP, and/or Modbus TCP protocol.
6. Modbus RTU/ASCII (and J-bus), Modbus TCP, BACnet MS/TP, BACnet IP, LonTalk FTT-10A, and WebServices shall be native to the NSCs. There shall not be a need to provide multiple NSCs to support all the network protocols, nor should there be a need to supply additional software to allow all three protocols to be natively supported. A sub-network of SDCUs using the BACnet MS/TP, LonTalk FTT-10A, and/or Modbus RTU protocol shall connect the local, stand-alone controllers with Ethernet-level Network Server Controllers/IP Routers.

Y.TCP/IP Level

1. The TCP/IP layer connects all of the buildings on a single Wide Area Network (WAN) isolated behind the campus firewall. Fixed IP addresses for connections to the campus WAN shall be used for each device that connects to the WAN.

Z. Fieldbus Level with Standalone Digital Control Units (SDCUs)

1. The fieldbus layer shall support all of the following types of SDCUs:
   a. BACnet SDCU requirements: The system shall consist of one or more BACnet MS/TP field buses managed by the Network Server Controller. Minimum speed shall be 76.8kbps. The field bus layer consists of an RS485, token passing bus that supports up to 127 Standalone Digital Control Units (SDCUs) for operation of HVAC and lighting equipment. These devices shall conform to BACnet standard 135-2007. The NSCs shall be capable of at least two BACnet MS/TP field buses for a total capability of 254 SDCUs per NSC.
   b. LonWorks SDCU requirements: The system shall consist of one or more LonWorks FTT-10A field buses managed by the Network Server Controller. Minimum speed shall be 76.8kbps. The field bus layer shall consist of up to 64 Lonworks SDCUs using peer-to-peer, event-driven communication for operation of HVAC and lighting equipment.
   c. Modbus SDCU requirements: The system shall consist of one or more Modbus RTU (RS-485 or RS-232) field buses managed by the Network Server Controller. The field bus layer shall consist of up to 31 SDCUs for operation of HVAC, power metering, and lighting equipment. If utilizing Modbus TCP, the field bus layer shall consist of up to 100 SDCUs for operation of HVAC, power metering, and lighting equipment. The NSCs shall be capable of at least two Modbus RTU field buses for a total capability of 62 SDCUs per NSC.
   d. NETWORK 8000 SDCU requirements: The system shall consist of one or more ASD or LCM field buses managed by the Network Server Controller. The field bus layer shall consist of up to 128 ASD SDCUs or 31 LCM SDCUs for operation of HVAC, power metering, and lighting equipment.
   e. I/NET SDCU requirements: The system shall consist of one or more controller LANs and subLANs managed by the Network Server Controller. The network shall consist of up to 100,000 I/NET points capable through numerous links and devices for operation of HVAC, power metering, and lighting equipment.

AA. BAS LAN Segmentation

1. The BAS shall be capable of being segmented, through software, into multiple local area networks (LANs) distributed over a wide area network (WAN). Workstations can manage a single LAN (or building), and/or the

entire system with all portions of that LAN maintaining its own, current database.

BB. Standard Network Support

1. All NSCs, Workstation(s) and Servers shall be capable of residing directly on the owner's Ethernet TCP/IP LAN/WAN with no required gateways. Furthermore, the NSC's, Workstation(s), and Server(s) shall be capable of using standard, commercially available, off-the-shelf Ethernet infrastructure components such as routers, switches and hubs. With this design the owner may utilize the investment of an existing or new enterprise network or structured cabling system. This also allows the option of the maintenance of the LAN/WAN to be performed by the owner's Information Systems Department as all devices utilize standard TCP/IP components.

CC. System Expansion

1. The BAS system shall be scalable and expandable at all levels of the system using the same software interface, and the same TCP/IP level and fieldbus level controllers. Systems that require replacement of either the workstation software or field controllers in order to expand the system shall not be acceptable.
2. Web-based operation shall be supported directly by the NSCs and require no additional software.
3. The system shall be capable of using graphical and/or line application programming language for the Network Server Controllers.

DD. Support For Open Systems Protocols

1. All Network Server Controllers must natively support the BACnet IP, BACnet MS/TP, LonWorks FTT-10, Modbus TCP, Modbus RTU (RS-485 and RS-232), and Modbus ASCII protocols.

Operator Workstation Requirements

EE. General

1. The operator workstation portion of the BAS shall consist of one or more full-powered configuration and programming workstations, and one or more web-based operator workstations. For this project provide a minimum of 10 concurrent operator users and/or 2 concurrent engineering users within the enterprise server.
2. The programming and configuration workstation software shall allow any user with adequate permission to create and/or modify any or all parts of the NSC and/or Enterprise Server database.

FF. General Administration and Programming Workstation Software

1. System architecture shall be truly client server in that the Workstation shall operate as the client while the NSCs shall operate as the servers. The client is responsible for the data presentation and validation of inputs while the server is responsible for data gathering and delivery.
2. The workstation functions shall include monitoring and programming of all DDC controllers. Monitoring consists of alarming, reporting, graphic displays, long term data storage, automatic data collection, and operator-initiated control actions such as schedule and set point adjustments.
3. Programming of SDCUs shall be capable of being done either off-line or on-line from any operator workstation. All information will be available in graphic or text displays stored at the NSC. Graphic displays will feature animation effects to enhance the presentation of the data, to alert

operators of problems, and to facilitate location of information throughout the DDC system. All operator functions shall be selectable through a mouse.

GG. User Interface:

1. The BAS workstation software shall allow the creation of a custom, browser-style interface linked to the user when logging into any workstation. Additionally, it shall be possible to create customized workspaces that can be assigned to user groups. This interface shall support the creation of "hot-spots" that the user may link to view/edit any object in the system or run any object editor or configuration tool contained in the software. Furthermore, this interface must be able to be configured to become a user's "PC Desktop" – with all the links that a user needs to run other applications. This, along with the Windows user security capabilities, will enable a system administrator to setup workstation accounts that not only limit the capabilities of the user within the BAS software, but may also limit what a user can do on the PC and/or LAN/WAN. This might be used to ensure, for example, that the user of an alarm monitoring workstation is unable to shutdown the active alarm viewer and/or unable to load software onto the PC.
2. System shall be able to automatically switch between displayed metric vs. imperial units based on the workstation/web stations localization.
3. Web stations shall have the capability to automatically re-direct to an HTTPS connection to ensure more secure communications.
4. Personalized layouts and panels within workstations shall be extended to web stations to ensure consistent user experiences between the two user interfaces.
5. Servers and clients shall have the ability to be located in different time zones, which are then synchronized via the NTP server.
6. Workstation shall indicate at all times the communication status between it and the server.

HH. User Security

1. The software shall be designed so that each user of the software can have a unique username and password. This username/password combination shall be linked to a set of capabilities within the software, set by and editable only by, a system administrator. The sets of capabilities shall range from View only, Acknowledge alarms, Enable/disable and change values, Program, and Administer. The system shall allow the above capabilities to be applied independently to each and every class of object in the system. The system must allow a minimum of 256 users to be configured per workstation. Additionally, the software shall enable the ability to add/remove users.
2. Additional requirements include mandatory change of passwords:
    a) At first logon with default credentials
    b) Of admin passwords before deploying via Project Configuration Servers

II. Automatic monitoring

1. The software shall allow for the automatic collection of data and reporting from any controller or NSC. The frequency of data collection shall be user-configurable.

JJ. Alarm Management

1. The software shall be capable of accepting alarms directly from NSCs or controllers, or generating alarms based on evaluation of data in

controllers and comparing to limits or conditional equations configured through the software. Any alarm (regardless of its origination) will be integrated into the overall alarm management system and will appear in all standard alarm reports, be available for operator acknowledgment, and have the option for displaying graphics, or reports.

2. Alarm management features shall include:
   a. A minimum of 1000 alarm notification levels at the NSC, workstation, and web station levels. At the Enterprise level the minimum number of active and viewable alarms shall be 10,000. Each notification level will establish a unique set of parameters for controlling alarm display, distribution, acknowledgment, keyboard annunciation, and record keeping.
   b. Automatic logging in the database of the alarm message, point name, point value, source device, timestamp of alarm, username and time of acknowledgement, username and time of alarm silence (soft acknowledgement).
   c. Playing an audible sound on alarm initiation or return to normal.
   d. Sending an email page to anyone specifically listed on the initial occurrence of an alarm. The ability to utilize email paging of alarms shall be a standard feature of the software integrated with the operating system's mail application interface (MAPI). No special software interfaces shall be required and no email client software must be running in order for email to be distributed. The email notification shall be able to be sent to an individual user or a user group.
   e. Individual alarms shall be able to be re-routed to a user at user-specified times and dates. For example, a critical high temp alarm can be configured to be routed to a Facilities Dept. workstation during normal working hours (7am-6pm, Mon-Fri) and to a Central Alarming workstation at all other times.
   f. An active alarm viewer shall be included which can be customized for each user or user type to hide or display any alarm attributes.
   g. The active alarm viewer can be configured such that an operator must type in text in an alarm entry and/or pick from a drop-down list of user actions for certain alarms.
   h. The active alarm viewer can be configured such that an operator must type in text in an alarm entry and/or pick from a drop-down list of causes for certain alarms. This ensures accountability (audit trail) for the response to critical alarms.
   i. The active alarm viewer can be configured such that an operator must confirm that all of the steps in a check list have been accomplished prior to acknowledging the alarm.
   j. The active alarm viewer shall, if filtered, show the quantity of visible and total number of alarms that are not equal to 'normal' and the quantity of disabled and hidden alarms.
   k. An operator shall have the capability to assign an alarm to another user of the system.
   l. Time schedules shall be able to be used to set control notifications to users.
   m. An operator shall have the capability to save and apply alarm favorites.

KK. Report Generation

1. The Reports Server shall be able to process large amounts of data and produce meaningful reports to facilitate analysis and optimization of each installation.
2. Reports shall be possible to generate and view from the operator Workstation, and/or Webstation, and/or directly from a reports-only web interface.
3. A library of predefined automatically generated reports that prompt users for input prior to generation shall be available. The properties and configurations made to these reports shall be possible to save as Dashboard reports, so that the configurations are saved for future used.
4. It shall be possible to create reports standard tools, such as Microsoft Report Builder 2.0 or Visual Studio, shall be used for customized reports.
5. Additional reports or sets of reports shall be downloadable, transferrable, and importable
6. All reports shall be able to be set up to automatically run or be generated on demand.
7. Each report shall be capable of being automatically emailed to a recipient in Microsoft Word, Excel, and/or Adobe .pdf format.
8. Reports can be of any length and contain any point attributes from any controller on the network.
9. Image management functionality shall be possible to enable the system administrators to easily upload new logos or images to the system.
10. It shall be possible to run other executable programs whenever a report is initiated.
11. Report Generator activity can be tied to the alarm management system, so that any of the configured reports can be displayed in response to an alarm condition.
12. Minimum supplied reports shall include:
    a. Activities Per Server Report
    b. Activities Per User Report
    c. Alarm Amount by Category Report
    d. Alarm Amount by Type Report
    e. Alarms Per Sever Report
    f. Current Alarm Report
    g. Most Active Alarm Report
    h. System Errors Per Server Report
    i. Top Activities Report
    j. Top Alarms Report
    k. Top System Errors Report
    l. Trend Log Comparison Report
    m. User Logins Report
    n. Users and Groups Reports
13. Minimum Energy Reports shall include:
    a. Energy Monitoring Calendar Consumption Report: Shall provide an interactive report that shows the energy usage on one or multiple selected days.
    b. Energy Monitoring Consumption Breakdown Report: Shall provide a report on energy consumption broken down using sub-metering.
    c. Energy Monitoring Consumption Report: Shall show the energy consumption against a specified target value.

LL. Scheduling

1. From the workstation or webstation, it shall be possible to configure and download schedules for any of the controllers on the network.
2. Time of day schedules shall be in a calendar style and viewable in both a graphical and tabular view.
3. Schedules shall be programmable for a minimum of one year in advance.
4. To change the schedule for a particular day, a user shall simply select the day and make the desired modifications.
5. Additionally, from the operator web stations, each schedule will appear on the screen viewable as the entire year, monthly, week and day. A simple mouse click shall allow switching between views. It shall also be possible to scroll from one month to the next and view or alter any of the schedule times.
6. Schedules will be assigned to specific controllers and stored in their local RAM memory. Any changes made at the workstation will be automatically updated to the corresponding schedule in the controller.
7. It shall be possible to assign a lead schedule such that shadow/local schedules are updated based upon changes in the Lead.
8. It shall be possible to assign a list(s) of exception event days, dates, date ranges to a schedule.
9. It shall be possible to view combined views showing the calendar and all prioritized exemptions on one screen.
10. It should accommodate a minimum of 16 priority levels.
11. Values should be able to be controlled directly from a schedule, without the need for special program logic.

MM. Saving/Reloading

1. The workstation software shall have an application to save and restore NSC and field controller memory files.
2. For the NSC, this application shall not be limited to saving and reloading an entire controller – it must also be able to save/reload individual objects in the controller. This allows off-line debugging of control programs, for example, and then reloading of just the modified information.

NN. Audit Trail

1. The workstation software shall automatically log and timestamp every operation that a user performs at a workstation, from logging on and off a workstation to changing a point value, modifying a program, enabling/disabling an object, viewing a graphic display, running a report, modifying a schedule, etc.
2. It shall be possible to view a history of alarms, user actions, and commands for any system object individually or at least the last 5000 records of all events for the entire system from Workstation.
3. The Enterprise server shall be able to store up to 5 million events.
4. It shall be possible to save custom filtered views of event information that are viewable and configurable in Workstation.
5. It shall be capable to search and view all forced values within the system.

OO. Fault Tolerant Enterprise Server Operation (Top level NSC)

1. A single component failure in the system shall not cause the entire system to fail. All system users shall be informed of any detectable component failure via an alarm event. System users shall not be logged off as a result of a system failure or switchover.

PP. Web-based Operator Software

	1. General: a. Day-to-day operation of the system shall be accessible through a standard web browser interface, allowing technicians and operators to view any part of the system from anywhere on the network. b. The system shall be able to be accessed on site via a mobile device environment with, at a minimum, access to overwrite and view system values. 2. Graphic Displays a. The browser-based interface must share the same graphical displays as the Administration and Programming Workstations, presenting dynamic data on site layouts, floor plans, and equipment graphics. The browser's graphics shall support commands to change set points, enable/disable equipment and start/stop equipment. b. Through the browser interface, operators must be able to navigate through the entire system, and change the value or status of any point in any controller. Changes are effective immediately to the controller, with a record of the change stored in the system database. 3. Alarm Management a. Systems requiring additional client software to be installed on a PC for viewing the web station from that PC will not be considered. b. Through the browser interface, a live alarm viewer identical to the alarm viewer on the Administration and Programming workstation shall be presented, if the user's password allows it. Users must be able to receive alarms, silence alarms, and acknowledge alarms through a browser. If desired, specific operator text must be able to be added to the alarm record before acknowledgement, attachments shall be viewable, and alarm checklists shall be available. QQ. Groups and Schedules 1. Through the browser interface, operators must be able to view pre-defined groups of points, with their values updated automatically. 2. Through the browser interface, operators must be able to change schedules – change start and stop times, add new times to a schedule, and modify calendars. RR. User Accounts and Audit Trail 1. The same user accounts shall be used for the browser interface and for the operator workstations. Operators must not be forced to memorize multiple passwords. 2. All commands and user activity through the browser interface shall be recorded in the system's activity log, which can be later searched and retrieved by user, date, or both. SS. Web Services 1. The installed system shall be able to use web services to "consume" Information within the Network Server/Controllers (NSCs) with other products and systems. Inability to perform web services within the NSCs will be unacceptable. 2. Shall be able to "consume" data into the system via SOAP and REST web services.
	Network Server Controllers (NSCs)-DDC Panel TT. Network Router Controllers shall combine both network routing functions, control functions, and server functions into a single unit.

UU. The BACnet NSC shall be classified as a "native" BACnet device, supporting the BACnet Network Server Controller (B-BC) profile. Controllers that support a lesser profile such as B-SA are not acceptable. NSCs shall be tested and certified by the BACnet Testing Laboratory (BTL) as BACnet Network Server Controllers (B-BC).

VV. The Network Server Controller shall provide the interface between the LAN or WAN and the field control devices, and provide global supervisory control functions over the control devices connected to the NRS.

WW. The NSCs shall be capable of whitelisting IPs to restrict access to a pre-defined list of hosts or devices.

XX. They shall also be responsible for monitoring and controlling their own HVAC equipment such as an AHU or boiler.

YY. They shall also contain graphics, trends, trend charts, alarm views, and other similar presentation objects that can be served to workstations or web-based interfaces. A sufficient number of NSCs shall be supplied to fully meet the requirements of this specification and the attached point list.

ZZ. It shall be capable of executing application control programs to provide:

1. Calendar functions
2. Scheduling
3. Trending
4. Alarm monitoring and routing
5. Time synchronization by means of an Internet site including automatic synchronization
6. Native integration of LonWorks controller data and Modbus controller data or BACnet controller data and Modbus controller data
7. Network Management functions for all LonWorks based devices

AAA. Hardware Specifications

1. Memory:
   a. The operating system of the controller, application programs, and all other portions of the configuration database, shall be stored in non-volatile, FLASH memory. Servers/Controllers shall contain enough memory for the current application, plus required history logging, plus a minimum of 20% additional free memory.
2. Each NRC shall provide the following on-board hardware for communication:
   a. One 10/100bT Ethernet for communication to Workstations, other NRCs and onto the Internet
   b. Two RS-485 ports for communication to BACnet MSTP bus or serial Modbus (software configurable)
   c. One TP/FT port for communication to LonWorks devices.
   d. One device USB port
   e. One host USB port
3. The NSC shall conform to a small footprint no larger than 100W x 125H x 75D mm (3.94W x 4.92H x 2.95D in).

BBB. Modular Expandability:

1. The system shall employ a modular I/O design to allow expansion. Input and output capacity is to be provided through plug-in modules of various types. It shall be possible to combine I/O modules as desired to meet the I/O requirements for individual control applications.
2. One shall be able to "hot-change" (hot-swap) the I/O modules preserving the system on-line without any intervention on the software; addressing and configuration shall be automatic.

3. If for any reason the backplane of the modular I/O system were to fail, I/O module addresses will be protected.

CCC. Hardware Override Switches:

1. All digital outputs shall, optionally, include three position manual override switches to allow selection of the ON, OFF, or AUTO output state. These switches shall be built into the unit and shall provide feedback to the controller so that the position of the override switch can be obtained through software. In addition each analog output shall be equipped with an override potentiometer to allow manual adjustment of the analog output signal over its full range, when the 3 position manual override switch is placed in the ON position.

DDD. Universal Input Temperatures

1. All universal inputs directly connected to the NSC via modular expansion shall be capable of using the following thermistors for use in the system without any external converters needed.
   1) 10 kohm Type I (Continuum)
   2) 10 kohm Type II (I/NET)
   3) 10 kohm Type III (Satchwell)
   4) 10 kohm Type IV (FD)
   5) Linearized 10 kohm Type V (FD w/11k shunt)
   6) Linearized 10 kohm (Satchwell)
   7) 1.8 kohm (Xenta)
   8) 1 kohm (Balco)
   9) 20 kohm (Honeywell)
   10) 2.2 kohm (Johnson)
2. In addition to the above, the system shall be capable of using the below RTD sensors, however it is not required that all universal inputs be compatible with them.
   1) PT100 (Siemens)
   2) PT1000 (Sauter)
   3) Ni1000 (Danfoss)

EEE. Local Status Indicator Lamps:

1. The NSC shall provide as a minimum LED indication of CPU status, Ethernet LAN status, and field bus status. For each input or output, provide LED indication of the value of the point (On/Off). The LED indication shall support software configuration to set whether the illumination of the LED corresponds to On or Off or whether the color when illuminated is Red or Green.

FFF. Real Time Clock (RTC):

1. Each NSC shall include a real time clock, accurate to 10 seconds per day. The RTC shall provide the following: time of day, day, month, year, and day of week. Each NSC will allow for its own UTC offset, depending upon the time zone. When the time zone is set, the NSC will also store the appropriate times for daylight savings time.
2. The RTC date and time shall also be accurate, up to 30 days, when the NSC is powerless.
3. No batteries may be used to for the backup of the RTC.

GGG. Power Supply:

1. The 24 VDC power supply for the NSCs shall provide 30 watts of available power for the NSC and associated IO modules. The system shall support the use of more than one power supply if heavily power consuming modules are required.

2. The power supply, NSC, and I/O modules shall connect power wise and communication wise via the separate terminal base allowing for ease of replacement and no separate or loose wiring.

HHH. Automatic Restart After Power Failure:

1. Upon restoration of power after an outage, the NSC shall automatically and without human intervention update all monitored functions, resume operation based on current, synchronize time and status, and implement special start-up strategies as required.

III. Data Retention:

1. During a power failure, the NSC shall retain all programs, configuration data, historical data, and all other data that is configured to be retained. There shall be no time restriction for this retention and it must not use batteries to achieve it.

JJJ. Software Specifications

1. The operating system of the controller, application programs, and all other portions of the configuration database such as graphics, trends, alarms, views, etc., shall be stored in non-volatile, FLASH memory. There will be no restrictions placed on the type of application programs in the system. Each NSC shall be capable of parallel processing, executing all control programs simultaneously. Any program may affect the operation of any other program. Each program shall have the full access of all I/O facilities of the processor. This execution of control function shall not be interrupted due to normal user communications including interrogation, program entry, printout of the program for storage, etc.
2. Each NSC shall have an available capacity of 4 GB of memory. This shall represent 2 GB for application and historical data and 2 GB dedicated for backup storage.

KKK. User Programming Language:

1. The application software shall be user programmable. This includes all strategies, sequences of operation, control algorithms, parameters, and set points. The source program shall be either a script-based structured text or graphical function block based and fully programmable by the user. The language shall be structured to allow for the configuration of control programs, schedules, alarms, reports, telecommunications, local displays, mathematical calculations, and histories. Users shall be able to place comments anywhere in the body of either script or function block programs.
2. Network Server Controllers that use a “canned” program method will not be accepted.

LLL. Control Software:

1. The NSC shall have the ability to perform the following pre-tested control algorithms:
   a. Proportional, Integral plus Derivative Control (PID)
   b. Two Position Control
   c. Digital Filter
   d. Ratio Calculator
   e. Equipment Cycling Protection

MMM. Mathematical Functions:

1. Each controller shall be capable of performing basic mathematical functions (+, -, *, /), squares, square roots, exponential, logarithms, Boolean logic statements, or combinations of both. The controllers shall be capable of performing complex logical statements including operators

such as >, <, =, and, or, exclusive or, etc. These must be able to be used in the same equations with the mathematical operators and nested up to five parentheses deep.

NNN. NSCs shall have the ability to perform any or all of the following energy management routines:

1. Time of Day Scheduling
2. Calendar Based Scheduling
3. Holiday Scheduling
4. Temporary Schedule Overrides
5. Optimal Start
6. Optimal Stop
7. Night Setback Control
8. Enthalpy Switchover (Economizer)
9. Peak Demand Limiting
10. Temperature Compensated Duty Cycling
11. CFM Tracking
12. Heating/Cooling Interlock
13. Hot/Cold Deck Reset
14. Hot Water Reset
15. Chilled Water Reset
16. Condenser Water Reset
17. Chiller Sequencing

OOO. History Logging:

1. Each NSC controller shall be capable of LOCALLY logging any input, output, calculated value or other system variable either over user defined time intervals ranging from 1 second to 1440 minutes or based upon a user configurable change of value. A minimum of 1000 logs, with a minimum of 100,000 records, shall be stored. Each log can record either the instantaneous, average, minimum or maximum value of the point. Logged data shall be downloadable to a higher level NSC long term archiving based upon user-defined time intervals, or manual command.
2. For extended trend logging a minimum of 1500 trends shall be capable, with a minimum number of 600,000 records within.
3. Management of a power meter replacement to ensure meter log data is accurate shall be possible in the NSC.
4. Every hardware input and output point, hosted within the NSC and attached I/O modules, shall be trended automatically without the requirement for manual creation, and each of these logs shall log values based upon a change of value and store at least 500 trend samples before replacing the oldest sample with new data.
5. The presentation of logged data shall be built into the server capabilities of the NSC. Presentation can be in time stamped list formats or in a chart format with fully configurable pen colors, weights, scales and time spans.
6. Tooltips shall be present, magnetic, and visible based on users preference.
7. Comments shall be visible whenever viewing the trend log list.

PPP. Alarm Management:

1. For each system point, alarms can be created based on high/low limits or in comparison to other point values. All alarms will be tested each scan of the NSC and can result in the display of one or more alarm messages or reports.

2. There is no limit to the number of alarms that can be created for any point
3. Alarms can be configured to be generated based upon a single system condition or multiple system conditions.
4. Alarms will be generated based on an evaluation of the alarm conditions and can be presented to the user in a fully configurable order, by priority, by time, by category, etc. These configurable alarm views will be presented to a user upon logging into the system regardless of whether the log in takes place at a WorkStation or a Webstation.
5. The alarm management system shall support the ability to create and select cause and action notes to be selected and associated with an alarm event. Checklists shall also be possible in order to present to an operator a suggested mode of troubleshooting. When acknowledging an alarm, it shall be possible to assign it to a user of the system such that the user is notified of the assignment and is made responsible for the alarm resolution.
6. Alarms must be capable of being routed to any BACnet workstation that conforms to the B-OWS device profile and uses the BACnet/IP protocol.

QQQ. Embedded Web Server

1. Each NSC must have the ability to serve out web pages containing the same information that is available from the WorkStation. The development of the screens to accomplish shall not require any additional engineering labor over that required to show them at the WorkStation itself.

BACnet Fieldbus and BACnet SDCUs –DDC panel

RRR. Networking

1. IP Network: All devices that connect to the WAN shall be capable of operating at 10 megabits per second or 100 megabits per second.
2. IP To Field Bus Routing Devices
   a. A Network Server Controller shall be used to provide this functionality.
   b. These devices shall be configurable locally with IP crossover cable and configurable via the IP network.
   c. The routing configuration shall be such that only data packets from the field bus devices that need to travel over the IP level of the architecture are forwarded.

SSS. Field Bus Wiring and Termination

1. The wiring of components shall use a bus or daisy chain concept with no tees, stubs, or free topology.
2. Each field bus shall have a termination resistor at both ends of each segment.
3. The field bus shall support the use of wireless communications.

TTT. Repeaters

1. Repeaters are required to connect two segments.
2. Repeaters shall be installed in an enclosure. The enclosure may be in an interstitial space.

