Request for Proposal for Selection of System Integrator (SI) for NDMC Smarty City Project "Design, Development, Built, Implementation, Operation and Maintenance of Command and Control Centre & Data Center, ERP Solution and integration with various Smart City / NDMC Applications".

Volume-I

NEW DELHI MUNICIPAL COUNCIL (NDMC)
PALIKA KENDRA, NEW DELHI

Disclaimer

The information contained in this Request for Proposal document ("**RFP document**") or subsequently provided to Applicant(s), whether verbally or in documentary or in any other form, by or on behalf of New Delhi Municipal Council (hereafter referred to as "NDMC") or any of its employees or advisors, is provided to the Applicant(s) on the