UUU. Field Bus Devices

1. General Requirements
   a. Devices shall have a light indicating that they are powered.

b. Devices shall be locally powered. Link powered devices (power is furnished from a central source over the field bus cable) are not acceptable.
c. Application programs shall be stored in a manner such that a loss of power does not result in a loss of the application program or configuration parameter settings. (Battery backup, flash memory, etc.)

VVV. Network Server Controllers (NSCs)

a. If NSCs have embedded I/O, all of the requirements for I/O that are described under Advance Application Controllers shall apply.
b. Shall support the export of data to NSCs from other vendors that support the data sharing, read property service.
c. Shall support the export of data using Change of Value (COV) initiation to NSCs from other vendors that support the subscription to data using the COV concept.
d. Shall support the export of data to any BACnet OWS that supports the data sharing, read property service.
e. Shall support the export of data using Change of Value (COV) initiation to any BACnet OWS that supports the subscription to data using the COV concept.
f. Shall provide trend log support for all of the devices on the field bus. They shall provide sufficient memory to store up to 300 samples for each variable required to be trended by the sequence of control.
g. Shall support the exporting of trend log data to any BACnet OWS that supports the read range BACnet service for trending.
h. Shall provide time schedule support for all of the devices on the field bus.
i. Shall support the editing of time schedule entries from any BACnet OWS that supports the BACnet service for writing of time schedule parameters.
j. Shall provide alarm message initiation for all alarms conditions from any of the field bus devices.
k. Shall deliver alarm messages to any BACnet OWS that supports the BACnet service for receiving alarm messages and is configured to be a recipient of the notification.
l. Shall support alarm acknowledgement from any BACnet OWS that supports the BACnet service for executing alarm/event acknowledgement.
m. Shall support the control of the out of service property and assignment of value or state to analog and binary objects from any BACnet OWS that supports writing to the out of service property and the value property of analog and binary objects.
n. Shall support the receipt and response to Time Synchronization commands from any device that supports the BACnet service for initiating time synchronization commands.
o. Shall support the “Who is?” and “I am.” BACnet service.
p. Shall support the “”Who has?” and “I have.” BACnet service.
q. Shall support Backup and Restore commands from any BACnet OWS that supports the initiation of Backup and Restore commands.
r. Shall be BTL certified.

WWW. Advance Application Controllers (B-AAC)

1. The key characteristics of a B-AAC are:
   a. They have physical input and output circuits for the connection of analog input devices, binary input devices, pulse input devices, analog output devices, and binary output devices. The number and type of input and output devices supported will vary by model.
   b. They may or may not provide support for additional input and output devices beyond the number of circuits that are provided on the basic circuit board. Support for additional I/O shall be provided by additional circuit boards that physically connect to the basic controller.
   c. The application to be executed by a B-AAC is created by an application engineer using the vendor's application programming tool.
   d. If local time schedules are embedded, the B-AAC shall support the editing of time schedule entries from any BACnet OWS that supports the BACnet service for writing of time schedule parameters.
   e. If local trend logging is embedded, the B-AAC shall support the exporting of trend log data to any BACnet OWS that supports the read range BACnet service for trending.
   f. If local alarm message initiation is embedded, the B-AAC shall:
      1) Deliver alarm messages to any BACnet OWS that supports the BACnet service for receiving alarm messages and is configured to be a recipient off the alarm message.
      2) Support alarm acknowledgement from any BACnet OWS that supports the BACnet service for executing alarm/event acknowledgement,
   g. Shall support the reading of analog and binary data from any BACnet OWS or Building Controller that supports the BACnet service for the reading of data.
   h. Shall support the control of the out of service property and assignment of value or state to analog and binary objects from any BACnet OWS that supports writing to the out of service property and the value property of analog and binary objects.
   i. Shall support the receipt and response to Time Synchronization commands from a BACnet Building Controller.
   j. Shall support the "Who is" and "I am." BACnet services.
   k. Shall support the "Who has" and "I have." BACnet services.
2. Analog Input Circuits
   a. The resolution of the A/D chip shall not be greater than 0.01 Volts per increment. For an A/D converter that has a measurement range of 0 to 10 VDC and is 10 bit, the resolution is 10/1024 or 0.00976 Volts per increment.
   b. For non-flow sensors, the control logic shall provide support for the use of a calibration offset such that the raw measured value is added to the (+/-) offset to create a calibration value to be used by the control logic and reported to the Operator Workstation (OWS).
   c. For flow sensors, the control logic shall provide support for the use of an adjustable gain and an adjustable offset such that a two point calibration concept can be executed (both a low range value and a high range value are adjusted to match values determined by a calibration instrument).

d. For non-linear sensors such as thermistors and flow sensors the B-AAC shall provide software support for the linearization of the input signal.

3. Binary Input Circuits
   a. Dry contact sensors shall wire to the controller with two wires.
   b. An external power supply in the sensor circuit shall not be required.
4. Pulse Input Circuits
   a. Pulse input sensors shall wire to the controller with two wires.
   b. An external power supply in the sensor circuit shall not be required.
   c. The pulse input circuit shall be able to process up to 20 pulses per second.
5. True Analog Output Circuits
   a. The logical commands shall be processed by a digital to analog (D/A) converter chip. The 0% to 100% control signal shall be scalable to the full output range which shall be either 0 to 10 VDC, 4 to 20 milliamps or 0 to 20 milliamps or to ranges within the full output range (Example: 0 to 100% creates 3 to 6 VDC where the full output range is 0 to 10 VDC).
   b. The resolution of the D/A chip shall not be greater than 0.04 Volts per increment or 0.08 milliamps per increment.
6. Binary Output Circuits
   a. Single pole, single throw or single pole, double throw relays with support for up to 230 VAC and a maximum current of 2 amps.
   b. Voltage sourcing or externally powered triacs with support for up to 30 VAC and 0.5 amps at 24 VAC.
7. Program Execution
   a. Process control loops shall operate in parallel and not in sequence unless specifically required to operate in sequence by the sequence of control.
   b. The sample rate for a process control loop shall be adjustable and shall support a minimum sample rate of 1 second.
   c. The sample rate for process variables shall be adjustable and shall support a minimum sample rate of 1 second.
   d. The sample rate for algorithm updates shall be adjustable and shall support a minimum sample rate of 1 second.
   e. The application shall have the ability to determine if a power cycle to the controller has occurred and the application programmer shall be able to use the indication of a power cycle to modify the sequence of controller immediately following a power cycle.
8. Local Interface
   a. The controller shall support the connection of a portable interface device such as a laptop computer or vendor unique hand-held device. The ability to execute any tasks other than viewing data shall be password protected. Via this local interface, an operator shall be able to:
      1) Adjust application parameters.
      2) Execute manual control of input and output points.
      3) View dynamic data.

XXX. Application Specific Devices

	1. Application specific devices shall have fixed function configurable applications. 2. If the application can be altered by the vendor's application programmable tool, the device is an advanced application controller and not an application specific device. 3. Application specific devices shall be BTL certified.
	DDC Sensors and Point Hardware YYY. Temperature Sensors 1. All temperature devices shall use precision thermistors accurate to +/- 1 degree F over a range of –30 to 230 degrees F. Space temperature sensors shall be accurate to +/- .5 degrees F over a range of 40 to 100 degrees F. 2. Room Sensor: Standard space sensors shall be available in an [off white] [black] enclosure made of high impact ABS plastic for mounting on a standard electrical box. 1) Where manual overrides are required, the sensor housing shall feature both an optional sliding mechanism for adjusting the space temperature set point, as well as a push button for selecting after hours operation. 2) Where a local display is specified, the sensor shall incorporate an LCD display for viewing the space temperature, set point and other operator selectable parameters. Using built in buttons, operators shall be able to adjust set points directly from the sensor. 3. Duct Probe Sensor: Sensing element shall be fully encapsulated in potting material within a stainless steel probe. Useable in air handling applications where the coil or duct area is less than 14 square feet. 4. Duct Averaging Sensor: Averaging sensors shall be employed in ducts which are larger than 14 square feet. The averaging sensor tube shall contain at least one thermistor for every 3 feet, with a minimum tube length of 6 feet. The averaging sensor shall be constructed of rigid or flexible copper tubing. 5. Pipe Immersion Sensor: Immersion sensors shall be employed for measurement of temperature in all chilled and hot water applications as well as refrigerant applications. Provide sensor probe length suitable for application. Provide each sensor with a corresponding pipe-mounted sensor well, unless indicated otherwise. Sensor wells shall be stainless steel for non-corrosive fluids below 250 degrees F and 300 series stainless steel for all other applications. 6. Outside Air Sensor: Provide the sensing element on the building's north side. Sensing element shall be fully encapsulated in potting material within a stainless steel probe. Probe shall be encased in PVC solar radiation shield and mounted in a weatherproof enclosure. Operating range -40 to 122 F, 7. A pneumatic signal shall not be allowed for sensing temperature. ZZZ. Humidity Wall Transmitter 1. Transmitters shall be accurate to +/- [1] [2] % at full scale. 2. Transmitter shall have replaceable sensing element. 3. Sensor type shall be thin-film capacitive. 4. Sensor element shall contain multipoint calibration on-board in nonvolatile memory 5. Operating range shall be 0 - 100% RH noncondensing, 50 to 95 F

6. Output shall be field selectable 4-20 mA or 0-5/0-10 VDC.
7. Transmitter shall accept 12-30 VDC or 24 VAC supply power.
8. Transmitter shall be available in an [off white] [black] enclosure made of high impact ABS plastic for mounting on a standard electrical box.
9. Transmitter shall have LCD display
10. Transmitter shall be available with a certification of NIST calibration
11. Transmitter shall have integrated temperature sensor

AAAA. Humidity Duct Transmitter

1. Transmitters shall be accurate to +/- [1] [2] % at full scale.
2. Transmitter shall be fully encapsulated in potting material within a stainless steel probe.
3. Transmitter shall have replaceable sensing element.
4. Sensor type shall be thin-film capacitive.
5. Sensor element shall contain multipoint calibration on-board in nonvolatile memory
6. Operating range shall be 0 - 100% RH noncondensing, -40 to 122 F
7. Output shall be 4-20 mA or 0-5/0-10 VDC.
8. Transmitter shall accept 12-30 VDC or 24 VAC supply power.
9. Transmitter shall be available with a certification of NIST calibration
10. Transmitter shall have integrated temperature sensor

BBBB. Humidity Outdoor Transmitter

1. Transmitters shall be accurate to +/- 2% at full scale.
2. Transmitter shall be fully encapsulated in potting material within a stainless steel probe. Probe shall be encased in PVC solar radiation shield and mounted in a weatherproof enclosure.
3. Transmitter shall have replaceable sensing element.
4. Sensor type shall be thin-film capacitive.
5. Sensor element shall contain multipoint calibration on-board in non-volatile memory
6. Operating range shall be 0 - 100% RH noncondensing, -40 to 122 F
7. Output shall be 4-20 mA or 0-5/0-10 VDC.
8. Transmitter shall accept 12-30 VDC or 24 VAC supply power.
9. Transmitter shall be available with a certification of NIST calibration
10. Transmitter shall have integrated temperature sensor

CCCC. Carbon Dioxide Wall Transmitter:

1. Sensor type shall be Non-dispersive infrared (NDIR).
2. Accuracy shall be ±30 ppm ±2% of measured value with annual drift of ±10 ppm. Minimum five year recommended calibration interval.
3. Repeatability shall be ±20 ppm ±1% of measured value
4. Response Time shall be <60 seconds for 90% step change
5. Outputs shall be field selectable [Analog: 4-20mA or 0-5/0-10VDC] [Protocol: Modbus or BACnet] with [SPDT Relay 1A@30VDC] [temperature setpoint slider]
6. Transmitter shall accept 12-30 VDC or 24 VAC supply power.
7. Temperature Range: [32° to 122°F (CO_2 only)] [50° to 95°F (with humidity option)]
8. Output range shall be programmable 0-2000 or 0-5000 ppm
9. Transmitter shall be available in an [off white] [black] enclosure for mounting on a standard electrical box.

10. Transmitter shall have LCD display for commissioning and provide additional faceplate to conceal LCD display where occupants may misinterpret CO2 readings.
11. Transmitter shall have integrated humidity sensor, temperature sensor

DDDD. Carbon Dioxide Duct Transmitter:

1. Sensor type shall be Non-dispersive infrared (NDIR).
2. Accuracy shall be ±30 ppm ±2% of measured value with annual drift of ±10 ppm. Minimum five year recommended calibration interval.
3. Repeatability shall be ±20 ppm ±1% of measured value
4. Response Time shall be <60 seconds for 90% step change
5. Outputs shall be field selectable Analog: 4-20mA or 0-5/0-10VDC with SPDT Relay 1A@30VDC
6. Transmitter shall accept 12-30 VDC or 24 VAC supply power.
7. Temperature Range: 32° to 122°F
8. Output range shall be programmable 0-2000 or 0-5000 ppm
9. Enclosure shall not require remote pickup tubes and make use of integrated H-beam probe to channel air flow to sensor.
10. Enclosure lid shall require no screws and make use of snap on features for attachment
11. Enclosure shall be made of high impact ABS plastic
12. Transmitter shall have LCD display
13. Transmitter shall have integrated humidity sensor, temperature sensor

EEEE. Air Pressure Transmitters.

1. Sensor shall be microprocessor profiled ceramic capacitive sensing element
2. Transmitter shall have 14 selectable ranges from 0.1 – 10" WC
3. Transmitter shall be +/- 1% accurate in each selected range including linearity, repeatability, hysteresis, stability, and temperature compensation.
4. Transmitter shall be field configurable to mount on wall or duct with static probe
5. Transmitter shall be field selectable for Unidirectional or Bidirectional
6. Maximum operating pressure shall be 200% of design pressure.
7. Output shall be field selectable 4-20 mA or 0-5/0-10 VDC linear.
8. Transmitter shall accept 12-30 VDC or 24 VAC supply power
9. Response time shall be field selectable T95 in 20 sec or T95 in 2 sec
10. Transmitter shall have an LCD display
11. Units shall be field selectable for WC or PA
12. Transmitter shall have provision for zeroing by pushbutton or digital input.
13. Transmitter shall be available with a certification of NIST calibration

FFFF. Liquid Differential Pressure Transmitters:

1. Transmitter shall be microprocessor based
2. Transmitter shall use two independent gauge pressure sensors to measure and calculate differential pressure
3. Transmitter shall have 4 switch selectable ranges
4. Transmitter shall have test mode to produce full-scale output automatically.
5. Transmitter shall have provision for zeroing by pushbutton or digital input.

6. Transmitter shall have field selectable outputs of 0-5V, 0-10V, and 4-20mA.
7. Transmitter shall have field selectable electronic surge damping
8. Transmitter shall have an electronic port swap feature
9. Transmitter shall accept 12-30 VDC or 24 VAC supply power
10. Sensor shall be 17-4 PH stainless steel where it contacts the working fluid.
11. Performance:

a. Accuracy shall be ±1% F.S. and ±2% F.S. for lowest selectable range
b. Long term stability shall be ±0.25%
c. Sensor temperature operating range shall be -4° to 185°F
d. Operating environment shall be 14° to 131°F; 10-90% RH noncondensing
e. Proof pressure shall be 2x max. F.S. range
f. Burst pressure shall be 5x max. F.S. range

12. Transmitter shall be encased in a NEMA 4 enclosure
13. Enclosure shall be white powder-coated aluminum
14. Transmitter shall be available with a certification of NIST calibration
15. [Transmitter shall be preinstalled on a bypass valve manifold]

GGGG. Current Sensors

1. Current status switches shall be used to monitor fans, pumps, motors and electrical loads. Current switches shall be available in split core models, and offer either a digital or an analog signal to the automation system.

HHHH. Current Status Switches for Constant Load Devices

1. General: Factory programmed current sensor to detect motor undercurrent situations such as belt or coupling loss on constant loads. Sensor shall store motor current as operating parameter in non-volatile memory. Push-button to clear memory.
2. Visual LED indicator for status.
3. Split core sensor, induced powered from monitored load and isolated to 600 VAC rms. Sensor shall indicate status from 0.5 A to 175 A.
4. Normally open current sensor output. 0.1A at 30 VAC/DC.
5. Basis of Design: Veris Model H608.

IIII. Current Status Switches for Constant Load Devices (Auto Calibration)

1. General: Microprocessor based, self-learning, self-calibrating current switch. Calibration-free status for both under and overcurrent, LCD display, and slide-switch selectable trip point limits. At initial power-up automatically learns average current on the line with no action required by the installer
2. Split core sensor, induced powered from monitored load and isolated to 600 VAC rms. Sensor shall indicate status from 2.5 A to 200 A.
3. Display: Backlit LCD; illuminates when monitored current exceeds 4.5A
4. Nominal Trip Point: ±40%, ±60%, or on/off (user selectable)
5. Normally open current sensor output. 0.1A at 30 VAC/DC.

JJJJ. Current Status Switches for Variable Frequency Drive Application

1. General: Microprocessor controlled, self-learning, self-calibrating current sensor to detect motor undercurrent and overcurrent situations such as belt loss, coupling shear, and mechanical failure on variable loads. Sensor shall store motor current as operating parameter in non-volatile memory. Push-button to clear memory and relearn.
2. Visual LED indicator for status.

3. Alarm Limits: ±20% of learned current in every 5 Hz freq. band
4. Split core sensor, induced powered from monitored load and isolated to 600 VAC rms. Sensor shall indicate status from 1.5 A to 150 A and from 12 to 115 Hz.
5. Normally open current sensor output. 0.1A at 30 VAC/DC.

KKKK. Liquid Flow, Insertion Type Turbine Flowmeter:

1. General: Turbine-type insertion flow meter designed for use in pipe sizes 1 1/2" and greater. Available in hot tap configuration with isolation valves and mounting hardware to install or remove the sensor from pipeline that is difficult to shut down or drain
2. Performance:
    1) Accuracy ±1% of rate over optimum flow range; ≥10 upstream and ≥5 downstream straight pipe diameters, uninterrupted flow
    2) Repeatability ±0.5%
    3) Velocity Range: 0.3 to 20 FPS
    4) Pressure Drop 0.5 psi or less @ 10 ft/sec for all pipe sizes 1.5" dia and up
    5) Pressure Rating: 1000 psi @ 70°F
3. Maximum Temperature Rating: 300°F
4. Materials: Stainless Steel or Brass body; Stainless steel impeller
5. Transmitter:
    1) Power Supply: 12 - 30VAC or 8 - 35VDC.
        a) Output: [Frequency] [4-20 mA] [Scaled Pulse]
    2) Temperature Range: 14° to 150°F
    3) Display: 8 character 3/8" LCD (Optional)
    4) Enclosure: NEMA 4, Polypropylene with Viton® sealed acrylic cover

LLLL. Liquid Flow/Energy Transmitter, Non-invasive Ultrasonic (Clamp-on):

1. General: Clamp-on digital correlation transit-time ultrasonic flow meter designed for clean liquids or liquids containing small amounts of suspended solids or aeration. Optional temperature sensors for BTU calculations.
2. Liquid: water, brine, raw sewage, ethylene, glycol, glycerin, others. Contact manufacturer for other fluid compatibility
3. Pipe Surface Temperature: Pipe dia 1/2" to 2":-40-185°F; Pipe dia > 2": -40-250°F
4. Performance:
    1) Flow Accuracy:
        a) Pipe dia 1/2" to 3/4" 1% of full scale
        b) Pipe dia 1" to 2" 1% of reading from 4-40 FPS
        c) Pipe dia 2" to 100" 1% of reading from 1-40 FPS
    2) Flow Repeatability ±0.01% of reading
    3) Velocity Range: (Bidirectional flow)
        a) Pipe dia 1/2" to 2" 2 to 40 FPS
        b) Pipe dia 2" to 100" 1 to 40 FPS
    4) Flow Sensitivity 0.001 FPS
    5) Temperature Accuracy (energy): 32-212°F; Absolute 0.45°F; Difference 0.18°F

6) Temperature Sensitivity: 0.05°F
7) Temperature Repeatability: ±0.05% of reading

5. Transmitter:
   1) Power Supply: 95 to 264 VAC, 47 to 63 Hz or 10 to 28 VDC.
   2) Output: [RJ45] [Modbus TCP/IP] [Ethernet/IP] [BACnet/IP] [Pulse] [4-20 mA] [RS-485 Modbus RTU}
   3) Temperature Range: -40 to +185°F
   4) Display: 2 line backlit LCD with keypad
   5) Enclosure: NEMA 4, (IP65), Powder-coated aluminium, polycarbonate
6. Agency Rating: UL 1604, EN 60079-0/15, CSA C22.2, CSA Class 1 (Pipe > 2")

MMMM. Analog Electric/Pneumatic Transducer:

1. General: Micro-controlled poppet valve for high accuracy and with no air loss in the system. Field configurable for pressure sensing in multiple applications.
2. Power Supply: 22-30VDC, 20-30VAC
3. Control Input: 4-20mA, 0-10V, 0-5V; jumper selectable
4. Performance:
   1) Accuracy: 1% full scale; combined linearity, hysteresis, repeatability
   2) Compensated Temperature Range: 25° to 140°F
   3) Temp Coefficient: ±0.05%°C
   4) Operating Environment: 10-90% RH, non-condensing; 25° to 140°F
5. Supply Pressure: 45 psig max.
6. Manual Override: Jumper selectable mode, digital pushbutton adjust
7. Alarm Contact: 100mA@30VAC/DC (Optional)
8. Control Range 0-20 psig or 3-15 psig; jumper selectable
9. Pressure Differential 0.1 psig (supply to branch)
10. Pressure Indication Electronic, 3-1/2 digit LCD
11. Housing: Mounted on standard SnapTrack; Optional clear dust cover

NNNN. Control Valves

1. Provide automatic control valves suitable for the specified controlled media (steam, water or glycol). Provide valves which mate and match the material of the connected piping. Equip control valves with the actuators of required input power type and control signal type to accurately position the flow control element and provide sufficient force to achieve required leakage specification.
2. Control valves shall meet the heating and cooling loads specified, and close off against the differential pressure conditions within the application. Valves should be sized to operate accurately and with stability from 10 to 100% of the maximum design flow.
3. Trim material shall be stainless steel for steam and high differential pressure applications.
4. Electric actuation should be provided on all terminal unit reheat applications unless electric heat is provided.

OOOO. Dampers

	1. Automatic dampers, furnished by the Building Automation Contractor shall be single or multiple blade as required. Dampers are to be installed by the HVAC Contractor under the supervision of the MSI. All blank-off plates and conversions necessary to install smaller than duct size dampers are the responsibility of the Sheet Metal Contractor. 2. Damper frames are to be constructed of 13 gauge galvanized sheet steel mechanically joined with linkage concealed in the side channel to eliminate noise as friction. Compressible spring stainless steel side seals and acetyl or bronze bearings shall also be provided. 3. Damper blade width shall not exceed eight inches. Seals and 3/8 inch square steel zinc plated pins are required. Blade rotation is to be parallel or opposed as shown on the schedules. 4. For high performance applications, control dampers will meet or exceed the UL Class I leakage rating. 5. Control and smoke dampers shall be Ruskin, or approved equal. 6. Provide opposed blade dampers for modulating applications and parallel blade for two position control. PPPP. Damper Actuators 1. Damper actuators shall be electronic, and shall be direct coupled over the shaft, without the need for connecting linkage. The actuator shall have electronic overload circuitry to prevent damage. For power-failure/safety applications, an internal mechanical, spring return mechanism shall be built into the actuator housing. Non-spring return actuators shall have an external manual gear release to allow positioning of the damper when the actuator is not powered. QQQQ. Smoke Detectors 1. Air duct smoke detectors shall be by Air Products & Controls or approved equal. The detectors shall operate at air velocities from 300 feet per minute to 4000 feet per minute. 2. The smoke detector shall utilize a photoelectric detector head. 3. The housing shall permit mechanical installation without removal of the detector cover. 4. The detectors shall be listed by Underwriters Laboratories and meet the requirements of UL 268A. RRRR. Airflow Measuring Stations 1. Provide a thermal anemometer using instrument grade self heated thermistor sensors with thermistor temperature sensors. 2. The flow station shall operate over a range of 0 to 5,000 feet/min with an accuracy of +/- 2% over 500 feet/min and +/- 10 ft/min for reading less than 500 feet/min.

i. Access Control System

- Access Controller Ethernet Based
  - The Access Controller's should be designed for both critical government & private sector security applications.
  - Below input & output modules should be onboard with the Controllers.
    - Universal Inputs : 12
    - Reader Inputs : 8
    - Tamper Input : 1
    - Digital Lock Output : 4

- The Access Controller's should be designed to support both entry & egress readers while supplying +5 or +12 VDC to each reader.
- The controller should support the data transfer rates upto 100 Mbps and should have IPSec/IKE encryption and authentication. Encryption (up to 192-bit) and authentication may be enabled for communication to and from workstations and controllers. Controller should utilizes Internet Protocol Security (IPSec) and Internet Key Exchange (IKE) for its encryption to assure tamperproof communications over the Ethernet.
- The Controller should be perfect for large systems. A controller servicing up to 8 areas can hold 480,000 personnel records. With such a large local storage capacity, access decisions can be made swiftly without waiting for validation by a remote server.
- Controller should have inbuilt 32 MB of flash memory and 128 MB of DDR SDRAM. The flash memory is used to preserve 12 MB of application and run-time data. The dynamic RAM is partitioned for dedicated functions: a full 12 MB for applications, 48 MB for personnel records and 8 MB for the operating system. The unused memory should be available for future enhancements. Personnel record data should be preserved using onboard batteries that can hold the data for at least 7 days without the use of an external UPS. If the controller has its application stored in flash and power loss lasts longer than what the battery can supply for RAM, the controller will send a message to Cyber Station and request that the personnel records automatically be reloaded when the power returns.
- The reader inputs should be powered by a dedicated processor allowing the controllers to support current and future devices for advanced applications. The hardware should be ready to support 260-bit encrypted data messages from the reader.
- It is important for controller to be able to contain potential threats when they are detected. The Controller should respond to Area Lockdown commands set from Access control software providing a quick method of sealing off areas. A simple click of a graphic or an automatic program response is all that is needed to disable card readers and exit requests in any given area. First responder personnel can still gain access to the area if their record is marked with "executive privilege".
- The Controller should be able to adapt access rights to a change in condition or "threat" levels. Each personnel record should be assigned a clearance level for each area to which they have access. When the condition is more severe than the person's clearance level then access is automatically denied. The Condition Level may be set manually through workstation or automatically through a program. A program can even be used to monitor national threat levels and adjust Condition Levels accordingly.
- Each controller should support the use of two expansion modules plus an Display unit. The expansion module is used for expanding the controller for special or access to doors. Modules can also be used to provide a cost effective entry reader only solution.
- The Access controller should support up to 32 Infinet nodes. The RS-485 programmable port can be set to support a wired or wireless Infinet field bus.
- The Controllers should be ready to support a wide range of card formats. Ideal for retrofits, The Controller lets you preserve existing cards by accepting standard formats (Weigand, ABA, HID Corporate-1000, CardKey) as well as custom

formats (Custom Weigand, Custom ABA). The Controller should support formats up to 260-bits making the controllers ready for government installations that must meet HSPD-12 and FIPS 201 standards.

- SNMP (Simple Network Messaging Protocol) messages may be sent to network monitoring software to inform IT managers as to the health and presence of the access controller on the corporate network. The Access Controller should also support the SNMP alarming option.

Parameters	Specifications
Controller	Microprocessor Based with 8 Readers 12 Inputs, 4 DO , 10/100 bT
Memory	DDR SDRAM: 128 MB Flash: 32 MB
Power	24 VAC , 50/60 Hz 12-28 VDC auto-sensing , 50/60 Hz
Power Consumption	90 VA (AC) 50 W (DC)
Real time Clock	Battery backed by an Internal Battery
Operation Environment	0-50 * C 10-90% RH (Non-Condensing)
Enclosure	UL open class, flammability rating of UL94-5V, IP 10
Mounting	Wall mount using fasteners.
Internal Battery	NiMH , 3.6 VDC, 800 mAh
Battery Backup	Minimum 7 days DDR SDRAM and real-time clock
Ethernet LAN Interface	10/100 Ethernet; ethernet cable with RJ-45 connector.
Serial Comm. Inteface	One RS-485 programmable port, software configurable for Infinet, wireless adapter, RoamIO2 or third-party system.
Input Voltage Range	0-5.115 volts DC
Input Impedance	10K ohm to 5.120V or 5M ohm with pull-up resistor disabled
Input Resolution	5.0 mV
Input Accuracy	±15mV (±0.56°C from -23°C to +66°C or ±1°F from -10°F to +150°F)
Alarm Inputs	12
Card Reader/Keypad Inputs	8, Each input can be connected to a card reader, dedicated keypad, or reader/keypad combination.
Card Reader Type	Wiegand, ABA, or CardKey (jumper selectable)
Max Number of Bits/Card	Up to 260 bits/card
Card Reader Power	+5 VDC @ 120 mA or +12 VDC @ 180 mA (jumper selectable)
Door Outputs	4 Nos. Form C relays with a manual override switch
Output Rating	24 VAC/30 VDC @ 3 A
Overrides	3-position manual override switch on each output for manual control of relay. LED override status indicator.
Status Indicator LEDs	CPU Active, Trasmit & Receive Data , Status of Ethernet activity & link etc.
Dip Switches	Universal inputs, 10 K ohm pull-up disable/enable
Listing & Certifications	FCC , ICES, CE, C-Tick, WEEE, UL/CUL , UL.

- **Input/output Expansion Module:** Up to two I/O modules and an xP-Display may be connected to a controller.

Parameters	Specifications

Operating Environment	32°–120°F (0–49°C), 10–95% RH (non-condensing)
Communications Interface	Through built-in Expansion Port on controller
Status Indicator LEDs	CPU Module is Active
Switches	RESET
Listing	CE,UL & FCC

ii. Smart card/Biometric fingerprint reader

Parameters	Specifications
Read Range	Card Up to 4" (10.2 cm) Key/Tag Up to 1.25" (3.2 cm)
Mounting	Mounting plate attaches to US/EU/ Asian back box, 52-60 mm Screw hole spacing (vertical or horizontal). LCD/Keypad reader Housing latches onto mounting plate; fingerprint module secured to reader with a screw.
Power Supply	9-12 VDC, Linear supply
Operating Temperature	32° F to 113° F (0° C to 45° C)
Operating Humidity	5% to 95% relative humidity non-condensing
Transmit Frequency	13.56 Mhz
Cable Distance	Wiegand/Clock-and-Data Interface: 500 ft (150 m) (22AWG), RS232: 50 ft (15 m), RS485: 4000 ft (1220 m), USB: 16 ft (4 m), UART: 1 ft (0.30 m).
Card Compatibility	iCLASS 15693 & 14443B - read-only on 16k bit (2k Byte), 32k bit (4k Byte); HID Application iCLASS 15693 & 14443B - read/write (RWKLB575 only) on 16k bit (2k Byte), 32k bit (4k Byte); Application Space
Certifications	UL,CE,FCC, C-Tick.
Housing Material	UL94 Polycarbonate
Resolution	500 dpi, 256-bit gray scale, 18 x 22 mm sensor area
Timing	Card read < 0.5 sec Fingerprint capture < 2 sec, typical 1 sec Verification of captured finger < 1 sec
False Accept/Reject Rate	FAR < 0.01%, FRR < 0.01%

iii. Electromagnetic Lock (LED with Lamp Indicator)

Parameters	Specifications
Magnet Size	250 x 42 x 26 mm
Armature Size	180 x 38 x 11 mm
Holding Force	Up to 600 lbs
Current Drain	480 mA+/- 10% / 12 VDC
Temperature	(-10 to 55) * C (14 to 131) * F
Weight	2.0 Kg

iv. Fixed Dome Cameras for Indoor Surveillance

#	Parameter	Minimum Specifications
1.	Video Compression	H.264
2.	Video Resolution	1920x1080
3.	Frame rate	25 fps in all resolutions

#	Parameter	Minimum Specifications
4.	Image Sensor	1/4" / 1/3" Progressive Scan CMOS
5.	Lens Type	Varifocal, C/CS Mount, IR Correction
6.	Lens	Fixed IRIS 2.8-10mm, F1.7, 10x digital zoom
7.	Minimum Illumination	0.9 lux
8.	Image settings	Compression, colour, brightness, sharpness, contrast, white balance, exposure control, backlight compensation, rotation
9.	Protocol	HTTP, HTTPS, FTP, SMTP, RTSP, RTP, TCP, UDP, RTCP, DHCP, UPnP, QoS, IPV4, IPV6
10.	Security	Password Protection, IP Address filtering, User Access Log
11.	Operating conditions	0 to 50°C
12.	Casing	Tamper Resistant casing for Indoor Environment

v. Door Frame Metal Detector

S. No.	Parameter	Minimum Specifications
1.	Technology	Microprocessor based
2.	No. of Zones	Minimum 6 Zones or Better
3.	Operation Frequency	User Selectable
4.	Sensitivity	100 sensitivity steps per program or better
5.	Metal Detection	Should detect: • Ferrous, Non-Ferrous, Ferrite Alloys • Uniformly in entire frame • In all orientation and • In all possible speed of interception Detection at correct zone levels without interference/false identification of adjacent zones.
6.	Alarm Signal	• Audible Alarm • Alphanumeric display & zone display • Remote alarm relay. • Option for remote zonal display unit. • Metering signals proportional to the mass of the detected target
7.	Reset Time	Minimum 0.3 seconds

8.	Traffic Light Status indicator	An LED indicating Green/Red status of the traffic light should be installed on the • Control unit display panel • Top and bottom of both side panels on the exit side of the metal
9.	Interference Suppression	• Should not interfere with adjacent installed DFMD's • Total immunity to environmental/ Radio Signals • Optimum compensation for external stationary metal
10.	Power Supply	• 220V AC 50 Hz. Mains • Battery Operated from and provided with 12V SMF battery of suitable capacity for 4 hours backup.
11.	Calibration	• Automatic & Manual • Built in Keypad • Provision for Remote control unit for parameter settings • Reset time adjustable
12.	Counter	Intelligent traffic counter for transit
13.	Safety	• Should conform to international standards of safety/radiations • Should be safe for heart pace makers • Should be data safe
14.	Self-Diagnostics	User friendly self-testing diagnostics to identify faulty condition
15.	Ambient temperature	From 0°C to 60°C
16.	Humidity	Up to 90% No Condensation
17.	Control Panel	Easily accessible, modular design with Standard plugs and connectors.
18.	Network Connectivity	• Compatibility to integrated physical security system via TCP IP • Adaptability to remote monitoring systems.
19.	Integration	• Integration with Other Access Control Devices like Turnstiles, Flap gates etc • Integration capability with cameras
20.	Construction	Light Weight, rigid, laminated side panels and cross piece, all plastic boots for panel protection base wheels for easy mobility.
21.	Standards	• Meets Electrical Safety and Compatibility Requirements • International Standards (IS) Command • CE/FCC/IEC/IEEE certified.

vi. Hand Held Metal Detector

#	Parameter	Minimum Specifications
1.	Display	The HHMD may be of LED display type or of LCD display type (type offered shall be clearly indicated in the offer). The following minimum LED indications should be available in the HHMD:- • ON indication, • Metal detection indication, • Low battery Indication
2.	Dimension	Area of search coil: Minimum 125 Sq. cm
3.	Sensitivity	There will not be any sensitivity control switch and calibration shall be automatic. The number of beeps will indicate the size of metal. Sensitivity should be very high so as to easily detect the following. It shall detect objects concealed in ferrite. • Ferrous Coins, Paper Pin, Paper clip, Knife/Blade, Stainless steel blade • Non Ferrous Aluminium tube, Copper plate, Brass plate
4.	Audio Alarm	Audio Alarm should: • be loud enough on detection of any metal • give an idea about the size of the objects by the number of beeps Detection of objects • detect ferrous and non-ferrous metals alloys in any possible orientation • Give distinct and different audio output in case of Ferrite detection
5.	Power Source	• Rechargeable - NiCD/NiMH pack each sufficient 50 hour operation without audio and 25 hours with audio on one charge • The HHMD should have inbuilt charging capacity
6.	Construction	Light Weight, Rugged, High Impact ABS case with reinforced coil compartment
7.	Tuning	Automatic
8.	Safety	Magnetic field generated by the HHMD should be harmless to magnetic media, electronic devices and heart pace makers.
9.	Temperature	From 0°C to 50°C
10.	Standards	Should conform IS:12126:1987/CE certified
11.	Miscellaneous	• Cleaning Kit • Technical manual

		• User handbook

vii. Boom Barriers

#	Parameter	Minimum Specifications
1.	Barrier Length	3 to 6 Meters (Depending upon Site requirement)
2.	Opening/ Closing Time	Maximum 2 secs
3.	Maximum Torque	600NM
4.	Duty Cycle	100%
5.	MCBF	Minimum 5000000 Cycles
6.	Power	230VAC
7.	Motor Power Supply	230VAC or 24VDC
8.	Operating Temperature	0 Deg C to 60 Deg C
9.	Operating Humidity	More than 95%
10.	IP Rating	IP 65 or better

3. Annexure 3 – Template for Pre-Bid Queries

Bidder shall submit all pre-bid queries in excel in the following format.

SL #	RFP Volume, Section	RFP page no	Content in the RFP	Clarification sought

4. Annexure 4 – Formats for Submission of the Pre-Qualification Bid

a. Pre-qualification bid checklist

Sl #	Checklist Items	Compliance (Yes or No)	Page No. and Section No. in bid
1.	RFP Document fees		
2.	Earnest Money Deposit		
3.	Pre-Qualification Covering letter		
4.	Consortium Agreement, if applicable as per Annexure 9		
5.	· Copy of Certification of Incorporation/Registration Certificate · PAN card · VAT registration ·		
6.	Audited financial statements for the last three financial years (FY 2013-14, 2014-15 and 2015-16). And Certificate from the Statutory Auditor		
7.	Declaration of non-blacklisting		
8.	Power of attorney for Lead Bidder of Consortium		
9.	Project Citations and Self-certifications, as Applicable		
10.	Total Responsibility Certificate		
11.	Valid ISO certification		

b. Pre-Qualification Bid Covering Letter

Date: dd / mm / yyyy

To,

[ ]

Sub: **Request for Proposal for Selection of System Integrator for Implementation of Bhopal Smart City Solution**

Ref: RFP No. **<<.....>> dated << .....>>**

Dear Sir,

With reference to your "**Selection of Master System Integrator And Cloud Service Provider for Integrated Data Centre for Smart Cities and City Integrated Command and Control Centers for the State of Madhya Pradesh"** we hereby submit our Prequalification bid, Technical Bid and Commercial Bid for the same.

We hereby declare that:

a. We hereby acknowledge and unconditionally accept that the BSCDCL can at its absolute discretion apply whatever criteria it deems appropriate, not just limiting to those criteria set out in the RFP and related documents, in short listing of Agency for providing services.

b. We have submitted EMD of INR 5 Crore (via DD or BG) and Tender fee of INR 50,000 online through e- procurement portal.

c. We hereby declare that all information and details furnished by us in the Bid are true and correct, and all documents accompanying such application are true copies of their respective originals.

d. We agree to abide by our offer for a period of 180 days from the date of opening of pre-qualification bid prescribed by **BSCDCL** and that we shall remain bound by a communication of acceptance within that time.

e. We have carefully read and understood the terms and conditions of the RFP and the conditions of the contract applicable to the RFP. We do hereby undertake to provision as per these terms and conditions.

f. In the event of acceptance of our bid, we do hereby undertake:
   i. To supply the products and commence services as stipulated in the RFP document
   ii. To undertake the project services for entire contract period from the date of signing of the contract as mentioned in the RFP document.
   iii. We affirm that the prices quoted are inclusive of design, development, delivery, installation, commissioning, training, providing facility management and handholding support, and inclusive of all out of pocket expenses, discounts etc.

g. We do hereby undertake, that, until a formal contract is prepared and executed, this bid, together with your written acceptance thereof and notification of award of contract, shall constitute a binding contract between us.

h. We understand that the **BSCDCL** may cancel the bidding process at any time and that **BSCDCL** is not bound to accept any bid that it may receive without incurring any liability towards the bidder.

i. We fully understand and agree to comply that on verification, if any of the information provided in our bid is found to be misleading the selection process, we are liable to be dismissed from the selection process or termination of the contract during the project, if selected to do so

In case of any clarifications please contact _____ email at _____

Thanking you,

Yours sincerely,

(Signature of the Lead bidder)

Printed Name

Designation

Seal

Date:
Place:
Business Address:

c. Company profile

A. Brief company profile (required for both bidder and consortium member)

SL. NO.	PARTICULARS	DESCRIPTION OR DETAILS
1.	Name of Bidder	
2.	Legal status of Bidder (company, Pvt. Ltd., LLP etc.)	
3.	Main business of the Bidder	
4.	Registered office address	
5.	Incorporation date and number	
6.	Service Tax number	
7.	VAT number	
8.	PAN details	
9.	Primary Contact Person (Name, Designation, address, mobile number, fax, email)	
10.	Secondary Contact Person (Name, Designation, address, mobile number, fax, email)	
11.	EMD details	
12.	Role in Consortium (if applicable)	Brief scope of work in the consortium

B. Certificate of Incorporation (required for both bidder and consortium member)

C. Financial Turnover

The financial turnover of the company is provided as follows:

	2012-13	2013-14	2014-15	2015-16
Annual Turnover				

Copy of audited financial statements or declaration from the appointed statutory auditor to be provided as proof of the financial turnover.

Positive net worth of the last five financial years as on 31.03.2016. Copy of self-certified statutory auditor certificate to be submitted along with the bid

D. Certifications (required for both bidder and consortium member)

Provide copy of valid certification for ISO certifications as required in Pre-Qualification criteria as on release date of the RFP.

d. Declaration of Non-Blacklisting

(To be provided on the Company letter head)

Declaration for Lead Bidder:

Place

Date

To,

[ ]

Subject: Self Declaration of not been blacklisted in response to the Request for Proposal for selection of "**Request for Proposal for Selection of System Integrator (MSI) for Implementation of Integrated Command and Control Center for Bhopal Smart City Development Corporation Limited (BSCDCL)at Bhopal"**

Ref: RFP No. **<<.....>> dated << .....>>**

Dear Sir,

We confirm that our company or firm, _____,is currently not blacklisted in any manner whatsoever by any of the State or UT and or Central Government / PSUs in India on any ground including but not limited to indulgence in corrupt practice, fraudulent practice, coercive practice, undesirable practice or restrictive practice.

(Signature of the Lead Bidder)

Printed Name

Designation

Seal

Date:

Place:

Business Address:

e. Declaration for Consortium Member:

(To be provided on the Company letter head)

{Place}

{Date}

To,

[ ]

Subject: Self Declaration of not been blacklisted in response to "**Request for Proposal for Selection of System Integrator (MSI) for Implementation of Integrated Command and Control Center for Bhopal Smart City Development Corporation Limited (BSCDCL)at Bhopal"**

Ref: RFP No. **<<.....>> dated << .....>>**

Dear Sir,

We confirm that our company or firm, _____,is currently not blacklisted in any manner whatsoever by any of the State or UT and or Central Government in India on any ground including but not limited to indulgence in corrupt practice, fraudulent practice, coercive practice, undesirable practice or restrictive practice.

(Signature of the Consortium Member)

Printed Name

Designation

Seal Date:

Place: Business Address:

f. Total Responsibility Certificate

This is to certify that we undertake the total responsibility for the defect free operation of the proposed solutions as per the requirement of the RFP for the duration mentioned in all the volumes of the RFP.

(Authorized Signatory)

Signature:
Name:
Designation:
Address:

Seal:
Date:

g. Self-certificate for Project execution experience (In Bidding Entity's Letter Head)

This is to certify that < Name of the Bidding entity > has been awarded with < Name of the Project > as detailed under:

Name of the Project	
Client's Name, Contact no. and Complete Address	
Contract Value for the bidder (in INR)	
Current status of the project (Completed/Ongoing)	
Activities completed by bidding entity as on bid submission date ***(N.B Only relevant activities as sought in the Criteria to be included)***	
Value of Work completed for which payment has been received from the client.	
Date of Start	
Date of Completion	

(Authorized Signatory)

Signature:
Name:
Designation:
Bidding entity's name
Address:

Seal:
Date:

5. Annexure 5 – Formats for Submission of the Technical Bid

a. Technical Bid Check-List

Sl #	Checklist Item	Compliance (Yes/No)	Page No. and Section No. in the Bid
1	Technical Bid Letter		
2	Credential summary		
3	Project Citations and Self-certifications, as applicable		
4	Detailed proposed solution		
5	Project plan and manpower plan		
6	Proposed CVs		
7	Compliance to Requirement (Technical / Functional Specifications)		
8	Proposed Bill of Material		
9	Manufacturers'/Producers' Authorization Form Anti-Collusion certificate		
10	Non-disclosure agreement		
11	Manufacturers'/Producers' Authorization Form (one for each OEM)		

b. Technical Bid Covering Letter

Date:
dd/mm/yyyy

To,

[ ]

Subject: Request for Proposal for Selection of System Integrator (MSI) for Implementation of Integrated Command and Control Center for Bhopal Smart City Development Corporation Limited (BSCDCL) at Bhopal

Ref: RFP No. **<<.....>> dated << .....>>**

Dear Sir,

I (in case of single bidder) or We, <<name of the undersigned Bidder and consortium members>>, having read and examined in detail all the bidding documents in respect of "**Selection of Master System Integrator And Cloud Service Provider for Integrated Data Centre for Smart Cities and City Integrated Command and Control Centers for the State of Madhya Pradesh"** do hereby propose to provide our services as specified in the bid submitted by us.

It is hereby confirmed that I / We are entitled to act on behalf of our company / corporation / firm / organization and empowered to sign this document as well as such other documents, which may be required in this connection.

We declare that all the services shall be performed strictly in accordance with the RFP documents.

We confirm that the information contained in this response or any part thereof, including its exhibits, and other documents and instruments delivered or to be delivered to BSCDCL,, Government of [State] is true, accurate, verifiable and complete. This response includes all information necessary to ensure that the statements therein do not in whole or in part mislead the department in its evaluation process. We also confirm that we shall not attract conflict of interest in principle.

We hereby declare that in case the contract is awarded to us, we shall submit the contract Performance bank guarantee in the form prescribed at Annexure 5 (a) of Section 9 of the RFP Volume I.

We hereby declare that our bid is made in good faith, without collusion or fraud and the information contained in the bid is true and correct to the best of our knowledge and belief.

We understand that our bid is binding on us and that you are not bound to accept a Bid you receive. This bid is valid for 180 days after opening of technical bid. We shall extend the validity of the bid if required by Purchaser.

Thanking you,

Yours sincerely,

(Signature of the Lead Bidder)

Printed Name

Designation

Seal

Date:

Place:

Business Address:

c. Credential Summary

Sl #	Project Name	Client Name	Client Type	Project Value (in INR)	Project Components	Documentary evidence provided (Yes or No)	Project Status (Completed or Ongoing or Withheld)
1							
2							
3							
4							
5							
6							
7							

- *Client type – Indicate whether the client is Government or PSU or Private*
- *Project Components – Indicate the major project components like setting up of NOC, Wide Area Network, city/ public Wi-Fi, application development for security surveillance, command and control center, Maintenance, Hardware procurement and deployment, DC setup and maintenance, Facility management services, provisioning manpower, IT support and maintenance*
- *Documentary evidence provided – Indicate the documentary evidence provided with the detailed project credential like work order or purchase order or completion certificate or letter of appointment*
- *Project Status – Completed (date of project completion) or Ongoing (project start date)*

d. Bidder's Experience - Client Citations

Prime Bidder or Consortium member is requested to furnish the credentials in the following format for both Pre-qualification and Technical criterion. All credentials should be followed by relevant documentary proof.

General Information	
Name of the project	
Client for which the project was executed	
Name and contact details of the client	
Project Details	
Description of the project	
Scope of services	
Technologies used	
Relevance to the current project	
Outcomes of the project	
Other Details	
Total cost of the project	
Total cost of the services provided by the respondent	
Duration of the project (no. of months, start date, completion date, current status)	
Other Relevant Information	
Letter from the client to indicate the successful completion of the projects (if any)	
Copy of Work Order/Agreement	

N.B - If the project is ongoing, bidder must clearly specify which of the stages/phases/milestones are completed and which are ongoing and at what stage of completion and produce a self-certificate as per the format provided in Section 6.7.

e. Overview of Proposed Solution

i. Structure of Proposed Solution

Bidders are required to provide a detailed approach & methodology to execute the entire project. Bidders are advised to comply with the below provided headers/Approach components while detailing out their solution.

Sl. No.	Item
1.	**Understanding of requirement and Implementation approach** · Understanding of requirements · Work Plan & its adequacy
2.	**Robustness and quality** · End to end integrated solution proposed · Hardware deployment and integration approach encompassing all solutions · Timelines and modalities for implementation in a time bound manner · Project implementation approach or strategy and operations and maintenance plan including comprehensiveness of fall-back strategy and planning during rollout · Any other area relevant to the scope of work and other requirements of the Project
3.	**Assessment of Manpower deployment, Training and Handholding plan** · Deployment strategy of Manpower · Contingency management · Mobilization of existing resources and additional resources as required · Training and handholding strategy (must include training of Operators before Go-Live and during implementation phase)

ii. Project Plan

A **Detailed Project Plan** covering break-up of each phase into the key activities, along with the start and end dates must be provided as per format given below.

Activity-wise Timelines							
Sl. No.	**Item of Activity**	**Month wise Program**					
		1	2	3	4	5	…
	Project Plan						
1	Activity 1						
1.1	Sub-Activity 1						
1.2	Sub-Activity 2						
2							
2.1							
2.2							
3							
3.1							
4							

Activity-wise Timelines

Sl. No.	Item of Activity	Month wise Program

Note: The above activity chart is just for the purpose of illustration. Bidders are requested to provide detailed activity & phase wise timelines for executing the project with details of deliverables & milestones as per their bid.

iii. Manpower Plan

I.Till Go-Live (Implementation)

Sl No.	Manpower	Months				Total
		Month 1	Month 2	.....	Month N	
1.	Program Manager					Onsite
2.	Cloud DC / DR Expert					Onsite
3.	Citizen Service/Municipal Domain expert					Onsite
4.	Water SCADA or Electrical SCADA expert					Onsite
5.	GIS expert					Onsite
6.	Surveillance Expert					Onsite
7.	ITMS Expert					Onsite
8.	Solution Architect					Onsite
9.	Project Manager-Software					Onsite
10.	Project Manager-Infrastructure					Onsite
11.	Database Architect					Onsite
12.	Security Expert					Onsite

13.	Command and Control Centre management Expert					Onsite
14.	Mobile App development Expert					Onsite

Above plan is required to be prepared separately for each city.

II. After Go-Live (Operation & Maintenance for 5 Years)
Following manpower has to be deployed for each city at their respective city ICCC.

#	Type of Resource	Minimum Quantity	Minimum Deployment during Operation and Maintenance phase
13.	Project Manager	1	100%
14.	Solution Architect	1	Onsite Support to Project team on need basis
15.	Project Manager-Software	1	100%
16.	Project Manager – Infrastructure	1	100%
17.	Database Architect/DBA	1	100%
18.	Cloud DC / DR Expert	1	100%
19.	Security Expert	1	Onsite Support to Project team on need basis
20.	Command Centre Expert	1	100%
21.	GIS expert	1	Onsite Support to Project team on need basis
22.	Help Desk Manager	1	100%
23.	Help Desk Executives (24*7 – 1 in each shift)	3	100%
24.	Command Center Operators (24*7 – 10 in each shift)	30	100%

f. Details of Resources proposed

Summary of Resources proposed

SL No.	Name of Staff	Proposed Role	Qualification	Certification	Experience	Area of Expertise	Position Assigned	Time committed for the engagement

g. Curriculum Vitae (CV) of Team Members

1	**Proposed Position**				
2	**Name of Firm**				
3	**Name of Expert**				
4	**Date of Birth**		**Citizenship:**		
5	**Education**				
6	**Membership in Professional Associations** (Professional Certifications)	•			
7	**Countries Of Work Experience**	•			
Language Skills (mark Excellent/Good/Average)		**Language**	**Read**	**Write**	**Speak**
		English			
		Hindi			
		<Add Language>			
8	**Employment Records**				

From:		To:	
Employer			
Position Held			

From:		To:	
Employer			
Position Held			

From:		To:	
Employer			
Position Held			

9	**Work Undertaken That Best Illustrates Capability To Handle The Tasks Assigned**

Project Name	
Year	
Location	
Client	
Main project Features	
Position Held	

Activities performed	

Expert's contact information:
e-mail:
phone:

Certification:

I, the undersigned, certify that to the best of my knowledge and belief that

- This CV correctly describes my qualifications and my experience
- I was not part of the team who wrote the Scope of Work for this RFP.
- I understand that any willful misstatement described herein may lead to my disqualification or dismissal, if engaged.

Name of Expert	Signature	Date

i. Compliance to Requirement (Technical / Functional Specifications)

The bidder should provide compliance to the requirement specifications (both technical and functional) specified in the Section 4 of the Volume II of this RFP. The same should be reproduced here, and compliance against each requirement line item should be marked.

j. Manufacturers'/Producers' Authorization Form

(This form has to be provided by the OEMs of the hardware and software solutions proposed. This letter should be on the letterhead of the manufacturer and should be signed by a person competent and having the power of attorney to bind the manufacturer.)

Date:

To,

The Chief Executive Officer
Bhopal Smart City Development Corporation Limited (BSCDCL)
Zone- 14, Bhopal Municipal Corporation, BHEL, Govindpura
Bhopal- 462023

Subject: Manufacturer's Authorization Form

Ref: RFP No. <<.....>> dated << .....>>

Dear Sir,

We_____ (Name of the OEM) who are established and reputable manufacturers of _____ (List of Goods) having factories or product development centers at the locations _____ or as per list attached, do hereby authorize. _____ (Name and address of the Bidder) to bid, negotiate and conclude the contract with you against RFP No. _____Dated _____for the above goods manufactured or developed by us.

We hereby extend, our warranty for the hardware goods supplied by the bidder and or maintenance or support services for software products against this invitation for bid by _____ (Name of the Bidder) as per requirements of this RFP.

Thanking you,

Yours faithfully,

(Signature)

For and on behalf of: _____ (Name of the OEM)

Authorised Signatory

Name:

Designation:

Place:

Date:

k. Anti-Collusion Certificate

[Certificate should be provided by Lead Bidder and on letter head]

Anti-Collusion Certificate

We hereby certify and confirm that in the preparation and submission of our Bid for **Selection of Master System Integrator And Cloud Service Provider for Integrated Data Centre for Smart Cities and City Integrated Command and Control Centers for the State of Madhya Pradesh** against the RFP issued by Purchaser, We have not acted in concert or in collusion with any other Bidder or other person(s) and also not done any act, deed or thing, which is or could be regarded as anti-competitive. We further confirm that we have not offered nor will offer any illegal gratification in cash or kind to any person or organization in connection with the instant bid.

(Signature of the Lead Bidder)

Printed Name

Designation

Seal

Date:

Place:

Business Address:

6. Annexure 6 – Formats for Submission of the Commercial Bid

Total Price Summary

Sl #	Commercial	Comments / Assumptions for Units (if any)	Per unit price (INR)	Year 1		Year 2		Year 3		Year 4		Year 5		Total
			1	2	3	4	5	6	7	8	9	10	11	12
				Units	Cost 3 = 2*1	Units	Cost 5 = 4*1	Units	Cost 7 = 6*1	Units	Cost 9 = 8*1	Units	Cost 11 = 10*1	12 = 3+5+7+9+11
1	**Initial IT set up per city**	**1 = a +b+c+d+e+f+g+h+i+j+k +l+m+n+o+p+q+r**												
a	**Initial set up per city- Implementation, configuration and activation,**	Cost of one edge device per city, Refer to Edge architecture definition- Sl # 29 of Functional Requirement of Command and Control Centre provided in Functional Specification provided in annexures of this RFP		5		2								
b	Video Wall	1 per city		5		2								

c	Operator Terminal	30 per city		150		60								
d	Office Desktop	30 per city		150		60								
e	Server Rack	1 server rack per city		5		2								
f	Servers	1 per city		5		2								
g	Storage (SAN Switch)	1 per city		5		2								
h	Flash Storage (for backup 500 TB)	1 per city		5		2								
i	LAN Cabling	Required LAN cabling cost per city with assumption of minimum area as 10000 sq. feet of ICCC		5		2								
j	LAN Switches	1 per city		5		2								
k	IP Phones	65 per city		325		130								
l	Laser Printer	3 per city		15		6								
m	Fixed Drone Cameras	10 per city		50		20								
n	Fire Alarm System	1 per city to address the need of 10000 sq. feet area of ICCC		5		2								
o	Public Address System	1 per city to address the need of 10000 sq. feet area of ICCC		5		2								
p	Access Control System (RFID/Proximity based, for all staff)	1 per city to address the need of 10000 sq. feet area of ICCC		5		2								
q	Aggregation Router	1 per city		5		2								

r	Situation Room Setup	Unit includes all the IT infrastructure as per RFP		5		2								
2	**Initial Non IT Setup for city ICCC**	**2 = a +b+c+d+e+f+g+h+i+j+k +l+m**												
a	Civil Work	Cost of required work for 10000 sq. feet		5		2								
b	Wiring and Earthing	Cost of required work for 10000 sq. feet		5		2								
c	UPS / SMPS Unit	2 units per city - Cost of required supply		10		4								
d	Power Backup / DG Set	1 units per city - Cost of required supply		5		2								
e	Ergonomic Chairs (for operators , meeting rooms, office staffetc.)	100 per city		500		200								
f	Operator Table	30 per city		150		60								
g	Office Desk	30 per city		150		60								
h	HVAC	Cost of required work for 10000 sq. feet		5		2								
i	Lighting	Cost of required work for 10000 sq. feet		5		2								
j	Conference Room Tables	3 per city		15		6								
k	Conference Table with table top touch	1 per city		5		2								

	screens/capacitive, 84'' (for 20 personnel) - for situation room													
l	LCD Projector (for meeting rooms)	4 per city		20		8								
m	Situation Room Setup (non IT)	Unit includes all the non IT infrastcrure except Conference Table with table top touch screens/capacitive, 84'' mentioned above as per RFP		5		2								
3	**O&M cost of Initial set up per city**	**3 = a +b+c+d+e+f+g+h+i+j+k +l+m+n+o+p+q+r**												
a	**Initial set up per city- Implementation, configuration and activation,**	Cost of one edge device per city, Refer to Edge architecture definition- Sl # 29 of Functional Requirement of Command and Control Centre provided in Functional Specification provided in annexures of this RFP		5		7		7		7		7		
b	Video Wall	1 per city		5		7		7		7		7		

c	Operator Terminal	30 per city		150		210		210		210		210		
d	Office Desktop	30 per city		150		210		210		210		210		
e	Server Rack	1 server rack per city		5		7		7		7		7		
f	Servers	1 per city		5		7		7		7		7		
g	Storage (SAN Switch)	1 per city		5		7		7		7		7		
h	Flash Storage (for backup 500 TB)	1 per city		5		7		7		7		7		
i	LAN Cabling	Required LAN cabling cost per city with assumption of minimum area as 10000 sq. feet of ICCC		5		7		7		7		7		
j	LAN Switches	1 per city		5		7		7		7		7		
k	IP Phones	65 per city		325		455		455		455		455		
l	Laser Printer	3 per city		15		21		21		21		21		
m	Fixed Drone Cameras	10 per city		50		70		70		70		70		
n	Fire Alarm System	1 per city to address the need of 10000 sq. feet area of ICCC		5		7		7		7		7		
o	Public Address System	1 per city to address the need of 10000 sq. feet area of ICCC		5		7		7		7		7		
p	Access Control System (RFID/Proximity based, for all staff)	1 per city to address the need of 10000 sq. feet area of ICCC		5		7		7		7		7		
q	Aggregation Router	1 per city		5		7		7		7		7		

r	Situation Room Setup	Unit includes all the IT infrastructure as per RFP		5		7		7		7		7		
4	**O&M cost for Initial Non IT Setup for city ICCC**	**4 = a +b+c+d+e+f+g+h+i+j+k +l+m**												
a	Civil Work	Cost of required work for 10000 sq. feet		5		7		7		7		7		
b	Wiring and Earthing	Cost of required work for 10000 sq. feet		5		7		7		7		7		
c	UPS / SMPS Unit	2 units per city - Cost of required supply		10		14		14		14		14		
d	Power Backup / DG Set	1 units per city - Cost of required supply		5		7		7		7		7		
e	Ergonomic Chairs (for operators , meeting rooms, office staffetc.)	100 per city		500		700		700		700		700		
f	Operator Table	30 per city		150		210		210		210		210		
g	Office Desk	30 per city		150		210		210		210		210		
h	HVAC	Cost of required work for 10000 sq. feet		5		7		7		7		7		
i	Lighting	Cost of required work for 10000 sq. feet		5		7		7		7		7		
j	Conference Room Tables	3 per city		15		21		21		21		21		
k	Conference Table with table top touch	1 per city		5		7		7		7		7		

	screens/capacitive, 84'' (for 20 personnel) - for situation room													
l	LCD Projector (for meeting rooms)	4 per city		20		28		28		28		28		
m	Situation Room Setup (non IT)	Unit includes all the non IT infrastcrure except Conference Table with table top touch screens/capacitive, 84'' mentioned above as per RFP		5		7		7		7		7		
5	**New Appliation integration in to the platform (per sensor vendor- to be charged once only if same sensor vendor is in multiple cities), Staging environment for a new application integration (Ref Sl # 100 of Functional Requirement of Command and Control Centre provided in Functional**	**5 = a +b+c+d+e+f+g+h**												

	Specification provided in annexures of this RFP)													
a	Video Surveillance for Citizen Safety and Security			5		2								
b	Integrated Enterprise Geographical Information System (GIS)			5		2								
c	Smart Parking Management and Guidance			5		2								
d	Smart and Integrated City Lighting			5		2								
e	Citizen Kiosks for Information and Govt. services			5		2								
f	Integrated Solid Waste Management			5		2								
g	Intelligent Transport Management System			5		2								
h	Intelligent Water Supply Management System			5		2								

6	**License cost per sensor (per Video and non-Video sensors Including**	**6 = a +b+c+d+e+f+g+h**												
	Support cost that includes 24X7 call support, triaging, etc..													
	Cost of cloud operation (monitoring and management) for the platform (ref Sl # 98, 99 of Functional Requirement of Command and Control Centre provided in Functional Specification provided in annexures of this RFP)													
a	Video Surveillance for Citizen Safety and Security			500		1000		1000		1000		1000		
b	Integrated Enterprise Geographical Information System (GIS)			1000		1500		2500		3500		3500		

c	Smart Parking Management and Guidance			1500		2500		3500		3500		3500		
d	Smart and Integrated City Lighting			1500		2500		3500		3500		3500		
e	Citizen Kiosks for Information and Govt. services			1500		2500		3500		3500		3500		
f	Integrated Solid Waste Management			1500		2500		3500		3500		3500		
g	Intelligent Transport Management System			1500		2500		3500		3500		3500		
h	Intelligent Water Supply Management System			1500		2500		3500		3500		3500		
7	**Cost of current city systems (ERP, e-gov systems, etc..) integration in to the platform (These are existing / planned applications which will be hosted indepnedntly. However needs to be integrated with ICCC**	**7 = a +b+c+d+e+f+g+h+i+j+k +l**												

	for analytics purposes)													
a	Integration of Municipal Corporation Call Centre			5		2								
b	Integration of Standard Municipal Corporation Services			5		2								
c	Integration with City Specific mobile / web Application			5		2								
d	Integration with DIAL 100			5		2								
e	Integration with DIAL 108 & Jannani Express			5		2								
f	Integration with City Water SCADA System			5		2								
g	Integration with Emergency Response and Disaster Mgmt.			5		2								
h	Integration with Met Department (Local Weather Forecast)			5		2								
i	Integration with Area Based Development (ABD) Services: i. Utilities ii. Lighting iii.			5		2								

	Metering iv. Surveillance													
j	Integration of Crowdsourcing Data with ICCC			5		2								
k	Integration with Fire Brigade Control System			5		2								
l	Integration with Solar Roof Top Project			5		2								
8	**Cloud and connectivity cost for applications integrated with common city command center platform (These are existing / planned applications which will be hosted independently. However needs to be integrated with ICCC for analytics purposes)**	**8 = a +b+c+d+e+f+g+h+i+j+k +l**												
a	Municipal Corporation Call Centre			5		2								
b	Standard Municipal Corporation Services			5		2								

c	City Specific mobile / web Application			5		2								
d	DIAL 100			5		2								
e	DIAL 108 & Jannani Express			5		2								
f	City Water SCADA System			5		2								
g	Emergency Response and Disaster Mgmt.			5		2								
h	Met Department (Local Weather Forecast)			5		2								
i	Area Based Development (ABD) Services: i. Utilities ii. Lighting iii. Metering iv. Surveillance			5		2								
j	Crowdsourcing Data with ICCC			5		2								
k	Fire Brigade Control System			5		2								
l	Solar Roof Top Project			5		2								
9	**Cost for number of client / user licenses for City Operations center platform**	**1 license per 200 sensor licenses (total of line 5 / 200)**		**60**		100		140		145		145		

10	**Dedicated Resources per City (Resources per city)**	**10 = a +b+c+d+e+f+g+h+i+j+k +l+m+n+o+p+q+r+s+t**												
a	Program Manager	man year cost (man month rate *12)		5		7		7		7		7		
c	Citizen Service/Municipal Domain expert	man year cost (man month rate *12)		5		7		7		7		7		
d	Cloud DC / DR Expert	man year cost (man month rate *12)		5		7		7		7		7		
e	Command and Control Centre management Expert	man year cost (man month rate *12)		5		7		7		7		7		
f	Database Architect/DBA	man year cost (man month rate *12)		5		7		7		7		7		
g	GIS expert	man year cost (man month rate *12)		5		7		7		7		7		
h	ITMS Expert	man year cost (man month rate *12)		5		7		7		7		7		
i	Mobile App development Expert	man year cost (man month rate *12)		5		7		7		7		7		
j	Project Manager-Infrastructure	man year cost (man month rate *12)		5		7		7		7		7		
k	Project Manager-Software	man year cost (man month rate *12)		5		7		7		7		7		
l	Security Expert	man year cost (man month rate *12)		5		7		7		7		7		
m	Solution Architect	man year cost (man month rate *12)		5		7		7		7		7		

n	Surveillance Expert	man year cost (man month rate *12)		5		7		7		7		7		
o	Water SCADA or Electrical SCADA expert	man year cost (man month rate *12)		5		7		7		7		7		
p	Command Center Operators (24*7 – 10 in each shift)	man year cost (man month rate *12)		150		210		210		210		210		
q	Help Desk Manager	man year cost (man month rate *12)		5		7		7		7		7		
r	Help Desk Executives (24*7 – 1 in each shift)	man year cost (man month rate *12)		15		21		21		21		21		
s	Physical Security Staff (24*7 – 3 in each shift)	man year cost (man month rate *12)		45		63		63		63		63		
t	Housekeeping Staff (24*7 – 2 in each shift)	man year cost (man month rate *12)		30		42		42		42		42		
11	**Network and Connectivity (for local application integrations, where video feeds are received)**													
	Intranet Bandwidth (within city)	150 Mbps		5		7		7		7		7		
12	**Year wise Total**													

13	**Total Net Present Value of the project (@9%)**		[redacted]

N.B –
Platform should offer a Pay-as-you-grow pricing model that facilitates a flexible approach to the city

The price quoted in the format given above will be used for evaluation purposes and will be treated as total envisaged value of the project. However the payment will be done on the basis of actual completion of the respective items in a particular month.

PBG will be required to be created by the appointed MSI based on the total net present value as shown in the financial bid.

Bidder must ensure that all amounts to be quoted in INR.

Unit priced for Manpower cost is per annum, and at the time of monthly payment – payment will be done as per man month rate which is equal to Manpower rate per annum divided by 12.

Assumptions of Units are provided in the financial bid table.

Value coated as total price must contain all the components required for the successful implementation of the project. Nothing extra will be paid by the authority beyond the value coated in the above form, until there is change request is approved by Authority.

Electricity and Water consumption bills will be initially paid by MSI, then reimbursed by BSCDCL along with invoice of following month.

Taxes as applicable at the time of invoicing shall be considered. Any changes (upward or downward) in the taxes/duties shall be accordingly revised at the time of actual payments and paid. Service Tax & Cess will be paid by BSCDCL as per the norms defined by Government of India at the time of actual payment.

Bidder is requested to check final figure in all the totals of the sheets. BSCDCL is not responsible for errors in the financial bid document.

Bidder is required to upload the updated financial bid in the prescribed excel format in the www.mpeproc.gov.in at the time of financial bid submission.

7. Annexure 7 (a) – Performance Bank Guarantee

Ref: _____ Date _____

Bank Guarantee No. _____

<Name>
<Designation>
<Addre
ss>
<Phone
Nos.>
<Fax
Nos.>
<Email
id>

Whereas, <<name of the supplier and address>> (hereinafter called "the System Integrator") has undertaken, in pursuance of contract no. <Insert Contract No.> dated. <Date> to provide Implementation services for <<name of the assignment>> to [BSCDCL] (hereinafter called "the Purchaser")

And whereas it has been stipulated by in the said contract that the bidder shall furnish you with a bank guarantee by a recognized bank for the sum specified therein as security for compliance with its obligations in accordance with the contract;

And whereas we, <Name of Bank> a banking company incorporated and having its head/registered office at <Address of Registered Office> and having one of its office at <Address of Local Office> have agreed to give the supplier such a bank guarantee.

Now, therefore, we hereby affirm that we are guarantors and responsible to you, on behalf of the supplier, up to a total of Rs.<Insert Value> (Rupees <Insert Value in Words> only) and we undertake to pay you, upon your first written demand declaring the supplier to be in default under the contract and without cavil or argument, any sum or sums within the limits of Rs. <Insert Value> (Rupees <Insert Value in Words> only) as aforesaid, without your needing to prove or to show grounds or reasons for your demand or the sum specified therein.

We hereby waive the necessity of your demanding the said debt from the bidder before presenting us with the demand.

We further agree that no change or addition to or other modification of the terms of the contract to be performed there under or of any of the contract documents which may

be made between you and the System Integrator shall in any way release us from any liability under this guarantee and we hereby waive notice of any such change, addition or modification.

This Guarantee shall be valid until <<Insert Date>>)

Notwithstanding anything contained herein:

I. Our liability under this bank guarantee shall not exceed Rs. <Insert Value> (Rupees <Insert Value in Words> only).

II. This bank guarantee shall be valid up to <Insert Expiry Date>)

III. It is condition of our liability for payment of the guaranteed amount or any part thereof arising under this bank guarantee that we receive a valid written claim or demand for payment under this bank guarantee on or before <Insert Expiry Date>) failing which our liability under the guarantee will automatically cease.

Date _____

Place _____

Signature _____

Witness _____

Printed name _____

(Bank's common seal)

8. Annexure 7 (b) – Bank Guarantee for Earnest Money Deposit

To,

<Name>

<Designation>

<Address>

<Phone Nos.>

<Fax Nos.>

<Email id>

Whereas <<Name of the bidder>> (hereinafter called 'the System Integrator') has submitted the bid for Submission of RFP <<RFP Number>> dated <<Date>> for <<Name of the assignment>> (hereinafter called "the Bid") to <<Purchaser>> .

Know all Men by these presents that we <<... >> having our office at <<Address>> (hereinafter called "the Bank") are bound unto the << Purchaser >> (hereinafter called "the Purchaser") in the sum of Rs. <<Amount in figures>> (Rupees <<Amount in words>> only) for which payment well and truly to be made to the said Purchaser, the Bank binds itself, its successors and assigns by these presents. Sealed with the Common Seal of the said Bank this <<Date>>.

The conditions of this obligation are:

1. If the Bidder having its bid withdrawn during the period of bid validity specified by the Bidder on the Bid Form; or
2. If the Bidder, having been notified of the acceptance of its bid by the Purchaser during the period of validity of bid

(a) Withdraws his participation from the bid during the period of validity of bid document; or

(b) Fails or refuses to participate in the subsequent Tender process after having been short listed;

We undertake to pay to the Purchaser up to the above amount upon receipt of its first written demand, without the Purchaser having to substantiate its demand, provided that in its demand the Purchaser will note that the amount claimed by it is due to it owing to the occurrence of one or both of the two conditions, specifying the occurred condition or conditions.

This guarantee will remain in force up to <<insert date>> and including <<extra time over and above mandated in the RFP>> from the last date of submission and

any demand in respect thereof should reach the Bank not later than the above date.

NOTHWITHSTANDING ANYTHING CONTAINED HEREIN:

I. Our liability under this Bank Guarantee shall not exceed Rs. <<Amount in figures>> (Rupees
<<Amount in words>> only)
II. This Bank Guarantee shall be valid up to <<*insert date*>>)
III. It is condition of our liability for payment of the guaranteed amount or any part thereof arising under this Bank Guarantee that we receive a valid written claim or demand for payment under this Bank Guarantee on or before <<insert date>>) failing which our liability under the guarantee will automatically cease.

(Authorized Signatory of the Bank)

Seal:

Date:

9. Annexure 8 – Non-Disclosure Agreement

WHEREAS, we the undersigned Bidder, _____, having our principal place of business or registered office at _____, are desirous of bidding for RFP No. <<>> dated <<DD-MM-2017>> "**Selection of Master System Integrator And Cloud Service Provider for Integrated Data Centre for Smart Cities and City Integrated Command and Control Centers for the State of Madhya Pradesh**" (hereinafter called the said 'RFP') to the "[BSCDCL]", hereinafter referred to as 'Purchaser'

and,

WHEREAS, the Bidder is aware and confirms that the Purchaser's business or operations, information, application or software, hardware, business data, architecture schematics, designs, storage media and other information or documents made available by the Purchaser in the RFP documents during the bidding process and thereafter, or otherwise (confidential information for short) is privileged and strictly confidential and or or proprietary to the Purchaser,

NOW THEREFORE, in consideration of disclosure of confidential information, and in order to ensure the Purchaser's grant to the Bidder of specific access to Purchaser's confidential information, property, information systems, network, databases and other data, the Bidder agrees to all of the following conditions.

It is hereby agreed as under:

1. The confidential information to be disclosed by the Purchaser under this Agreement ("Confidential Information") shall include without limitation, any and all information in written, representational, electronic, verbal or other form relating directly or indirectly to processes, methodologies, algorithms, risk matrices, thresholds, parameters, reports, deliverables, work products, specifications, architecture, project information, security or zoning strategies & policies, related computer programs, systems, trend analysis, risk plans, strategies and information communicated or obtained through meetings, documents, correspondence or inspection of tangible items, facilities or inspection at any site to which access is permitted by the Purchaser.

2. Confidential Information does not include information which:
   a. the Bidder knew or had in its possession, prior to disclosure, without limitation on its confidentiality;

b. information in the public domain as a matter of law;
c. is obtained by the Bidder from a third party without any obligation of confidentiality;
d. the Bidder is required to disclose by order of a competent court or regulatory authority;
e. is released from confidentiality with the written consent of the Purchaser.

The Bidder shall have the burden of proving hereinabove are applicable to the information in the possession of the Bidder.

3. The Bidder agrees to hold in trust any Confidential Information received by the Bidder, as part of the Tendering process or otherwise, and the Bidder shall maintain strict confidentiality in respect of such Confidential Information, and in no event a degree of confidentiality less than the Bidder uses to protect its own confidential and proprietary information. The Bidder also agrees:

   a. to maintain and use the Confidential Information only for the purposes of bidding for this RFP and thereafter only as expressly permitted herein;
   b. to only make copies as specifically authorized by the prior written consent of the Purchaser and with the same confidential or proprietary notices as may be printed or displayed on the original;
   c. to restrict access and disclosure of Confidential Information to their employees, agents, consortium members and representatives strictly on a "need to know" basis, to maintain confidentiality of the Confidential Information disclosed to them in accordance with this clause; and
   d. to treat Confidential Information as confidential unless and until Purchaser expressly notifies the Bidder of release of its obligations in relation to the said Confidential Information.

4. Notwithstanding the foregoing, the Bidder acknowledges that the nature of activities to be performed as part of the Tendering process or thereafter may require the Bidder's personnel to be present on premises of the Purchaser or may require the Bidder's personnel to have access to software, hardware, computer networks, databases, documents and storage media of the Purchaser while on or off premises of the Purchaser. It is understood that it would be impractical for the Purchaser to monitor all information made available to the Bidder's personnel under such circumstances and to provide notice to the Bidder of the confidentiality of all such information.

   Therefore, the Bidder shall disclose or allow access to the Confidential Information only to those personnel of the Bidder who need to know it for the proper performance of their duties in relation to this project, and then only to the extent reasonably necessary. The Bidder will take appropriate steps to ensure that all

personnel to whom access to the Confidential Information is given are aware of the Bidder's confidentiality obligation. Further, the Bidder shall procure that all personnel of the Bidder are bound by confidentiality obligation in relation to all proprietary and Confidential Information received by them which is no less onerous than the confidentiality obligation under this agreement.

5. The Bidder shall establish and maintain appropriate security measures to provide for the safe custody of the Confidential Information and to prevent unauthorised access to it.

6. The Bidder agrees that upon termination or expiry of this Agreement or at any time during its currency, at the request of the Purchaser, the Bidder shall promptly deliver to the Purchaser the Confidential Information and copies thereof in its possession or under its direct or indirect control, and shall destroy all memoranda, notes and other writings prepared by the Bidder or its Affiliates or directors, officers, employees or advisors based on the Confidential Information and promptly certify such destruction.

7. Confidential Information shall at all times remain the sole and exclusive property of the Purchaser. Upon completion of the Tendering process and or or termination of the contract or at any time during its currency, at the request of the Purchaser, the Bidder shall promptly deliver to the Purchaser the Confidential Information and copies thereof in its possession or under its direct or indirect control, and shall destroy all memoranda, notes and other writings prepared by the Bidder or its Affiliates or directors, officers, employees or advisors based on the Confidential Information within a period of sixty days from the date of receipt of notice, or destroyed, if incapable of return. The destruction shall be witnessed and so recorded, in writing, by an authorized representative of the Purchaser. Without prejudice to the above the Bidder shall promptly certify to the Purchaser, due and complete destruction and return. Nothing contained herein shall in any manner impair rights of the Purchaser in respect of the Confidential Information.

8. In the event that the Bidder hereto becomes legally compelled to disclose any Confidential Information, the Bidder shall give sufficient notice and render best effort assistance to the Purchaser to enable the Purchaser to prevent or minimize to the extent possible, such disclosure. Bidder shall not disclose to a third party any Confidential Information or the contents of this RFP without the prior written consent of the Purchaser. The obligations of this Clause shall be satisfied by handling Confidential Information with the same degree of care, which the Bidder applies to its own similar Confidential Information but in no event less than reasonable care.

For and on behalf of:

(BIDDER)

Authorised Signatory	Office Seal:
Name:	Place:
Designation:	Date :

10. Annexure 9 - Consortium Agreement

DRAFT MEMORANDUM OF UNDERSTANDING EXECUTED BY MEMBERS OF THE CONSORTIUM

[On Non-judicial stamp paper of INR 100 duly attested by notary public]

This Memorandum of Understanding (MoU) entered into this day of [Date] [Month] 2015 at [Place] among _____ _____ (hereinafter referred to as "_____") and having office at [Address], India, as Party of the First Part and _____ _____ (hereinafter referred as "_____") and having office at [Address], as Party of the Second Part and _____ _____
(hereinafter referred as "_____") and having office at [Address], as Party of the Third Part.

The parties are individually referred to as Party and collectively as Parties.

WHEREAS DIT, Govt. of [state] has issued a Request for Proposal dated [Date] (RFP) from the Applicants interested in **Selection of Master System Integrator And Cloud Service Provider for Integrated Data Centre for Smart Cities and City Integrated Command and Control Centers for the State of Madhya Pradesh:**

AND WHEREAS the Parties have had discussions for formation of a Consortium for bidding for the said Project and have reached an understanding on the following points with respect to the Parties' rights and obligations towards each other and their working relationship.

AS MUTUAL UNDERSTANDING OF THE PARTIES, IT IS HEREBY AGREED AND
DECLARED AS FOLLOWS:

i. The purpose of this Agreement is to define the principles of collaboration among the Parties to:
    a. Submit a response jointly to Bid for the "**Selection of Master System Integrator And Cloud Service Provider for Integrated Data Centre for Smart Cities and City Integrated Command and Control Centers for the State of Madhya Pradesh"** as a Consortium.
    b. Sign Contract in case of award.

c. Provide and perform the supplies and services which would be ordered by the Purchaser pursuant to the Contract.

ii. This Agreement shall not be construed as establishing or giving effect to any legal entity such as, but not limited to, a company, a partnership, etc. It shall relate solely towards the Purchaser for "**Selection of Master System Integrator And Cloud Service Provider for Integrated Data Centre for Smart Cities and City Integrated Command and Control Centers for the State of Madhya Pradesh"** for and related execution works to be performed pursuant to the Contract and shall not extend to any other activities.

iii. The Parties shall be jointly and severally responsible and bound towards the Purchaser for the performance of the works in accordance with the terms and conditions of the BID document, and Contract.

iv. ---------- (Name of Party) shall act as Lead Partner of the Consortium. As such, it shall act as the coordinator of the Party's combined activities and shall carry out the following functions:

a. To ensure the technical, commercial and administrative co-ordination of the work package
b. To lead the contract negotiations of the work package with the Purchaser.
c. The Lead partner is authorized to receive instructions and incur liabilities for and on behalf of all Parties.
d. In case of an award, act as channel of communication between the Purchaser and the Parties to execute the Contract

v. That the Parties shall carry out all responsibilities as Developer in terms of the Project Agreement.

vi. That the broad roles and the responsibilities of each Party at each stage of the Bidding shall be as below:

Party A: _____

Party B: _____

Party C: _____

vii. That the broad roles and the responsibilities of each Party at each stage of the Project Execution shall be as below:

Party A: _____

Party B: _____

Party C: _____

viii. That the Parties affirm that they shall implement the Project in good faith and shall take all necessary steps to see the Project through expeditiously.

ix. That this MoU shall be governed in accordance with the laws of India and courts in [state] shall have exclusive jurisdiction to adjudicate disputes arising from the terms herein.

In witness whereof the Parties affirm that the information provided is accurate and true and have caused this MoU duly executed on the date and year above mentioned.

(Party of the first part) (Party of the second part) (Party of the third part)

Witness:

i. _____ _____
ii. _____ _____

11. Annexure 10 - Format for Power of Attorney to Authorize Signatory

POWER OF ATTORNEY

[To be executed on non-judicial stamp paper of the appropriate value in accordance with relevant Stamp Act. The stamp paper to be in the name of the company who is issuing the power of attorney.]

We, M/s._____ (name of the firm or company with address of the registered office) hereby constitute, appoint and authorise Mr. or Ms._____ (Name and residential address) who is presently employed with us and holding the position of _____, as our Attorney to do in our name and our behalf all or any of the acts, deeds or things necessary or incidental to our RFP for the Project _____ (name of the Project), including signing and submission of the RFP response, participating in the meetings, responding to queries, submission of information or documents and generally to represent us in all the dealings with Client or any other Government Agency or any person, in connection with the works until culmination of the process of bidding till the Project Agreement is entered into with _____ (Client) and thereafter till the expiry of the Project Agreement.

We hereby agree to ratify all acts, deeds and things lawfully done by our said Attorney pursuant to this power of attorney and that all acts, deeds and things done by our aforesaid Attorney shall and shall always be deemed to have been done by us.

(Add in the case of a Consortium)

Our firm is a Member or Lead bidder of the Consortium of _____, _____ and _____.

Dated this the _____ day of _____ 2015

(Signature and Name of authorized signatory)

_____

(Signature and Name in block letters of all the remaining partners of the firm Signatory for the Company)

Seal of firm Company

Witness 1: Witness 2:

Notes:

a. *To be executed by all the members individually.*
b. *The Mode of execution of the power of attorney should be in accordance with the procedure, if any laid down by the applicable law and the charter documents of the executant(s) and when it is so required the same should be under common seal affixed in accordance with the required procedure.*

12. Annexure 10 - Format for Power of Attorney for Lead bidder of Consortium

[To be executed on non-judicial stamp paper of the appropriate value in accordance with relevant Stamp Act. The stamp paper to be in the name of the company who is issuing the power of attorney]

Whereas _____ has invited RFP response for _____ (Name of the Project)

Whereas, the Members of the Consortium comprising of M/s._____, M/s._____, M/s._____ and M/s._____ (the respective names and addresses of the registered offices to be given) are interested in bidding for the Project and implementing the same in accordance with the terms and conditions contained in the RFP Documents.

Whereas, it is necessary for the members of the Consortium to designate one of them as the lead member with all necessary power and authority to do, for and on behalf of the Consortium, all acts, deeds and things as may be necessary in connection with the Consortium's RFP response for the Project.

NOW THIS POWER OF ATTORNEY WITNESSETH THAT

We, M/s._____ and M/s _____ and M/s_____ hereby designate M/s. _____
being one of the members of the Consortium, as the lead member of the Consortium, to do on behalf of the Consortium, all or any of the acts, deeds or things necessary or incidental to the Consortium's RFP response for the Project, including submission of the RFP response, participating in meetings, responding to queries, submission of information or documents and generally to represent the Consortium in all its dealings with Client or any other Government Agency or any person, in connection with the Project until culmination of the process of bidding till the Project Agreement is entered into with Client and thereafter till the expiry of the Project Agreement.

We hereby agree to ratify all acts, deeds and things lawfully done by our said Attorney pursuant to this power of attorney and that all acts, deeds and things done by our aforesaid Attorney shall and shall always be deemed to have been done by us or Consortium.

Dated this the _____ day of _____ 2017

_____

(signature)

_____

(Name in Block Letter of Executant) *[seal of Company]*

Witness 1 Witness 2

Notes:

To be executed by all the members individually, in case of a Consortium.
The Mode of execution of the power of attorney should be in accordance with the procedure, if any laid down by the applicable law and the charter documents of the executant(s) and when it is so required the same should be under common seal affixed in accordance with the required procedure.

13. Annexure 11: Common guidelines/ comments regarding the compliance of equipment/ systems

1. The specifications mentioned for various IT / Non-IT components are indicative requirements and should be treated for benchmarking purpose only. Bidders are required to undertake their own requirement analysis and may propose higher specifications that are better suited to the requirements.

2. Any manufacturer and product name mentioned in the Tender should not be treated as a recommendation of the manufacturer / product.

3. None of the IT / Non-IT equipment's proposed by the Bidder should be End of Life product. It is essential that the technical proposal is accompanied by the OEM certificate in the format given in Section 5.11 (Form 10) of Volume I of this Tender, where-in the OEM will certify that the product is not end of life & shall support for at least 7 years from the date of Bid Submission.

4. Technical Bid should be accompanied by OEM's product brochure / datasheet. Bidders should provide complete make, model, part numbers and sub-part numbers for all equipment/software quoted, in the Technical Bid.

5. Bidder should ensure that only one make and model is proposed for one component in Technical Bid for example all workstations must belong to a single OEM and must be of the same model etc.

6. Bidders 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.

7. All equipment, parts should be original and new.

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

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

10. 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 empanelled vendors) to ensure that the application is free from any vulnerability; and approved by the BSCDCL.

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

12. The Successful Bidder should also propose the specifications of any additional hardware/Non IT infrastructure, if required for the system.

13. The design consideration of the system is given in this volume. The Successful Bidder must provide the architecture of the solution it is proposing.

14. 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.

15. All the hardware and software supplied should be from the reputed Original Equipment Manufacturers (OEMs) and approved by BSCDCL.

16. All licenses should be in the name of the BSCDCL and should be Perpetual.

17. The proposed solution of MSI should meet the minimum specification requirements for respective component, bidder need to size the solution components to meet the project requirement. In case any of the system / appliance could not meet the performance requirement during the implementation testing or operations phase, MSI will be responsible to change the same with equivalent/better product without any additional cost to BSCDCL.

18. All components to be maintained in redundancy with Active - Active / Active-Passive Clustering based on the SLA requirements, architecture and performance. Bidder need to provide the compliance with respect to each clause and clear reference-able document, highlighting how the stated requirement is being met. All components should be sized to meet the required performance and SLA level when one of the redundant devices is down.

19. The proposed solution should be optimized for power, rack space, bandwidth while ensuring high availability and no single point of failure across the architecture.

20. The proposed systems and IT Infrastructure components like servers, storage, network etc. should be of enterprise class and must be current as per OEMs latest offering, in line with advancements of technology in these domains. Bidder need to provide the published benchmarks for the stated systems along with the sizing assessment sheet being certified by the OEM for the stated systems. All the components should be able to handle expected loads and provision the desired transaction times and throughputs.

21. The proposed systems and IT infrastructures components like servers, storage, network devices and software systems should be latest as per current technology trends and it should be upgradable. It is MSI's responsibility to proactively take care of system obsolescence planning. The systems should not become obsolescent before 5 years (of O&M). For proposed hardware and software systems, support from OEMs should be available for at-least 5 years (of O&M). Failing which it will be MSI's responsibility to provide support free of cost for initial 5 years of O&M.

22. Servers should be based on x86 platform in high density form factor to ensure optimal power and space usage. However, bidder may suggest rack form factor for any specific server usage, stating clearly the benefits being derived without compromising on the power and cooling factors.

23. The database layer should utilize the database servers for consolidating the database requirements. The architecture should have horizontal scalability. Benefits/additional security, reliability, availability features at the server level architecture would be given due consideration during evaluation

24. Redundancies/teaming should be maintained at different interconnecting fabrics so as to avoid any single point of failure / performance bottleneck

25. Networking equipment should be capable of processing IPV4 & IPV6 traffic. Security features that are delivered shall be IP v 6 ready.

26. All devices should be IPv4 and IPv6 ready from day-1. MSI shall deploy IPv4 and IPV6 dual stack supported network from day-1. The proposed solution and all appliances should meet this requirement. The MSI shall also be responsible for security adherence on both IPv4 and IPv6.

27. Bidder should utilize virtualization technology to optimise the solution and provide benefits for the overall Cost of ownership and ease of maintenance.

28. Proposed environment at DC should support set up and operations of multiple OEMs / brands of servers and storage without having any compatibility issue.

29. In future if BSCDCL plans to monetize the project, MSI should not have any objection. Rather it will be expected by the MSI to provide full support to BSCDCL.

30. If BSCDCL decides to retain the command centre operators (some or all or none) provided by MSI after the project tenure, MSI will not have any objection.

14. Annexure 12- ICCC -Design Consideration

a. Key Design Considerations

Key design considerations taken into account are as follows –

- System is Designed for Projected Population of 2031.
- 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

The key guiding principles considered for building the integrated Smart Governance solution are the following:

- **Transformational nature of Smart City applications** - Instead of imitating paper process in electronic form, applications should look to fully embrace mobile adoption, digital signature, online authentication, etc. to transform the processes completely and offer wider choice and no/low touch point for residents to interact directly. It is critical that project design are aligned to larger trends and designed for next decade rather than past.
- **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 like virtual environments ,creating sandbox), components coupled loosely to allow changes in sub-system level without affecting other parts, architected to work completely within a heterogeneous compute, storage, and multi-vendor environment. Simulated services environment can help agencies to save cost, Infrastructure and time in testing multiple application integrations.
- **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.
- **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.

- **Security and privacy of data** - Security and privacy of data within the integrated Smart City system 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.
- **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 10 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 BSCDCL 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 BSCDCL)
- **API Approach-** BSCDCL has decided to adopt Open API as the guiding paradigm to achieve the above goals. Though BSCDCL system would develop a portal but that would not be the only way for interacting with the BSCDCL 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 BSCDCL system. These applications will connect with the BSCDCL system via secure BSCDCL 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,
    - Consumption across technologies and platforms(mobile, tablets, desktops, etc.) based on the individual requirements
    - Automated upload and download of data

- Ability to adapt to changing taxation and other business rules and end user usage models
- Integration with customer software (GIS, Accounting systems).
- Simulated services environment can help agencies to save cost, Infrastructure and time in testing multiple application integrations.
- Open APIs should have a security and management layer for all interfaces.

- **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 behaviour. 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 BSCDCL Smart City system 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.

b. 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.

BSCDCL system will be built on the following core principles:

i. 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 BSCDCL system is

envisaged as a faceless system with 100% API driven architecture at the core of it. BSCDCL 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.

ii. 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. System shall use open standards and protocols like BPMN, BPEL, OWASP, WSDL, SOAP, etc.

iii. 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.

iv. 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.

v. 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.
- ***User Base*** **-** Must support Ten Thousand users (knowledge workers) with projected growth of 10 %/year. Concurrent users at peak time may be assumed to be at least 10% of the user base. The design of the Solution should be scalable to handle increasing number of users.
- ***Data Volume-*** Ability to support 20 % projected volume growth 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 Smart City system. Each of the logical layers would be loosely coupled with its adjacent layers
- **Data partitioning and parallel processing** - Smart City system 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** – Smart City system 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.

vi. 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/MSI 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.

vii. 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.

viii. 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:
    - 3 sec for welcome page
    - 5 sec for static pages
    - 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
    - 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.
    - 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)
    - Support the target packaging components like (Mobile Website, Hybrid App, Native App, Web App and Application Development, Eclipse tooling platforms)
    - Support the ability to write code once and deploy on multiple mobile operating systems
    - Support integration with native device API
    - Support utilization of all native device features
    - Support development of applications in a common programing language
    - Support integration with mobile vendor SDKs for app development and testing
    - Support HTML5, CSS3, JS features for smartphone devices
    - Support common protocol adapters for connection to back office systems (i.e. HTTP, HTTPS, SOAP, XML for format)
    - Support JSON to XML or provide XHTML message transformations
    - Support multi-lingual and language internalization
    - Support encrypted messaging between server and client components

ix. 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 BSCDCL system should be prevented
- Ensure minimum data loss(expected zero data loss)

x. 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.

xi. 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.

xii. 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.

xiii. 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

c. 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 Center while any external application of the Smart City ecosystem will reside in outside premises.

The need for a Service Oriented Architecture (SOA) and API Governance architecture is felt that will facilitate in defining an enterprise integration platform. An SOA and API Lifecycle Management 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 and help secure API based business critical transaction.

SOA /API is an architectural style that allows the integration of heterogeneous applications & users into flexible and lightweight 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 proposed integration architecture is depicted below. All real-time data integration across the enterprise applications will be through middleware based enterprise integration platform.

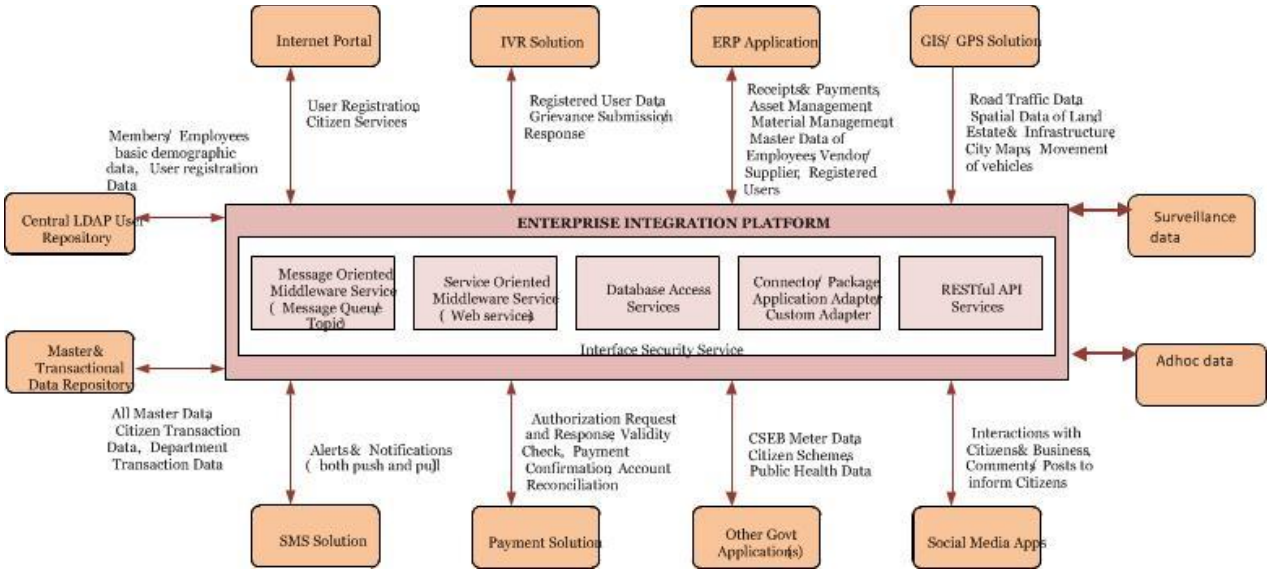


Figure 1: Integration Framework

The following are the various integration modes and techniques that could be leveraged -

- SOAP / REST 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 -
    - 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.
    - Should protects against threats and OWASP vulnerabilities and controls access with Single Sign-On and identity management, providing end-to-end security for apps, mobile, and IoT.
    - Solution should be able to protect against cross-site scripting (XSS), injection attacks (Xpath SQL , XQuery etc.) and DoS attacks.
    - SMS application, acting as the SMS Gateway, will make use of Java Communication 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.
    - 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
    - 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.

- GIS/GPS solution with traffic management, surveillance and land & estate management applications to capture the data pertaining to location traces left by GPS-enabled smartphones and Wi-Fi network logins, road traffic condition, movement of vehicles and spatial data of land, estate and Smart City infrastructure.

- Message based interfacing technique will be leveraged for real-time asynchronous integration mode. The following integration points could be considered for message based interfacing -
  - Central LDAP with ERP to synchronize member and employee user registration data
  - 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)
  - Employee attendance data with ERP (HR Module) to capture data pertaining to employee location and attendance
  - Departmental applications with ERP (Asset Management module) to exchange data for procurement and maintenance of any assets or infrastructure items for each department.
  - Municipal operations application with ERP (Material Management module) to capture materials related transaction and inventory data for public works
  - Other government applications with Smart City application to exchange data for government procurement, public health schemes, welfare schemes, citizen health and BEB meters.
- RESTful API service based interfacing technique will be leveraged for the following integration areas-
  - 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.
  - Access and use of various internal functions related to operations and administration of Smart City for departmental and 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 -
  - Initial data migration to cleanse, validate and load the data extracted from source systems into target tables

- 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 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.
    - The solution should have features to communicate across different services, process them and expose as single aggregate service to facilitate business functionality
    - ESB should support SOA standards such as XML, XSLT, BPEL, web services standards and messaging standards.
    - ESB should support all industry standards interfaces for interoperability between different systems
    - ESB should support the following integration security standards:
        - Authentication
        - Authorization
        - Encryption
        - Secure Conversation
        - Non-repudiation
        - XML Firewalls
        - Security standards support

- WS-Security 1.1
- WS-Trust 1.3
- WS-Secure Conversations 1.3
- WS-Basic Security Profile

- The solution should support routing to all internal & external systems.
- The solution should have comprehensive auditing capabilities to support any internal or external audits.
- The solution should provide configurable logging feature for supporting error handling.
- The solution should include feature of service registry for managing all services.
- The solution should support Business Activity Monitoring. One should be able to do a real time analysis of the data flowing within the ESB. One should be also able to monitor Key Performance Indicators.
- The solution should be able to interoperate and connect with applications deployed on a number of platforms including, AIX, HP-UX, Sun Solaris, Windows, Linux etc.
- The solution should support a whole suite of adapters such as Data Handler for XML, Exchange, Lotus Domino, industry standard packaged solutions etc.
- The solution should support various messaging patterns e.g. synchronous, asynchronous, pub/sub, multicast, etc.
- The solution should support SQL access to relational databases. Integration capabilities with NoSQL databases would be also advised.
- The proposed ESB should support Time Control and Notification for messaging
- The ESB should have an capabilities of Routing, Enrichment, Update, Transformation Processing
- The ESB should support for Message Expiry configuration

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 , 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 smart city. 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 for Voice Extensible Markup Language (VoiceXML)
- Should support speech recognition that interprets spoken words as texts (Advanced Speech Recognition).
- Should support playing of pre-recorded sounds
- 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
- Should provide provision for voice mailbox and voice recognition

There are multiple ways of integration of the solution with other systems is envisaged. These may be through Web Services, Message Queuing, File based or API based. The integration and data sharing mechanism may be either in Batch Mode or Needs basis (synchronous or asynchronous). Some of the key requirements of the interface/integration are mentioned below:

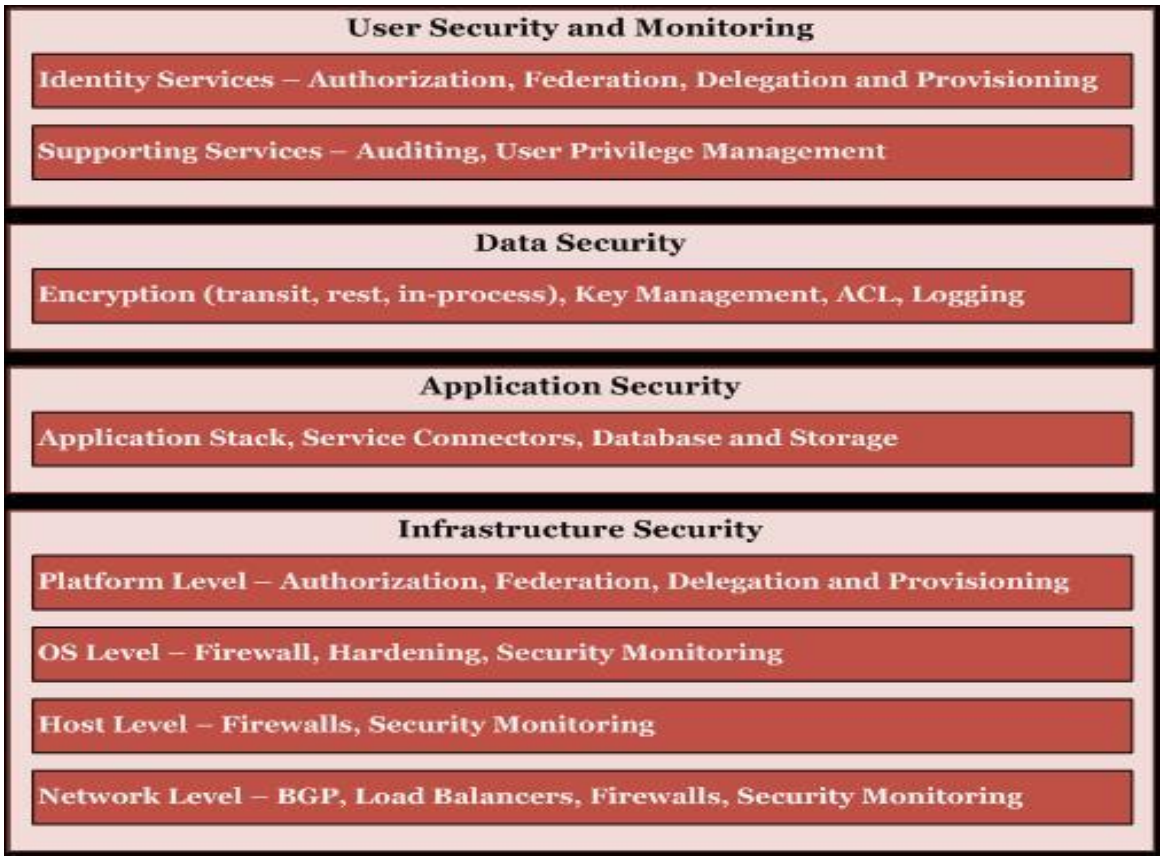
- Interface Definition
- Interface Owner
- Interface Type
- Interface Format
- Frequency
- Source System
- API/Service/Store Procedure
- Entitlement Service
- Consuming System
- Interface Layout (or) Schema

- Should have provision for exceptional scenarios
- Should have syntax details such as data type, length, mandatory/option, default values, range values etc.
- Error code should be defined for every validation or business rule
- Inputs and outputs should be defined
- Should be backward compatible to earlier datasets
- Data exchange should provide transactional assurance
- Response time and performance characteristics should be defined for data exchange
- The failover scenarios should be identified

d. Data exchange should be auditable

Data exchange should abide by all laws on privacy and data protection Security Architecture

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. A diagrammatic representation of the security framework for the envisaged Smart City system is provided below.



Some of the key security principles are explained below.

MSI must comply with the Cyber Security Model framework circulated vide Ministry of Urban Development's OM No. K-15016/61/2016-SC-I dated 20th May 2016 and another guidelines issued by MoUD for Control and Command Center.

i. 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 / software security token etc
- Something you are, such as a fingerprint, a retinal scan, or other biometric methods

Levels of Authentication

Based on the security requirements the following levels of authentication should be evaluated.

- For applications handling sensitive data it is recommended that in the least one factor authentication key in the form of a password is essential. Strong password complexity rules should be enforced to ensure confidentiality and integrity of the data
- For applications handling highly sensitive data it is recommended that two factor authentication mechanisms should be considered. The first line of defence 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.
- The solution should not store user passwords, hash of passwords and any pre-shared secret. It should only be a copy of the user credential, which should reside only with the user.

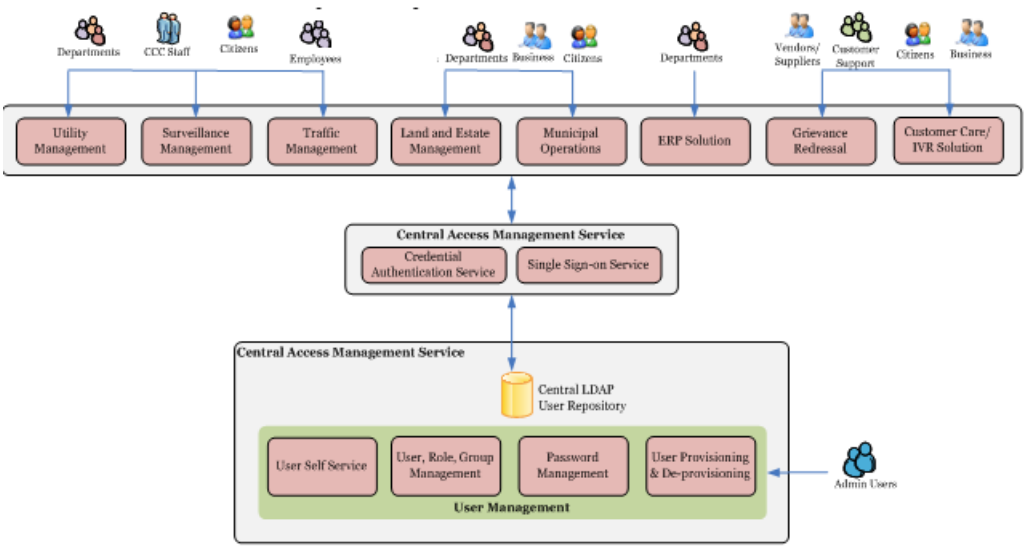
Centralized Identity and Access Management Model

It is recommended to adopt an enterprise level centralized authentication model that is secured and ensures that user has a single credential to access the all the services.

In this model there will a centralized authentication services with provision for centralized user registration and user credential store. A centralized user repository

(directory services) for the storage of user credentials will also store the authorization information for the user which will be used in different application.

The proposed centralized Identity and Access Management solution is depicted below –



Central Access Management Service

This service will provide the central authentication service for the users/groups created by verification of the user credentials against the central LDAP user repository. When a user tries to login to any centralized application e.g. single window portal, departmental sub-systems or ERP solution, the user credentials will be validated through the central authentication service.

Single Sign-On service will centrally maintain user session thus preventing user from multiple login when trying to access multiple applications.

Central Identity Management Service

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

User management service will cover user administrative functionalities like creation, propagation and maintenance of user identity and privileges.

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

The central user repository will store the user identity data and deliver it to other services (e.g. central authentication service) for credential verification. Adherence to LDAP v3 standard has been the dominant standard for central user repository

Enforce a robust and strong password policies that will allow users to change/reset password with password expiry and account lockout features, define and implement complex password rules and session timeout policies.

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

ii. Data Security

Traditional Structured Enterprise Data

MSI should protect Integrated Smart City System 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 defences 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 Smart City System are the following –

- Data security policies and standards to be developed and adopted across Smart City applications of all the cities 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:* should have extensive inbuilt security and access control mechanisms. Based on this, the system keeps track of the various functions accessed by any users.

Secure Big Data Environment

As the Integrated Smart City System will be capturing observation, interaction and monitoring data from various devices (like sensors, scanners, detectors, meters and cameras) and systems (like GIS, social media) on a real-time basis and processing them, it is imperative that the data repository will have the following characteristics - ability to handle large amounts of data, distributed redundant data storage, parallel task processing, extremely fast data insertion, extensible, centralized management and orchestration. This would necessitate considering the corresponding security concerns and countermeasures from a big data perspective.

It is essential to adhere to the following requirements for designing the big data security controls of Smart City system:

- No compromise with the basic functionality of the cluster
- Provision for scalability in line with the cluster
- No compromise with the essential big data characteristics
- Dealing with the security threat to big data environments or data stored within the cluster (refer the table below)

The key security concerns that must be addressed during design process are provided in the table below:

Technical Area	Security Concern	Description
Architecture	Distributed nodes to enable massive parallel computation	Difficulty in verifying security consistency across a highly distributed cluster of possibly heterogeneous platforms
Architecture	Replication into multiple copies and movement of big data to ensure redundancy and resiliency	Missing the centralized data security model where a single copy of data is wrapped in various protections until it is used for processing
Architecture	No built in security within big data stacks except service-level authorization and web proxy capabilities	Big data systems are built on the web services model with very few facilities to counter common web threats and hence vulnerable to well-known attacks

Technical Area	Security Concern	Description
Operation	No built in encryption method to protect data, copied from the cluster and at rest	Provision for encryption of data at rest to guard against attempts to access data outside established application interfaces is not present with most NoSQL variants. Moreover any external encryption tool selected needs to have adequate horizontal scalability and transparency to work with big data.
Operation	Lack of built-in facility to provide separation of duties between different administrators across the nodes	Each node in a big data system has at least one administrator with full access to its data. So any direct unwanted access to data files or data node processes can be addressed through a combination of access controls, separation of duties and encryption technologies, which are not available out-of-the-box for big data system.
Operation	Introduction of a corrupted node or service into a big data cluster through cloning of a node or exact replica of a client app or service	Big data system like Hadoop uses Kerberos to authenticate users and add-on services to the cluster. But a corrupt client can be inserted onto the network using credentials extracted from virtual image files or snapshots.
Operation	No built-in monitoring to detect misuse or block malicious queries	All the available external monitoring tools review data and user requests only at the API layer of the big data system

The implications for taking into consideration the above security concerns for a big data environment and the related requirements of security controls for the Smart City System are the following -

- Kerberos, already built in the Hadoop infrastructure, has to be set up for validating inter-service communication, helping to keep corrupt nodes and application out of the big data cluster, protecting web control access and making administrative functions harder to compromise.
- File layer encryption needs to be established for consistent protection from credentialed user access and multi-key support across different platforms regardless of OS/platform/storage type, while ensuring that this encryption is transparent to both Hadoop and calling applications and scales out as the cluster grows.
- Key management service needs to be leveraged to distribute keys and certificates, and manage different keys for each group, application and user in order to prevent access of encryption keys to an attacker.
- Validation process for patches, application configuration, machine images, certificates and Hadoop stack must be in place prior to deployment in a multi-node environment.
- Audit Capabilities: The system provides for a system-wide audit control mechanism that works in conjunction with the big data environment.
- Secure Communication: SSL/TLS implementation technique needs to be used for secure communication between two nodes or between a node and an application.

- Logging: Collection and management of event data through logging within the big data cluster has to be ensured in order to keep the records of activity for detecting attacks, diagnosing failures or investigating unusual behaviour.

Additionally for any service based on cloud environment, there are three main security challenges namely multi-tenancy, divided responsibility and dynamic environment. In this context, one of the key concerns for the customers would be protection of sensitive/confidential/personal data through access control, encryption, integrity and origin verification.

In cloud environments, the amount of data at rest, in transit and in use is considerably larger than in traditional networks. So the following technologies should be considered to discover and remedy security vulnerabilities related to integrity protection of data to be used by the IT systems of Smart City. They can be used separately or can complement each other in achieving desired outcome.

- Symmetric cryptography: It utilizes the same shared key to encrypt plain text message from the sender and decrypt cipher text for the recipient, and thus is relatively faster in processing large volume of data.
- Public key infrastructure (PKI): It utilizes public-private key pairs to verify the integrity of data.
- Keyless Signing Infrastructure (KSI): It utilizes data hashes and hash trees for generating and publishing a root hash for the data to be integrity protected. It then verifies the data integrity using signature tokens that enable data verification using the previously published root.

KSI technology does not rely on a single key that could be breached and no key is needed to verify if data matches the root hash. Hence it provides greater efficiency in the context of big data.

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.

iii. Application Security

- Smart City system 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
- Smart City system should have Role based access, encryption of user credentials. Application level security should be provided through leading practices and standards including the following:
    - Prevent SQL Injection Vulnerabilities for attack on database
    - Prevent XSS Vulnerabilities to extract user name password (Escape All Untrusted Data in HTML Contexts and Use Positive Input Validation)
    - Secure Authentication and Session Management control functionality shall be provided through a Centralize Authentication and Session Management Controls and Protect Session IDs from XSS
    - 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
    - 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)
    - 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
    - Prevent Insufficient Transport Layer Protection Vulnerabilities (enable SSL for all sensitive pages, set the secure flag on all sensitive cookies and secure backend connections
    - Prevent Id Redirects and Forwards Vulnerabilities
    - 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.

iv. Infrastructure Security

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

Physical Security of ICCC Premises

- MSI will be required to do the physical security arrangements for the ICCC premises during contract period.

- MSI will be required to manage the access cards and access control for ICCC premises during contract period.

- MSI will be required to provide security guards at the ICCC premises during contract period.

- Physical security arrangements should be 24*7, as the operations of ICCC is conceived to be 24*7.

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

Software Defined Security at Application End Points

- Deploy Software Defined Security Architecture at the Virtualization layer at the Host level to guarantee that each and every Application gets its security policy and enforcements at the point closest to its existence.

- The Software Defined Security (SDS) architecture should be able to enforce the Security Policy at the Virtual NIC level of the Application VM thus offering highest and closest level of security.
- The SDS should allow the Firewall Policy to be tied to each Virtual Machine and the policy should automatically move with the movement of the Virtual Machine, thus bringing Security Policy Portability.
- The Software Defined Security Architecture offers the integration of Industry leading solutions around Antivirus, Anti Malware, IPS, Next Generation Firewall etc. to be integrated in the Security Policy template through Service Insertion or Service Chaining.
- The SDS Framework to be deployed which should create virtual / logical Application or Service isolation from each other, dynamically controlled through template or blueprint, thus creating an environment or architecture of Risk or Breach Containment, post any successful security breach.
- The SDS should be able to instantaneously provision security policy through templates or by creating unique Security Groups of the VMs based on Operating Systems, Workload Type (Web, App or DB), Machine Name, Services running, Regulatory requirement etc. and apply Automated and Centralised Security Policy based on this context or grouping.

e. Software Development Lifecycle

Continuous Build and Deployment

The Bhopal Smart City system 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.

At its core, Continuous Delivery is all about releasing high-quality software to the market faster and with less effort—a simple goal, but one that requires new thinking around the people, processes and technologies driving your application delivery efforts.

A set of practices and principles in software engineering aimed at, building, testing and releasing software, faster and more frequently. These principles help reduce the cost, time and risk of delivering changes, and ultimately value, to customers by allowing for more incremental changes to applications in production.

With an application release automation, teams can easily plan and create a comprehensive release plan that incorporates tasks performed by third party tools and orchestrates the promotion from one environment to the next, streamlining the entire process to eliminate hand-offs.

Simplifying build and configuration of new environment instances means testing can occur early and often. Defects and errors are found sooner in the cycle to significantly reduce re-work. Teams have easy access to the test data they need to create real-world

'production-like' environments that enable more thorough testing and yield more accurate results, so errors or defects are discovered long before an app is deployed to production, so there's no negative impact to customer experience.

A dedicated 'development / customization' environment should be proposed and setup. The MSI must provision separate development and testing environment for application development and testing to simplifying build and configuration of new environment instances means testing can occur early and often. Defects and errors are found sooner in the cycle to significantly reduce re-work. Teams have easy access to the test data they need to create real-world 'production-like' environments that enable more thorough testing and yield more accurate results, so errors or defects are discovered long before an app is deployed to production, so there's no negative impact to customer experience. 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.

f. Quality Assurance & Audit

A thorough quality check is proposed for the Bhopal Smart City system 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 BSCDCL. 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.
- Using simulated test environment in order to find the defects and bugs in much earlier SDLC so that they do not escape into next phase/environment.

- Indicate / demonstrate to BSCDCL that all applications installed in the system have been tested.

i. Automated Testing

MSI is expected to perform automated testing with following features:

- Should support multi-layer test scenarios with a single solution.
- Should support and execute testing on GUI and UI-Less (standard Web Services, non-SOAP Web Services, such as REST, etc.) Components.
- Should allow version control of tests and test assets providing ability to compare versions and identify changes.
- Should allow centralized storage and management of tests and test assets including external resources used by tests.
- Should have an IDE environment for QA engineers which should be configurable.
- Should provide local system monitoring to test and validate performance issues including memory leakage, CPU overload and network overload to determine if specific business scenarios exceed desired performance thresholds.
- Should provide Auto-documentation while creating of automated tests.
- Should generate reports that can diagnose defects and can be exported to (PDF, XML , Html) (mandatory) and doc (optional) formats.
- Report with summary data, pie charts and statistics for both the current and previous runs needs to be provided.
- Should enable thorough validation of applications through a full complement of checkpoints such as GUI object, database, XML, XPath, etc.
- Should provide Unicode support for multilingual application testing.
- Should be able to record the test Execution into a video file for viewing later.
- Should provide facility to parameterize tests to generate/assign test case output values automatically during runtime.

ii. 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 Bhopal Smart City system 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.

iii. Audits & Inspections

MSI is expected to perform the following activities for overall ICCC Audits & Inspections organized by BSCDCL or its authorized agency:

- Should provide necessary information at the time of such activities
- Should provide necessary environment and access to the authorized personal for conducting such activities

- Should provide necessary evidences for Audits (if asked by the auditor / inspector) at the time of such activities.

15. Annexure 13 : Change Control Note

Change Control Note	**CCN Number:**
Part A: Initiation	
Title:	
Originator:	
Sponsor:	
Date of Initiation:	
Details of Proposed Change	
(To include reason for change and appropriate details/specifications. Identify any attachments as A1, A2, and A3 etc.)	
Authorized by BSCDCL	Date:
Name:	
Signature:	
Received by the Bidder	Date:

Name:	
Signature:	

Change Control Note	**CCN Number:**
Part B :	**Evaluation**

(Identify any attachments as B1, B2, and B3 etc.)

Changes to Services, payment terms, payment profile, documentation, training, service levels and component working arrangements and any other contractual issue.

Brief Description of Solution:

Impact:

Deliverables:

Timetable:

Charges for Implementation:

including a schedule of payments)	
Other Relevant Information: (including value-added and acceptance criteria)	
Authorized by the Bidder	**Date:**
Name:	
Signature:	
Change Control Note	**CCN Number :**
Part C : Authority to Proceed	
Implementation of this CCN as submitted in Part A, in accordance with Part B is: (tick as appropriate)	
Approved **Rejected** **Requires Further Information** (as follows, or as Attachment 1 etc.)	
For BSCDCL and its nominated Agencies	**For SI**
Signature	Signature
Name	Name
Title	Title
Date	Date

16. Annexure 14: Form of Agreement

THIS Agreement made the .....date of.....2016, between.....(hereinafter.....referred to as the "MSI") of the one part and ..... (hereinafter called the "BSCDCL") of the other part.

WHEREAS MSI has the required professional skills, personnel and technical resources, has agreed to provide the Services on the terms and conditions set forth in this Contract and is about to perform services as specified in this RFP .....(hereinafter called "works") mentioned, enumerated or referred to in certain Contract conditions, specification, scope of work, other sections of the RFP, covering letter and schedule of prices which, for the purpose of identification, have been signed by ..... on behalf of the .....
SI and .....(the BSCDCL) on behalf of the BSCDCL and all of which are deemed to form part of the Contract as though separately set out herein and are included in the expression "Contract" whenever herein used.

NOW, THEREFORE, IT IS HEREBY AGREED between the parties as follows:

a. The BSCDCL has accepted the tender of MSI for the provision and execution of the said works for the sum of .....upon the terms laid out in this RFP.
b. SI hereby agrees to provide Services to BSCDCL, conforming to the specified Service Levels and conditions mentioned
c. The following documents attached hereto shall be deemed to form an integral part of this Agreement:

Complete Request for Proposal (RFP) Document	*RFP and corrigendum and addendum, if any*
Break-up of cost components	*Lead Bidder's Commercial bid*
The BSCDCL's Letter of Intent dated <<>>	*To be issued later by the BSCDCL*
SI's Letter of acceptance dated <<>>	*To be issued later by the SI*
Bid submitted by MSI as per file No. <<>>	

d. The mutual rights and obligations of the "BSCDCL" and MSI shall be as set forth in the Agreement, in particular:
   - SI shall carry out and complete the Services in accordance with the provisions of the Agreement; and
   - the "BSCDCL" shall make payments to MSI in accordance with the provisions of the Agreement.

NOW THESE PRESENTS WITNESS and the parties hereto hereby agree and declare as follows, that is to say, in consideration of the payments to be made to MSI by the BSCDCL as hereinafter mentioned, MSI shall deliver the services for the said works and shall do and perform all other works and things in the Contract mentioned or described or which are implied there from or there in respectively or may be reasonably necessary for the completion of the said works within and at the times and in the manner and subject to the terms, conditions and stipulations mentioned in the said Contract.

AND in consideration of services and milestones, the BSCDCL shall pay to MSI the said sum of .....or such other sums as may become payable to MSI under the provisions of this Contract, such payments to be made at such time and in such manner as is provided by the Contract.

IN WITNESS WHEREOF the parties hereto have signed this deed hereunder on the dates respectively mentioned against the signature of each.

Signed	Signed
Name : _____	Name : _____
Designation : _____	Designation : _____
Date :	Date :
Place :	Place :
in the presence of :	**in the presence of :**
Signed	Signed
Name : _____	Name : _____
Designation : _____	Designation : _____
Date :	Date :
Place :	Place :

17. Annexure 15: Details of ICT Systems of Smart Cities in Madhya Pradesh

Current ICT based systems of Bhopal City and integration scope

There are various state of the art IT systems/initiatives already deployed in the city or being deployed. Following are the few important IT systems of the city and their features. BSCDCL envisages to integrate these IT systems with command and control center of smart city Bhopal.

Sl. No	List of Services	Brief of Scope for Integration
1	Integration of Smart Parking	• ICCC will be required to integrate with CCDCSC and command center of the Smart Parking solution, which is a PAN City initiative. • ICCC will be required to receive feeds on the status of parking across the city which are managed by the Smart Parking command center (feeds received from all the edge devices of the Parking Solution). • These feeds will provide information of available, non-available parking slots, functional and non - functional parking slots. • ICCC will also be required get video feeds from the parking areas on real-time basis. • Such video feeds will only be saved for 7 days. • These video feeds will also help monitor assets of Municipal corporations, MPUADD. • All the information received will also be required to be mapped on the GIS map. • All the information received from the smart parking command center will also go into the Analytical layer which will help city in better planning and running of operations. • ICCC should also be able to trigger the commands / alerts (if required) to the respective command center. • This initiative is under Municipal Corporations.
2	Integration of Public Bike Sharing	• ICCC will be required to integrate with the CCDCSC and command center of the Public Bike Sharing solution, which is a PAN City initiative. • ICCC will be required to receive feeds on the status of utilization of public bike sharing docks across the city. • These feeds will provide information of available, non-available cycles in slots, functional and non - functional PBS stations. • ICCC will also be required get video feeds from the PBS stations on real-time basis. • Such video feeds will only be saved for 7 days.

		• These video feeds will also help monitor assets of MCs, MPUADD and respective authorities. • ICCC will also be required to get information regarding the position of the cycles deployed under the PBS project. • All the information received will also be required to be mapped on the GIS map. • All the information received from the PBS command center will also go into the Analytical layer which will help city in better planning and running of operations. • ICCC should also be able to trigger the commands / alerts (if required) to the respective command center.
3	Integration of Smart Pole & Smart Lighting	• ICCC will be required to integrate with CCDCSC and command center of Smart Poles (Pan City Initiative) to receive all kinds of feeds such as environment sensor, lighting sensors. Video, etc. • ICCC will be required to get information on the status of working of the installed LED lights, as well as other sensors and other cameras. • ICCC will also get real-time video feed from the installed Smart Poles. • Such video feeds will only be saved for 7 days. • These video feeds will also help monitor assets of MCs and respective authorities. • All the information received will also be required to be mapped on the GIS map. • All the information received from the Smart Pole command center will also go into the Analytical layer which will help city in better planning and running of operations. • ICCC should also be able to trigger the commands / alerts (if required) to the respective command center.
4	Integration of Solid Waste Mgmt. Services (Tracking of Solid Waste Vehicles)	• ICCC will be required to integrate with the control room of Solid Waste Vehicle tracking project (Pan City Initiative) to receive feeds on the location of the solid waste vehicles. • ICCC will also get other information which is received in the control room 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 center will also go into the Analytical layer which will help city in better planning and running of operations. • ICCC should also be able to trigger the commands / alerts (if required) to the respective command center. • This initiative is managed respective Municipal Corporations.

5	Integration of Intelligent Traffic Management System (Police)	• ICCC will be required to integrate with Command Center of Traffic Management System, to receive real-time feeds of the camera installed by them. • These video feeds will not be saved, but will be utilized in Analytical layer to help administration monitor its assets and do a better urban planning. • ICCC will also be required to send video feeds received from Smart Parking, Smart Pole, PBS in real-time basis to the command center of Traffic (if required). • ICCC should also be able to trigger the commands / alerts (if required) to the respective command center.
6	Integration of MCs Call Centre & Municipal Services (Web portal and Mobile applications)	• ICCC will be required to integrate its helpdesk and system with Municipal Corporations call center, in case if there is some information or notification is to be sent to Municipal Corporations call center for doing some action in the field regarding Municipal Corporation work. • All the information received from the command center will also go into the Analytical layer which will help city in better planning and running of operations. • ICCC will be required to integrate with the backend system of Bhopal Municipal Corporation services which is SAP based system to monitor the performance of the application. • Along with this ICCC should be able to show the utilization by citizens of various sections of any mobile application in the form of a Dashboard. • ICCC should be able to integrate with the existing ICT systems and edge / end / mobile devices of various Municipal Corporations departments such as Garden, General Administration Department, Water Supply, Sewerage, Assessment and Collection (Property Tax, Shops and establishment), Fire (Fire Brigade Section), Transport of Heavy Vehicles and Maintenance (Workshop), Audit and License Issue to receive and send information. • ICCC should be able to map the data received from various Municipal Corporations departments on its GIS Platform. • ICCC will be required to send Municipal Corporations field agents alerts and notifications for any emergency / incidents / disaster in the city for doing required action. ICCC system should also be able to get acknowledgement from the receivers.

7	Integration with Smart MAP (GIS)	• ICCC will be required to use the GIS platform developed by SPVs of respective smart city. • There will be a requirement for enhancing the existing platform and using it in the ICCC for doing all the necessary actions. • This is an ESRI based platform with almost 96 layers. • Along with this ICCC should be able to show the utilization by citizens of various sections of Bhopal Plus application in the form of a Dashboard. • All the information received from the application will also go into the Analytical layer which will help city in better planning and running of operations.
8	Integration with Mobile App (e.g. Bhopal Plus)	• ICCC will be required to integrate with the backend system of Bhopal Plus to monitor the performance of the application. • Along with this ICCC should be able to show the utilization by citizens of various sections of Bhopal Plus application in the form of a Dashboard. • All the information received from the application will also go into the Analytical layer which will help city in better planning and running of operations.
9	Integration with DIAL 100	• ICCC will be required to integrate with the command center of DIAL 100, which is a public safety initiative by Police Department. ICCC will be required to get information regarding the location and other details of DAIL 100 vehicles present in Bhopal area. • Such information will be useful in case of incident / disaster management for the city. • All the information received from the command center will also go into the Analytical layer which will help city in better planning and running of operations. • ICCC should also be able to trigger the commands / alerts (if required) to the respective command center. • ICCC will be required to integrate to send the alerts and notifications for any emergency / incidents / disaster in the city for doing required action.
10	Integration with DIAL 108 & Jannani Express	• ICCC will be required to integrate with the command center of DIAL 108 and Jannani Express, which is a public health initiative by Health Department. ICCC will be required to get information regarding the location and other details of DAIL 108 & Jannani Express vehicles present in Bhopal area. • Such information will be useful in case of emergency / incident / disaster management for the city.

		• All the information received from the command center will also go into the Analytical layer which will help city in better planning and running of operations. • ICCC should also be able to trigger the commands / alerts (if required) to the respective command center. • ICCC will be required to integrate to send the alerts and notifications for any emergency / incidents / disaster in the city for doing required action.
11	Integration with Transport Management System (e.g. BCLL)	• ICCC will be required to integrate with command center of BCLL to get all kinds of feeds from Transport Management 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 center will also go into the Analytical layer which will help city in better planning and running of operations. • ICCC should also be able to trigger the commands / alerts (if required) to the respective command center.
12	Integration with CCTV Surveillance (Police Dep't.)	• ICCC will be required to integrate with Command Center of CCTV System, to receive real-time feeds of the camera installed by them. • These video feeds will not be saved, but will be utilized in Analytical layer to help administration monitor its assets and do a better urban planning. • ICCC will also be required to send video feeds received from Smart Parking, Smart Pole, PBS in real-time basis to the command center of Police (if required). • ICCC should also be able to trigger the commands / alerts (if required) to the respective command center.
13	Integration with Dynamic Market Place (e.g. Mayor Express)	• ICCC will be required to integrate with the backend system of Dynamic Market Place (Mayor Express) to monitor the performance of the application. • Along with this ICCC should be able to show the utilization by citizens of various sections of Dynamic Market Place application in the form of a Dashboard. • All the information received from the application will also go into the Analytical layer which will help city in better planning and running of operations. • This is Municipal Corporations initiative.

14	Integration with Emergency Response and Disaster Mgmt.	• ICCC will be required to integrate with existing ICT system of the Emergency Response and Disaster Management to send them alerts and notifications for any emergency / incidents / disaster in the city for doing required action. • ICCC system should also be able to get acknowledgement from the receivers. • All the information received from the application will also go into the Analytical layer which will help city in better planning and running of operations.
15	Integration with Water Management System	• ICCC will be required to integrate Water Management System control room to get all kinds of sensor and edge devices feeds. • ICCC should be able to map this information on the GIS layer and help authority monitor the water management of the city. • ICCC should also be able to trigger the commands / alerts (if required) to the respective command center. • All the information received from the application will also go into the Analytical layer which will help city in better planning and running of operations.
16	Integration with Met Department (Local Weather Forecast)	• ICCC should be able to receive real-time data on the weather forecast from Met Department and map the same on its platform as well as GIS layer. • All the information received from the application will also go into the Analytical layer which will help city in better planning and running of operations. • This information will also help in predictive analysis for urban planning based on weather forecast.
17	Integration with Area Based Development (ABD) Services: i. Utilities ii. Lighting iii. Metering iv. Surveillance	• ICCC will be required to integrate with control rooms / systems all the listed services of the Area Based development (ABD). • These services are planned for the near future. • ICCC will be required to get all kinds of feeds from all the sensors / edge devices installed for these services in the field. • In case of video feeds, feeds will only be saved for only 7 days. • ICCC will be required to monitor these services in real-time and manage the operations of these services. • All the information received from the application will also go into the Analytical layer which will help city in better planning and running of operations. • This information will also help in predictive analysis.

18	Integration of Crowdsourcing Data with ICCC	MSI has to make provision in the ICCC for receiving the data from crowdsourcing and perform standard operation at ICCC. It is planned to collect data as part of future IT initiative under which citizen of Bhopal would be sharing data. Received data would be part of existing data repository where data is received from various type of sensors owned by Bhopal smart City. All the operations like data analytics will be performed on the received data through crowdsourcing too. Connectivity between end devices and ICCC will be provided by MPUADD. For example, in near future if any resident welfare society intends to share data with MPUADD (ICCC) for surveillance purpose, this video feed would be received at ICCC and become part of other feeds coming from various CCTV camera installed in the city by MPUADD.
19	Integration with Fire Brigade Control System	Fire brigade section is the part of Bhopal Municipal Corporation. There are 18 fire brigade vehicles and 15 motor bikes are available to cater to whole city. Municipal Corporations has plans to strengthen and upgrade the fire brigade control system of the city. MSI has to integrate the city fire brigade control system with ICCC. This will help Municipal Corporations in efficient usage of its resources and to achieve minimum response time in case of rescue operations. For example: If the ICCC receives information about fire in the city, the ICCC should able to trigger a command to appropriate fire station and its vehicle which can reach within minimum time with guidance about traffic conditions and shortest route.
20	Integration with Solar Roof Top Project	• ICCC will be required to integrate the energy management system of solar roof top project to get all kinds of sensor and edge devices feeds. • ICCC should be able to map this information on the GIS layer and help authority monitor the energy management system of the city. • ICCC should also be able to trigger the commands / alerts (if required) to the respective stakeholders. • All the information received from the application will also go into the Analytical layer which will help city in better planning and running of operations.

Smart Parking

The objective of Smart Parking is to better manage the parking areas of the city and provide seamless information to users of parking slots. Smart Parking is a pan city initiative for all the parking areas which falls under purview of Municipal Corporations and managed by Municipal Corporations. Under this minimum 60 parking areas will

be managed. Minimum 6500 two wheelers and 3500 four wheelers parking slots will be managed under smart parking project. There will be a sensor based smart parking solution, one sensor for each parking slot which will help in better manage and knowing the status of parking slot and subsequently provide parking availability status to end users.

Public Bike Sharing

Public bike sharing system is a service in which bikes will be made available to the citizens of Bhopal city on shared basis. Public bike sharing project will allow citizens to borrow a bike from one point and return it at another point. Following are the main features of public bike sharing system:

a. There will be 50 Stations, 500 smart Bicycles across the city with onboard computer and GPS
b. Fare Collection device on each smart bicycle – using NFC, Smart Card and Pin Code
c. The central control system collects data from each station for efficient planning and operation of the system.
d. This data is used to make decisions on redistribution of cycles around stations during the hours of operations.
e. The Cycle sharing system is also being integrated with the fare collection system of the BRT system to aid the multimodal integration.

Smart Pole

The smart Pole or intelligent pole project envisage installation of 400 poles across the city. Each smart pole will be equipped with multiple utilities like CCTV cameras, environmental sensors, Wi-Fi services, Smart LED Lights. Following are the key features of this project:

a. Converting 20000 traditional street lights to LED based intelligent lights
b. 400 Smart poles with capability to accommodate multi operator telecom Base Stations for 2G/3G/LTE to reduce mobile call drops
c. 400 Surveillance cameras inbuilt into smart poles
d. Wi-Fi hotspots - 100
e. Interactive Digital Signage for traffic & business - 400
f. Environment sensors – 100
g. 48 core , 200 km of citywide Optical Fiber Cable network to enable connected communities
h. Network/cloud controlled EV Charging at 100 poles
i. State of the art control and command center (for smart poles) for the O&M of services for 15 years

Solid Waste Management Services

Principally Solid Waste Management refers to control of generation, storage, collection, transport or transfer, processing and disposal of solid waste materials in a way that best addresses the range of public health, conservation, economics, aesthetic, engineering and other environmental considerations. Under this project all the vehicles involved in collection of solid waste are being tracked. Following are the key attributes of this project:

a. Installation of GPS devices on all the vehicles, RFID Tags, RFID Readers.
b. GPS Based Application software (Vehicle Tracking System) integrated with GPS, RFID devices
c. GPS/GPRS System, RFID, fuel sensors for all vehicles. Minimum number of vehicles is 300 (232 current).
d. Cloud based data center
e. Infrastructure including Server and Control center (with video wall). Software with MIS reports.
f. Provision for alerts to the Central Command center on Scheduled Missed Trips, over speeding vehicles, unauthorized stoppage and /or non-stoppage of the vehicles at designated bins & route deviation by vehicles etc.

Intelligent Transport Management System

"Intelligent Traffic Management System (ITMS) includes setting up Automatic Number Plate Recognition (ANPR) system, Red Light Violation Detection (RLVD) Cameras with E-Challan System at specified locations of Bhopal City. Following are the key features of ITMS system.

a. All buses equipped with GPS based Automatic Vehicle Location System (AVLS) connected with Central Control and Command Center (of ITMS).
b. Real time tracking and monitoring of Bus Operations.
c. 16 Ft X 6 Ft Video Wall comprising of 08 Nos. of High Resolution LED Panels at Control room.
d. Bus Stops are connected with Command Center reflecting Expected Time of Arrival (ETA) on Passenger Information System (PIS)
e. All the buses are equipped with 04 Nos. of PIS in buses and PAS in buses. .
f. Signal Priority for BRTS buses
g. Automatic Fare Collection
h. Number of Bus Stops – 100
i. Number of Buses – 225 (in future 300)
j. Real time tracking and monitoring of bus operations
k. Bus stops are connected with command center

Municipal Corporations Call Center

Municipal Corporations call center is a public grievances redressal system related to municipal services. All the issues /complains related to municipal services are addressed by Municipal Corporations call center. Citizen of Bhopal city residing in Bhopal municipal area can call the call center and register their complaints. In future Municipal Corporations call center will also be used as one of the channels for taking request for dynamic market place.

Bhopal Smart Map (GIS)

Smart Map is a web-GIS portal developing as part of Bhopal Smart City Project, a web-based application addresses issues affecting urban areas, through GIS based plans adopting smart city concept. GIS provides an effective and efficient way to handle infrastructure and asset related data and its associated attribute information from multiple sources for better decision support, improved governance and to deliver better citizen services. It aims to facilitate the citizens of Bhopal with various services. The portal allows the public to easily discover and search for geospatial and textual data, though modules like know your ward. It enables users to view multiple data layers on a map and perform various functions for data analysis like search and query. The advanced search and query tools enables users to search for specified features like Landmarks, Heritage sites, Museum etc., based on the map layers.

a. 96 layered GIS cutting across departments.
b. Citizen portal - Map visualization module, Query module, and location based information module, education, health services, public feedback, transport, cultural and community events.
c. Property and other taxes.
d. Heritage

Bhopal Plus (App)

Bhopal Plus is a mobile application. It is an integrated platform enabling and promoting "Collaborative Participatory Governance, Centralized Citizen Service Delivery, Live City Feeds, Citizen Grievance Redressal, etc. The goal of the platform is to make citizen engagement an integral part of policy planning and implementation. Following are the key features of Bhopal Plus:

a. Citizen Collaboration platform
b. Citizen Services (G2C & B2C)
c. Smart city dashboard
d. Grievance Redressal
e. Integration with external apps (Dynamic market place, women safety application, etc.)

Municipal Corporations Municipal Services

These are pan city citizen services, which are hosted using SAP based web application and

they are also hosted on Bhopal plus mobile application, these services include:

a. Water Tax;
b. Property Tax;
c. Birth Registration;
d. Death Registration;
e. Marriage Registration; etc.

There are some more services of various Municipal Corporations departments such as Water Supply, Sewerage, Assessment and Collection (Property Tax, Shops and establishment), Fire Protection (Fire Brigade Section.

Water Management System

Municipal Corporations manages the water supply system of the city, which was previously dependent on two sources viz., the Kolar dam which supplies 155 MLD to southern, eastern and central parts of the city and the Upper Lake with 105.75 MLD supplies central and northern parts of the city. These two sources are rain fed and hence, were susceptible to seasonal variations. In addition to these there are 1104 tube-wells accounting to approximately 50 MLD supply supplemented through Ground water.

Under water management system of the city it is planned to use supervisory control and data acquisition system. Under this project approximately 3 lakh edge devices would be connected through data acquisitions system in whole city.

Advantages of SCADA System:

The entire water supply and distribution system shall be upgraded to control from the remote station. SCADA system will enable the authority to monitor the system on real time basis and will also help the authority to see the functioning of individual plant as well as to change / correct the working set points at the plant locations.

The SCADA shall transfer the water distribution network data in real time to the Water Supply Information Management System (WIMS) to enable real time analysis of the distribution system.

Following are the features of WIMS

a. Installation of measuring devices spread over the city for automatic data transfer, at a central location having network facility with main server of the administrative system of the utility.
b. The main role of WIMS will be to gather, analyze and present data from various software packages and will provide a data connectivity link that will enable the operations engineers to make informed decisions on

improving the operating efficiently of the network.

c. Use of the software will enable authorities to make informed decisions on operating strategies, to improve the level of service and equability of supplies in all the areas.

d. A tool to compare billing information with actual flow in each zone.

e. Reliable information to improve the capacity and operating strategy of the network to distribute the available supplies. The basis or planning future capacity strengthening and modeling towards 24-hour continuity of supplies.

DIAL 100

DIAL 100 is an emergency response system of police department. Madhya Pradesh police has set up a state level centralized dial 100 control room cum command center in Bhopal for police related emergencies and other services to help people in distress. The proposed center is be equipped with latest technological tools like GIS MAP for whole state, CAD (Computer aided dispatch) and GPS enabled 1000 first response vehicles to attend to handle public distress calls for services. At present approximately 100 vehicles are deployed in Bhopal City. Police personnel are equipped with wireless Radios, CUG GSM connectivity and other model gadgets. As soon as a person makes a call on "100" number, it is received at the center by well trained staff who will take necessary person details, incident details, and location details. Besides computer systems will also validate at the same on the basis of CLI database, GIS MAP, Vehicle database, and other information available in public domain. The trained dispatcher immediately dispatches nearest available one or more well equipped first response vehicle. Each vehicle is monitored and tracked through the GPS based AVLS equipment fitted in the vehicle.

DIAL 108

It is and emergency medical services where citizens can call the ambulance during emergency. This medical ambulances are running across the State of M.P. and is also popularly known as "108 Ambulance Service". This Emergency Medical Ambulance Services, with a fleet of 554 Basic Life Support (BLS) Ambulances and 50 Advance Life Support (ALS) Ambulances deployed strategically across the State of Madhya Pradesh supported with a fully functional centralized call center situated near TB Hospital, Idgah Hills, Bhopal which is receiving more than 25000 calls per day and handling approx. 2500 emergencies on daily basis. GPS with Biometric System has been installed in ambulances. There are around 200 ambulances are operational in Bhopal city.

Objectives:

To provide round the clock pre-hospital emergency transportation care (ambulance) services across the state. Improve the access to Medical & Health care, police and fire

service, particularly attending emergency situations relating to pregnant women, neonates, parents of neonates, infant and children in situations of serious ill health and all other emergencies in the general population: and thereby assist the state to achieve the critical Millennium Development goals in the health sector, i.e. reduction of infant mortality rate, and maternal mortality rate, and in general reduce the vulnerability of the people by providing access to Emergency Response Services.

Traffic Management System

Traffic police of MP at present issues spot challans and court challans manually in the form of hand written hard copy format for violations of various traffic rules in force in Bhopal. The data of prosecution for traffic violations with various combinations for report generation and monitoring is fed manually and maintained in various formats for the purpose of traffic management.

With Traffic Management System MP Police intends to procure the RLVD and e-Challan system under this Project for management of traffic violations in near real time, data maintenance, generation of prosecution reports and to prosecute repeat violators for appropriate punishment as provided in Motor Vehicle Act. The purpose of this project is to ensure that all traffic violations are recorded in real time and stolen vehicles are tracked and legally prosecuted accordingly.

Safe City Cameras Feed

This project has an objective to implement holistic and integrated video surveillance system which includes Command and Control center, Video Management Software and Video Analytics for fifty cities of the state of Madhya Pradesh. Under this city at present 650 CCTV cameras are and 100 ANPR Cameras (Automatic Number Plate Recognition) installed at 135 locations (approximate) In Bhopal city. The key advantages of this project are:

- To provide assistance to citizen at the time of emergency
- To effectively manage Road Traffic
- To make use of technology for traffic challan
- Support police to maintain Law and Order
- To help in investigation of crime
- Help in preventing, detecting and dealing with criminal activities with minimum turnaround time
- Provide alerts and video analytics for counter terrorism
- Monitoring of suspicious people, vehicles, objects etc. with respect to protecting life and property and maintaining law and order in the city
- Continuous monitoring of some important locations/ public places in city area like area near to railway station, airport and other public places for keeping eye on regular activities & for emergency support

Dynamic Market Place (Mayor Express)

Dynamic Market Place is e-Market place providing various kinds of services to citizens. The services includes: Electrician, Plumber, Carpenter, Mason, Driver, Gardener, Painter, Accountant, Air Conditioner Servicing, Baby Sitter, Beautician, Car Cleaner, Cook, Dish Washer, Domestic Maid, House Cleaning, Pest Control, Photographer, etc. The objective of this project is to provide an operational platform for the dynamic market place which will be integrated with Municipal Corporations Call Center and Bhopal+ Application at the front end.

Crowdsourcing of Data

It is planned to collect data as part of future IT initiative under which citizen of Bhopal would be sharing data. Received data would be part of existing data repository where data is received from various type of sensors owned by Bhopal smart City. All the operations like data analytics will be performed on the received data through crowdsourcing too. Connectivity between end devices and ICCC will be provided by MPUADD. For example, in near future if any resident welfare society intends to share data with MPUADD (ICCC) for surveillance purpose, this video feed would be received at ICCC and become part of other feeds coming from various CCTV camera installed in the city by MPUADD.

Fire Brigade Control System

Fire brigade section is the part of Bhopal Municipal Corporation. There are 18 fire brigade vehicles and 15 motor bikes are available to cater to whole city. Municipal Corporations has plans to strengthen and upgrade the fire brigade control system of the city. MSI has to integrate the city fire brigade control system with ICCC. This will help Municipal Corporations in efficient usage of its resources and to achieve minimum response time in case of rescue operations.
For example: If the ICCC receives information about fire in the city, the ICCC should able to trigger a command to appropriate fire station and its vehicle which can reach within minimum time with guidance about traffic conditions and shortest route.

Solar Roof Top

India is endowed with vast solar energy potential. From an energy security perspective, solar is the most secure of all sources, since it is abundantly available. Theoretically, a small fraction of the total incident solar energy (if captured effectively) can meet the entire country's power requirements. It is also clear that given the large proportion of poor and energy un-served population in the country, every effort needs to be made to exploit the relatively abundant sources of energy available to the country. While, today, domestic coal based power generation is the cheapest electricity source, future scenarios suggest that this could well change.
The broad aim of this project is to develop and deploy new and renewable energy for supplementing the energy requirements of the city. Remote monitoring systems of all the solar roof top installed on Govt. of Private buildings will be monitored through ICCC. This will] result in better planning and running the operations from energy management perspective.

Current ICT based systems of Indore City and integration scope

Indore Smart City Development Limited (ISCDL) intends to develop a State-of-the-Art Command Control and Communication Center of the Indore City, which will help to deliver, inter alia, the below services but not limited to these;

Video Surveillance for Citizen Safety and Security

The Video Surveillance Project is managed by Indore Police Department. The objective of this project is Citizen Safety and Security solution that will enable city to plan events, effective monitoring of infrastructure, track incidents enabling quicker response etc. It will help in enforcement of law, monitoring of public areas, analyze patterns and other following aspects:

- Quicker response to incidents;
- Assistance for more effective operations;
- Improved situational awareness;
- Better attractiveness to businesses and workers;
- Improved planning and resource allocation;

This project has implemented about 350 CCTV Camera which are controlled and monitored by Indore Police Department and it has been planned to view event based CCTV Camera video feeds at the Command Control and Communication Center. The number of videos feeds based on the events shall be finalized during the requirement gathering phase. In addition to the 350 CCTV Cameras, the proposed Smart Pole project shall install 1600 CCTV cameras under the Indore Smart City project. The Smart Pole shall be connected through a network of Optic Fiber cable and the video feeds of the 1600 CCTV Cameras shall be linked seamlessly with the Command Control and Communication Center through Optic Fiber Cable (OFC). Additionally, ISCDL Citizens Mobile application shall provide Crowd Sourced Real Time data, Geo Tagged, CCTV Broadcast streams over available Public Wi-Fi/3G/4G to the Command Control and Communication Center. These requirements are mentioned in the Indore Smart City “RFP for Selection of Concessionaire for Implementation of Intelligent Street pole at Indore under PPP”, where the concessionaire shall suffice the requirements of erecting the CCTV cameras, transmitting the live videos feeds from the 1600 CCTV Cameras to the Command Control and Communication Center through OFC.

Integrated 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. IMC owns licenses of Desktop GIS software and had built data layers which consist of administrative boundary, planning and landuse. However, most of the GIS based activities of IMC has been limited to few departments predominantly to support the planning activities. ISCDL is in the phase of upgrading the existing licenses of Desktop GIS licenses and procurement of additional licenses under the DGS&D and NICSI rate contract. Apart from the Desktop GIS licenses the Web GIS software shall be hosted on the cloud environment along with the spatial and attribute data bases. The Enterprise GIS software shall integrate with different

Smart City Applications that are to be hosted on Cloud and visible in the Command Control and Communication Center.
Apart from this, following services shall be configured through Web GIS software
• Location Based Services
• Vehicle Tracking and Management System (VTMS)
• Mobile GIS Services
• 3D GIS with "What if" analysis
• Mapping Gallery for Inter-Dept use of Maps/ data Integration of Applications and disparate databases

Smart Parking Management and Guidance

The Smart Parking initiative in Indore is aimed at providing parking management and guidance system. This shall be achieved via a sensor based smart parking solution to identify each parking bay and enable availability of accurate parking information. Parking Lots for Smart parking Solution can be categorized into three types:

a) **Indoor (Covered) Parking Lots:** This type of parking consists of all covered parking areas considered under this project. The parking lot usually has an enclosed or sheltered area segregated for parking generally inside a building or commercial complex. The Parking Solutions shall cover but not limited to entry and exit barriers, single space recognition, motorized bay locks controlled by Mobile App, bay availability information, advanced bay booking facility and map based guidance system up to individual bay.

b) **Open (Outdoor) Parking Lots:** This type of parking consists of demarcated open parking lots a fenced area or zone demarcated for parking near a street or road. It shall include but not limited to entry and exit barriers, single space recognition, motorized bay locks controlled by Mobile App, bay availability information, advanced bay booking facility and map based guidance system up to individual bay.

c) **Street Parking:** This include street parking which are individual marked parking bay on street. It should include but not limited to single space recognition logic using motorized bay locks controlled by Mobile App, bay availability information and map based guidance system up to individual.

The key objectives from the smart parking initiative;
• To uniquely identify all parking bay through motorized parking bay lock logic

• To enable accurate information on availability of parking bays in real time through monitoring entry and exit of each vehicle in each parking bay

• To enable parking guidance system to direct drivers to available parking bay through dynamic signages and a map interface in the citizens mobile smart parking application

• To enable users to pay on the bays or reserve parking bays via citizen mobile app or Indore Smart City online portal

• To generate revenues from mCoupon's during the process of finding, reserving or parking a vehicle.

• To ensure that revenue leakages from parking contracts are completely eradicated.

Intelligent Street Pole

The Smart Streetlight Monitoring Initiative will monitor the multi Utility Smart Poles, CCTV Camera, Wi-Fi service with dedicated OFC Network, Smart LED Lights, and Sensors (motion, light, environmental, etc.) to help in energy optimization and ensure that there are no dark spots on the streets. Streetlights are essential elements of a municipal services. It affects residents' sense of safety while influencing a city's ability to create an inviting environment for business and tourism. The existing outdoor light consumes very high amount of electricity. Therefore, ISCDL intends to implementation Smart and integrated lighting system considering following aspects of it;
• Reducing energy consumption, cost, and its maintenance;
• Enhancing situational awareness, real-time collaboration, and decision making across city;
• Adding intelligent IT innovations to transportation, civic utilities, public safety without adding significantly more physical infrastructure;
• Improving Real-time data communications with low latency to improve safety and security.

It will have following components;
• Wi-Fi Hotspots
• LED Lights
• CCTV Surveillance
• Environmental Sensors
• Active Geo Transponders: for third party Location Based Services
• EV Charging Points
• Smart Bill Board
• Smart 3/4 G or Wi-Fi button for SOS Application – Linkage with the concern departments for addressing the alert
• Mobile Application – for monitoring and evaluation, controlling the infrastructure.
• Smart Citizen Mobile Application – for citizen centric applications: eGOV services, Smart parking, Crowd Sourced CCTV.
• Telecom Network Management – OFC Connectivity, Application Software, Integration with all sub-modules

The RFP of this project has been released by ISCDL. The primary function of the smart poles will be to provide street lighting, mobile broadband infrastructure, Wi-Fi hotspot services, Active Geo location transponder for location based services and surveillance camera. These facilities will be connected to the Command Control and Communication Center, where it will be constantly monitored and managed. The concessionaire may also use the smart pole for other commercial purposes, namely, smart
bill board, electronic vehicle charging, environmental sensor etc. It should however be ensured that the primary functions are not hampered in any way while using the same for other commercial purposes.

Citizen Web Portal, Mobile & Kiosks Services

Web Portal, Mobile Application & Kiosk Services will be interface for all citizens' services with the city administration. It will serve as window of information about Indore Smart City and as a platform to deliver services online while providing an avenue to disseminate information to citizens. Online systems in compliance with various standard operating procedures will bring transparency in city administration. It shall allow ISCDL to engage with citizens through the use of social media, online communities elsewhere on the Web.

Integrated Solid Waste Management

Indore Smart City Development Limited (ISCDL) had floated a RFP for a GPS based Vehicle Tracking Solution (VTS) for monitoring, route tracking for Municipal Solid Waste (MSW), IP based CCTV Cameras to monitor the number of headcounts at Public & Community Toilets and Integrated Weighbridge Vehicle Monitoring System at the landfill site. The scope also includes supply, Implementation and maintenance of web based and mobile based software system to capture and store data from GPS devices, CCTV cameras, integrated weighbridge and finally generation of necessary MIS reports (Tabular, Map based). The project was awarded and the vendor has deployed the solution to ISCDL.
The overall scope consists of 3 sections – (1) GPS based VTS, (2) CCTV solution and (3) Integrated Weighbridge system. The vendor shall Supply, Install and commission GPS based Vehicle Tracking System, Tracking Solution with IP cameras for Community and Public Toilets and Integrated Weighbridges Monitoring System.
The MSI shall provide support to integrate the system with the Command Control and Communication Center and provide manpower to operate and maintain the system for 3 years.
The scope of the project covers the following components:
• Vehicle Tracking
• Weighbridge Automation
• CCTV Cameras in Public Toilets
• Automation of Waste to Energy Plant
• CCTV Cameras, RFID based garbage disposal sites
• Automation of Solid Waste Plant through distributed control systems, etc.
• Intelligent Waste Bins, Dynamic Routing of Garbage vehicles

Intelligent Transport Management System

Public transport should always be the trademark of a better transportation system for a city or a state. The role of public transport is vital, particularly to reduce the use of personalized transport. This system should be such that it can work in co-ordination with the existing transportation systems. An efficient mass transportation system is very much needed for sustainability of not only the economy but also for reducing stress due to pollution on the environment.
To achieve above objective, City of Indore has established a Special Purpose Vehicle (SPV) in the form of public limited company Atal Indore City Transport Services Ltd (AICTSL) to implement, operate & manage reliable and efficient public transport services within and around Indore city. AICTSL runs city buses through a PPP model with several bus operators. The various stakeholders of AICTSL are IMC, Indore Development ISCDL (IDA), Madhya Pradesh State Government and Private Bus Operators.

To address the growing demand, congestion, reliability and to provide a better public transportation system to the people of Indore, AICTSL has implemented a Bus Rapid Transit (BRT) System on one of the prime corridors in Indore. Indore BRT Phase I project comprised of the AB Road corridor that extended from Niranjanpur Chouraha (Circle) to Rajiv Gandhi Chouraha (Circle) with a length of 11.4 Km. There are 21 closed median bus-stations and 15 signalised intersections on the corridors.
The AB Road pilot corridor was the first corridor that was implemented on a pilot basis with state-of-the-art Intelligent Transportation Management Systems (ITMS) which includes the following sub-systems;
• Automatic Fare Collection Systems (AFCS)

• Automatic Vehicle Location System

• Passenger Information System at BRT Stations

• Traffic Management Centre Systems

• Communications network for the deployed systems

AICTL also operate city buses on more than 16 routes with more than 110 buses. It covers 120 bus stops.
Now, under smart city initiatives, ISCDL has envisaged to further strengthen the existing services with achieving following objectives;
• Enhance Situational Awareness of existing traffic conditions on real time basis
• Develop ability to Assimilate and Analyze and real time transport information and historic trends to enable automated transport control and support decision making on transport management strategies
• Create linkages to support Information Dissemination of traffic management strategies and user information through traffic controllers, Information Portal, Variable Message Signs, Web Services and APIs
• Implement Intelligent Bus-Q Shelters
• Ensure long term Capacity Building through training and support for city administrators

Intelligent Water Supply Management System

IMC manages its own water supply and distribution system, O&M and also the billing system. Indore City Water demand is divided into Consumer, Industrial and floating population. An integrated approach shall sustain water supply services, improvement in operation and mitigation of other issues related to water quality and sanitation. The project aims to conduct consumer survey to analyze the water demand from the nodes and understand the existing flow in the distribution network. This will help to analyze the existing demand and project the demand in the immediate future.
There is an urgent need to convert the present intermittent water supply systems to 24x7 continuous water supply systems. The Intelligent Water Supply Management System shall include consumer survey, GIS mapping, computerized billing, hydraulic modeling, water audit and energy audit.
1 Consumer survey and GIS mapping will help in identifying all the legal and illegal connections. The up to date consumer billing data can be fed to computer software specifically developed for billing and collection which will result in increase in revenue generation.

2 Hydraulic modeling is essential for checking adequacy of service reservoirs and pipes for delivering 24x7 water supplies. New operating zones will be formulated to deliver water at equitable pressure. Such kind of engineered approach will help in designing a robust system for water supply with optimum investment.
3 Water audit identifies zone wise NRW in the system which enables development of priority wise action plan.
4 Energy audit helps identifying optimum investment in electrical equipment such that efficiency can be improved which will directly reduce the bill for the electricity.
5 Installation of IoT based Bulk Meters at ESR/GSRs at the inlet and outlet of the tank
6 Centralized SCADA for Water Network Monitoring.

ISCDL has appointed an Engineering Consultant for the ABD area for procurement & deployment of SCADA system. MSI shall integrate SCADA with different Smart City Applications that are hosted and visible in Command Control and Communication Center.

Smart Education

Education services in Indore shall have an improved infrastructure and service delivery mechanism through ICT intervention. This will enable city to create safer and modern facilities for students and teachers. Global experts and teachers will be able connect with students using internet interventions for sharing their knowledge and experience. This system of education will also be used to provide education to remote places where teachers cannot be recruited. This will play a vital role in improving the overall literacy rate of the society and will allow education to reach to all section of society curtailing the obstacles that our society faces today.
The following ICT initiatives have been envisaged to make education interactive and effective;

a) Smart Interactive Education

Smart classroom with Wi-Fi based internet connectivity will help to conduct collaborative learning programs using video conferencing, which will allow students from different schools to have an access to the teachings of different schools/teachers who are awarded with better performance assessment. Also similar collaboration with national and international level good schools will also be conducted, to provide students with an exposure to world class education. This will also allow students to interact with students from various schools across the globe, to share knowledge among them and take career oriented counselling from various professionals and seniors. Such schools will be able to arrange online trainings for students on subjects wherein they themselves don't have a permanent faculty for the said subjects/topic. Also the online library shall be provided to students with facilities of e-books and online notes sharing which will make the teaching experience more interactive and fun for all.

b) Smart School Management System

This will include the online recruitment of teachers, online centralized admission system, attendance of teachers and students using biometric system and student & teacher performance review system. This system will help to make a robust the review system which bring transparency and efficiency in school procedures. The school data will be monitored online by administration, teachers and parents and thus will have a positive impact on the result and performance of students. Better results will be

directly linked to the performance assessment and such schools and teachers will be given recognition at district and state level in form of prize/awards.

c) E-Monitoring System

Schools will be provided with CCTV surveillance for monitoring the activities at school which will not only allow school and district administration to monitor activities of school but will also provide safer avenues for students and teachers. Also the GPS tracking and CCTV surveillance for school buses will also provide the safe and efficient system for students travel. Smart 3/4G or Wi-Fi connected buttons shall be installed to raise one press alerts identifying location as well as type of incidents, these buttons shall provide a proactive security approach for students, teachers and school administrators in distress.

Smart Health

In India Only 31% of the population uses Government medical facilities. Even the lowest socio-economic strata are forced to use private & charitable facilities with inadequate Govt. health Infrastructure for proactive disease mitigation. It is utmost important to revive and plan measures to upgrade existing health infrastructure by integrating dispensaries and health posts for preventive and curative care.
The Purpose of Smart Health are as follows:
1. Delivery of quality health services
2. Ensure availability, accessibility and affordability of services to all categories of people
3. Fulfill demands of the patients to their satisfaction
4. Improve health indicators by setting targets and fixing time limit for the same.

The following ICT initiatives are envisaged to initiate a Smart Health component
1. Reforms in medical record keeping in line with ICD guidelines. Computerization of hospital records.
2. CCTV at important patient care area
3. Health card linked to Aadhar Cards
4. Health Applications for follow up reminder, medicine reminder, location of nearest ASHA/ANM/ PHC/ CHC, etc.
5. Call Centre at City level to track and monitoring patient health post visit to health center to ensure continuum of care
6. Hospital Information Management System with medical, administrative, ERP, EMR and integrated with PACS, Lab equipment at DH/ CHC/ PHC
7. MIS/ KPI monitoring system to provide visibility of performance of resources and effectiveness of the programs
8. Trend analysis and future disease analysis. Implementing Planning measures to cater to future healthcare needs of the city

Smart 3/4G or Wi-Fi connected buttons shall be installed to raise one press alerts identifying location as well as type of incidents such as: Code Blue, Code Red: Distress, these buttons shall provide a proactive security approach for Hospital Staff and Patient in distress.

Wastewater Management System

The project shall include management of the entire water cycle from production, treatment, transport, storage and delivery to the customer's tap. It shall involve replacement of house service connections, rehabilitation of treatment facilities, service reservoirs and pipelines.
Currently, the industrial sector in Indore, which is one of the biggest consumers of water, is supplied fresh treated potable water. They would easily use wastewater treated up to the secondary level. As much as ~60 to 70% of the water being supplied to cities is right there. It only needs to be treated and supplied to industries. Good potable water that industries get shall be swapped for residential and drinking purposes.
A secure internet-based smart system shall be used for monitoring and managing pump installations in commercial buildings, water supply networks, wastewater plants, etc.

Smart Grid

Smart Grid shall facilitate efficient and reliable end-to-end intelligent two-way delivery system from source to sink through integration of renewable energy sources, smart transmission and distribution. In this way Smart Grid technology shall bring efficiency and sustainability in meeting the growing electricity demand with reliability and best of the quality.
Smart Grid shall also enable real time monitoring and control of power system as well as help in reduction of AT&C losses, demand response and demand side management, power quality management, outage management, smart home energy system etc.
Smart Grid shall act as a backbone infrastructure to enable new business models like electric vehicles, smart communities apart from more resilient and efficient energy system and tariff structures etc.

Current ICT based systems of Jabalpur City and integration scope

There are various state of the art IT systems/initiatives already deployed in the city or being deployed. Following are the few important IT systems of the city and their features which JSCL envisages to integrate these IT systems with command and control centre of smart city Jabalpur:

Smart Parking
Smart Parking is a pan city initiative for all the parking area which is managed by JMC.
Public Bike Sharing

f. Stations, Bicycles with onboard computer and GPS
g. Fare Collection device on each smart bicycle – using NFC, Smart Card and Pin Code
h. The central control system collects data from each station for efficient planning and operation of the system.
i. This data will be used to make decisions on redistribution of cycles around stations during the hours of operations.

Solar Roof Top

Jabalpur Smart City proposal envisages 10% of its energy requirement to be fulfilled with Solar Energy.
3.1 MW solar roof top energy project is envisaged under this project.

Smart Pole
Converting traditional street lights to LED based intelligent lights
Smart poles with capability to accommodate multi operator telecom Base Stations for 2G/3G/LTE to reduce mobile call drops
Surveillance cameras inbuilt into smart poles
Wi-Fi hotspots
Interactive Digital Signage for traffic & business
Environment sensors
Optical Fiber Cable network to enable connected communities
Network/cloud controlled EV Charging at 100 poles
State of the art control and command centre (for smart poles) for the O&M of services for 15 years

Solid Waste Management Services
Installation of GPS devices on all the vehicles, RFID Tags, RFID Readers.
GPS Based Application software (Vehicle Tracking System) integrated with GPS, RFID devices
GPS/GPRS System, RFID, fuel sensors for all vehicles.
Cloud based data centre
Infrastructure including Server and Control centre (with video wall). Software with MIS reports.
Provision for alerts to the Central Command centre on Scheduled Missed Trips, over speeding vehicles, unauthorized stoppage and /or non-stoppage of the vehicles at designated bins & route deviation by vehicles etc.

Intelligent Transport Management System
"Intelligent Traffic Management System (ITMS) includes setting up Automatic Number Plate Recognition (ANPR) system, Red Light Violation Detection (RLVD) Cameras with E-Challan System at specified locations of Jabalpur City. Following are the key features of ITMS system.

All buses equipped with GPS based Automatic Vehicle Location System (AVLS) connected with Central Control and Command Centre (of ITMS).

Real time tracking and monitoring of Bus Operations.
16 Ft X 6 Ft Video Wall comprising of 08 Nos. of High Resolution LED Panels at Control room.
Bus Stops are connected with Command Centre reflecting Expected Time of Arrival (ETA) on Passenger Information System (PIS)
All the buses are equipped with 04 Nos. of PIS in buses and PAS in buses. .
Signal Priority for BRTS buses
Automatic Fare Collection
Number of Bus Stops – 100
Number of Buses – 225 (in future 300)
Real time tracking and monitoring of bus operations
Bus stops are connected with command centre

JMC Call Centre

JMC call centre is a public grievances redressal system related to municipal services. All the issues /complains related to municipal services are addressed by JMC call centre. In future JMC call centre will also be used as one of the channels for taking request for dynamic market place.

Jabalpur Smart Map (GIS)
GIS cutting across departments.
Citizen portal - Map visualization module, Query module, and location based information module, education, health services, public feedback, transport, cultural and community events.
Property and other taxes.
Heritage

JMC Municipal Services
These are pan city citizen services, which are hosted using SAP based web application and they are also hosted on Jabalpur plus mobile application, these services include:

Water Tax
Property Tax
Birth Registration
Death Registration
Marriage Registration

Water Management System (SCADA)
Approx. 3 lakh edge devices would be connected through data acquisitions system in whole city.

DIAL 100
It is an emergency response system of police department
Approx. 70 vehicles are operation in city providing services to citizen.

DIAL 108
It is and emergency medical services where citizens can call the ambulance during emergency

Traffic Management System
Traffic police of MP at present issues spot challans and court challans manually in the form of hand written hard copy format for violations of various traffic rules in force in Jabalpur. The data of prosecution for traffic violations with various combinations for report generation and monitoring is fed manually and maintained in various formats for the purpose of traffic management.

With Traffic Management System MP Police intends to procure the RLVD and e-Challan system under this Project for management of traffic violations in near real time, data maintenance, generation of prosecution reports and to prosecute repeat violators for appropriate punishment as provided in Motor Vehicle Act. The purpose of this project is to ensure that all traffic violations are recorded in real time and stolen vehicles are tracked and legally prosecuted accordingly.

Safe City Cameras Feed
It is basically CCTV surveillance system of Jabalpur city

Traffic management – city signals (100 signals minimum with ANPR cameras), E-Challan system

Jabalpur 311 Application:
Jabalpur 311 has been developed to help citizens in availing municipal services. Through this app citizens can address these issues directly to city authorities. Execution of payments of municipal taxes will also be easy through this app. Following facilities are available to citizens through this app:
Registering for Death and Birth Certificates
Lease Renewal
Food & Drug License Renewal
Connecting emergency helpline
Payment of Taxes (Water, Property etc)
Availing new water connection
Online Building Plan Approval and Application Tracking
Tracking of Ration Card Information
Redressal of Grievances
Booking of Water Tankers and Public Community Halls
Other Municipal related Services

JCTSL RT:
This application is for booking of shuttle services from Jabalpur Airport to Jabalpur Smart City

JCTSL Cab booking service:
Jabalpur City Transport Services Limited has launched cab services for citizens. Currently cab booking through this service is based on SMS, Missed Call, Call and web based. Soon this service will be hosted on application and will have to be integrated with ICCC.

J-CARD

Automatic Building Permission Approval System (ABPAS-DCR Cell)

S.No	List of Services	Brief of Scope for Integration
1	Integration of Smart Parking	ICCC will be required to integrate with the command centre of the Smart Parking solution, which is a PAN City initiative. ICCC will be required to receive feeds on the status of parking across the city which are managed by the Smart Parking command centre (feeds received from all the edge devices of the Parking Solution). These feeds will provide information of available, non-available parking slots, functional and non - functional parking slots. ICCC will also be required get video feeds from the parking areas on real-time basis. Such video feeds will only be saved for 7 days. These video feeds will also help monitor assets of JMC, JSCL and JCTSL All the information received will also be required to be mapped on the GIS map. All the information received from the smart parking command centre will also go into the Analytical layer which will help city in better planning and running of operations. ICCC should also be able to trigger the commands / alerts (if required) to the respective

		command centre. This initiative is under JMC.
2	Integration of Public Bike Sharing	ICCC will be required to integrate with the command centre of the Public Bike Sharing solution, which is a PAN City initiative. ICCC will be required to receive feeds on the status of utilization of public bike sharing docks across the city. These feeds will provide information of available, non-available cycles in slots, functional and non - functional PBS stations. ICCC will also be required get video feeds from the PBS stations on real-time basis. Such video feeds will only be saved for 7 days. These video feeds will also help monitor assets of JMC, JSCL and JCTSL. ICCC will also be required to get information regarding the position of the cycles deployed under the PBS project. All the information received will also be required to be mapped on the GIS map. All the information received from the PBS command centre will also go into the Analytical layer which will help city in better planning and running of operations. ICCC should also be able to trigger the commands / alerts (if required) to the respective command centre. This imitative is managed by JSCL.
3	Integration of Smart Pole & Smart Lighting	ICCC will be required to integrate with command centre of Smart Poles (Pan City Initiative) to receive all kinds of feeds such as environment sensor, lighting sensors. Video, etc. ICCC will be required to get information on the status of working of the installed LED lights, as well as other sensors and other cameras. ICCC will also get real-time video feed from the installed Smart Poles. Such video feeds will only be saved for 7 days. These video feeds will also help monitor assets of JMC, JSCL and JCTSL. All the information received will also be required to be mapped on the GIS map. All the information received from the Smart Pole command centre will also go into the Analytical layer which will help city in better planning and running of operations. ICCC should also be able to trigger the commands / alerts (if required) to the respective command centre. This imitative is managed by JSCL.

4	Integration of Solid Waste Management Services (ICT based monitoring of Waste Management System)	ICCC will be required to integrate with the control room of Solid Waste Vehicle tracking project (Pan City Initiative) to receive feeds on the location of the solid waste vehicles. ICCC will also get other information which is received in the control room 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. ICCC should also be able to trigger the commands / alerts (if required) to the respective command centre. This imitative is managed by JMC.
5	Integration of Intelligent Traffic Management System	ICCC will be required to integrate with Command Centre of Traffic Management System, to receive real-time feeds of the camera installed by them. These video feeds will not be saved, but will be utilized in Analytical layer to help administration monitor its assets and do a better urban planning. ICCC will also be required to send video feeds received from Smart Parking, Smart Pole, PBS in real-time basis to the command centre of Traffic (if required). ICCC should also be able to trigger the commands / alerts (if required) to the respective command centre.
6	Integration of JMC Call Centre &JMC Services	ICCC will be required to integrate its helpdesk and system with JMC call centre, in case if there is some information or notification is to be sent to JMC call centre for doing some action in the field regarding Municipal Corporation work. 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. ICCC will be required to integrate with the backend system of Jabalpur Municipal Corporation services which is SAP based system to monitor the performance of the application. Along with this ICCC should be able to show the utilization by citizens of various sections of Jabalpur Plus application in the form of a Dashboard. ICCC will be required to send JMC field agents alerts and notifications for any emergency / incidents / disaster in the city for doing required action. ICCC system should also be able to get acknowledgement from the receivers.
7	Integration with Jabalpur Smart MAP (GIS)	ICCC will be required to use the GIS platform developed by JSCL for the city. There will be a requirement for enhancing the existing platform and using it in the ICCC for doing all the necessary actions. This is an ESCRI based platform with almost 96 layers. Along with this ICCC should be able to show the utilization by citizens of various sections of Jabalpur Plus application in the form of a Dashboard. All the information received from the application will also go into the Analytical layer which will help city in better planning and running of operations.

8	Integration with Apna Nigam	ICCC will be required to integrate with the backend system of Jabalpur Plus to monitor the performance of the application. Along with this ICCC should be able to show the utilization by citizens of various sections of Jabalpur Plus application in the form of a Dashboard. All the information received from the application will also go into the Analytical layer which will help city in better planning and running of operations.
11	Integration with Transport Management System (BTMS of JCTSL)	ICCC will be required to integrate with command centre of JCTSL to get all kinds of feeds from Transport Management 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. ICCC should also be able to trigger the commands / alerts (if required) to the respective command centre.
12	Integration with CCTV Surveillance (Police Dep't.)	ICCC will be required to integrate with Command Centre of CCTV System, to receive real-time feeds of the camera installed by them. These video feeds will not be saved, but will be utilized in Analytical layer to help administration monitor its assets and do a better urban planning. ICCC will also be required to send video feeds received from Smart Parking, Smart Pole, PBS in real-time basis to the command centre of Police (if required). ICCC should also be able to trigger the commands / alerts (if required) to the respective command centre.
13	Integration with Emergency Response and Disaster Mgmt.	ICCC will be required to integrate with existing ICT system of the Emergency Response and Disaster Management to send them alerts and notifications for any emergency / incidents / disaster in the city for doing required action. ICCC system should also be able to get acknowledgement from the receivers. All the information received from the application will also go into the Analytical layer which will help city in better planning and running of operations.
14	Integration with Water Management System (SCADA)	ICCC will be required to integrate Water Management System (SCADA) control room to get all kinds of sensor and edge devices feeds. ICCC should be able to map this information on the GIS layer and help authority monitor the water management of the city. ICCC should also be able to trigger the commands / alerts (if required) to the respective command centre. All the information received from the application will also go into the Analytical layer which will help city in better planning and running of operations.
15	Integration with Met Department (Local Weather Forecast)	ICCC should be able to receive real-time data on the weather forecast from Met Department and map the same on its platform as well as GIS layer. All the information received from the application will also go into the Analytical layer which will help city in better planning and running of operations. This information will also help in predictive analysis.

16	Integration with Area Based Development (ABD) Services: i. Utilities ii. Lighting iii. Metering iv. Surveillance	ICCC will be required to integrate with control rooms / systems all the listed services of the Area Based development (ABD). These services are planned for the near future. ICCC will be required to get all kinds of feeds from all the sensors / edge devices installed for these services in the field. In case of video feeds, feeds will only be saved for only 7 days. ICCC will be required to monitor these services in real-time and manage the operations of these services. All the information received from the application will also go into the Analytical layer which will help city in better planning and running of operations. This information will also help in predictive analysis.

Current ICT based systems of Ujjain City and integration scope

There are various state of the art IT systems/initiatives already deployed in the city or being deployed. Following are the few important IT systems of the city and their features which USCL envisages to integrate these IT systems with command and control centre.

Smart Parking
Smart Parking is a pan city initiative for all the parking area which is managed by Ujjain Municipal Corporation.

Solar Roof Top
Ujjain Smart City proposal envisages some percentage of its energy requirement to be fulfilled with Solar Energy.
solar roof top energy project is envisaged under this project.

Smart Pole
Converting traditional street lights to LED based intelligent lights
Smart poles with capability to accommodate multi operator telecom Base Stations for 2G/3G/LTE to reduce mobile call drops
Surveillance cameras inbuilt into smart poles
Wi-Fi hotspots
Interactive Digital Signage for traffic & business
Environment sensors
Optical Fiber Cable network to enable connected communities
Network/cloud controlled EV Charging at 100 poles
State of the art control and command centre (for smart poles) for the O&M of services for 15 years

Solid Waste Management Services
Installation of GPS devices on all the vehicles, RFID Tags, RFID Readers.
GPS Based Application software (Vehicle Tracking System) integrated with GPS, RFID devices
GPS/GPRS System, RFID, fuel sensors for all vehicles.
Cloud based data centre
Infrastructure including Server and Control centre (with video wall). Software with MIS reports.

Provision for alerts to the Central Command centre on Scheduled Missed Trips, over speeding vehicles, unauthorized stoppage and /or non-stoppage of the vehicles at designated bins & route deviation by vehicles etc.

Intelligent Transport Management System

"Intelligent Traffic Management System (ITMS) includes setting up Automatic Number Plate Recognition (ANPR) system, Red Light Violation Detection (RLVD) Cameras with E-Challan System at specified locations of Jabalpur City. Following are the key features of ITMS system.

All buses equipped with GPS based Automatic Vehicle Location System (AVLS) connected with Central Control and Command Centre (of ITMS).

Real time tracking and monitoring of Bus Operations.

16 Ft X 6 Ft Video Wall comprising of 08 Nos. of High Resolution LED Panels at Control room.
Bus Stops are connected with Command Centre reflecting Expected Time of Arrival (ETA) on Passenger Information System (PIS)
All the buses are equipped with 04 Nos. of PIS in buses and PAS in buses. .
Signal Priority for BRTS buses
Automatic Fare Collection
Number of Bus Stops ~100
Number of Buses – 200
Real time tracking and monitoring of bus operations
Bus stops are connected with command centre

Municipal Corporation Call Centre

Call centre is a public grievances redressal system related to municipal services. All the issues /complains related to municipal services are addressed by call centre. In future UMC call centre will also be used as one of the channels for taking request for dynamic market place.

Smart Map (GIS)

GIS cutting across departments.
Citizen portal - Map visualization module, Query module, and location based information module, education, health services, public feedback, transport, cultural and community events.
Property and other taxes.
Heritage

Municipal Services

These are pan city citizen services, which are hosted using SAP based web application and they are also hosted on Jabalpur plus mobile application, these services include:

Water Tax
Property Tax
Birth Registration
Death Registration
Marriage Registration

Water Management System (SCADA)

Approx. 2 lakh edge devices would be connected through data acquisitions system in whole city.

DIAL 100
It is an emergency response system of police department
Approx. 50 vehicles are operation in city providing services to citizen.

DIAL 108
It is and emergency medical services where citizens can call the ambulance during emergency

Traffic Management System
Traffic police of MP at present issues spot challans and court challans manually in the form of hand written hard copy format for violations of various traffic rules in force in ujjain. The data of prosecution for traffic violations with various combinations for report generation and monitoring is fed manually and maintained in various formats for the purpose of traffic management.

With Traffic Management System MP Police intends to procure the RLVD and e-Challan system under this Project for management of traffic violations in near real time, data maintenance, generation of prosecution reports and to prosecute repeat violators for appropriate punishment as provided in Motor Vehicle Act. The purpose of this project is to ensure that all traffic violations are recorded in real time and stolen vehicles are tracked and legally prosecuted accordingly.

Safe City Cameras Feed
It is basically CCTV surveillance system of Ujjain city
Traffic management – USCL envisaged city signals to be equipped with (135 CCTV cameras), E-Challan system

S.No	List of Services	Brief of Scope for Integration
1	Integration of Smart Parking	ICCC will be required to integrate with the command centre of the Smart Parking solution, which is a PAN City initiative. ICCC will be required to receive feeds on the status of parking across the city which are managed by the Smart Parking command centre (feeds received from all the edge devices of the Parking Solution). These feeds will provide information of available, non-available parking slots, functional and non - functional parking slots. ICCC will also be required get video feeds from the parking areas on real-time basis. Such video feeds will only be saved for 7 days. These video feeds will also help monitor assets of USCL and municipal corporation All the information received will also be required to be mapped on the GIS map. All the information received from the smart parking command centre will also go into the Analytical layer which will help city in better planning and running of operations. ICCC should also be able to trigger the commands / alerts (if required) to the respective command centre.

3	Integration of Smart Pole & Smart Lighting	ICCC will be required to integrate with command centre of Smart Poles (Pan City Initiative) to receive all kinds of feeds such as environment sensor, lighting sensors. Video, etc. ICCC will be required to get information on the status of working of the installed LED lights, as well as other sensors and other cameras. ICCC will also get real-time video feed from the installed Smart Poles. Such video feeds will only be saved for 7 days. These video feeds will also help monitor assets of USCL. All the information received will also be required to be mapped on the GIS map. All the information received from the Smart Pole command centre will also go into the Analytical layer which will help city in better planning and running of operations. ICCC should also be able to trigger the commands / alerts (if required) to the respective command centre.
4	Integration of Solid Waste Management Services (ICT based monitoring of Waste Management System)	ICCC will be required to integrate with the control room of Solid Waste Vehicle tracking project (Pan City Initiative) to receive feeds on the location of the solid waste vehicles. ICCC will also get other information which is received in the control room 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. ICCC should also be able to trigger the commands / alerts (if required) to the respective command centre.
5	Integration of Intelligent Traffic Management System	ICCC will be required to integrate with Command Centre of Traffic Management System, to receive real-time feeds of the camera installed by them. These video feeds will not be saved, but will be utilized in Analytical layer to help administration monitor its assets and do a better urban planning. ICCC will also be required to send video feeds received from Smart Parking, Smart Pole in real-time basis to the command centre of Traffic (if required). ICCC should also be able to trigger the commands / alerts (if required) to the respective command centre.
6	Integration of Call Centre & municipal Services	ICCC will be required to integrate its helpdesk and system with USCL call centre, in case if there is some information or notification is to be sent to USCL call centre for doing some action in the field regarding Municipal Corporation work. 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. ICCC will be required to send USCL field agents alerts and notifications for any emergency / incidents / disaster in the city for doing required action. ICCC system should also be able to get acknowledgement from the receivers.

7	Integration with GIS MAP	ICCC will be required to use the GIS platform developed by JSCL for the city. There will be a requirement for enhancing the existing platform and using it in the ICCC for doing all the necessary actions. This is an ESCRI based platform with almost 96 layers. Along with this ICCC should be able to show the utilization by citizens of various sections of Jabalpur Plus application in the form of a Dashboard. All the information received from the application will also go into the Analytical layer which will help city in better planning and running of operations.
11	Integration with Transport Management System	ICCC will be required to integrate with command centre of Transport department to get all kinds of feeds from Transport Management 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. ICCC should also be able to trigger the commands / alerts (if required) to the respective command centre.
12	Integration with CCTV Surveillance (Police Dep't.)	ICCC will be required to integrate with Command Centre of CCTV System, to receive real-time feeds of the camera installed by them. These video feeds will not be saved, but will be utilized in Analytical layer to help administration monitor its assets and do a better urban planning. ICCC will also be required to send video feeds received from Smart Parking, Smart Pole etc in real-time basis to the command centre of Police (if required). ICCC should also be able to trigger the commands / alerts (if required) to the respective command centre.
13	Integration with Emergency Response and Disaster Mgmt.	ICCC will be required to integrate with existing ICT system of the Emergency Response and Disaster Management to send them alerts and notifications for any emergency / incidents / disaster in the city for doing required action. ICCC system should also be able to get acknowledgement from the receivers. All the information received from the application will also go into the Analytical layer which will help city in better planning and running of operations.
14	Integration with Water Management System (SCADA)	ICCC will be required to integrate Water Management System (SCADA) control room to get all kinds of sensor and edge devices feeds. ICCC should be able to map this information on the GIS layer and help authority monitor the water management of the city. ICCC should also be able to trigger the commands / alerts (if required) to the respective command centre. All the information received from the application will also go into the Analytical layer which will help city in better planning and running of operations.
15	Integration with Met Department (Local Weather Forecast)	ICCC should be able to receive real-time data on the weather forecast from Met Department and map the same on its platform as well as GIS layer. All the information received from the application will also go into the Analytical layer which will help city in better planning and running of operations. This information will also help in predictive analysis.

16	Integration with Area Based Development (ABD) Services: i. Utilities ii. Lighting iii. Metering iv. Surveillance	ICCC will be required to integrate with control rooms / systems all the listed services of the Area Based development (ABD). These services are planned for the near future. ICCC will be required to get all kinds of feeds from all the sensors / edge devices installed for these services in the field. In case of video feeds, feeds will only be saved for only 7 days. ICCC will be required to monitor these services in real-time and manage the operations of these services. All the information received from the application will also go into the Analytical layer which will help city in better planning and running of operations. This information will also help in predictive analysis.

Current ICT based systems of Gwalior City and integration scope

Current ICT based systems of Sagar City and integration scope

Current ICT based systems of Satna City and integration scope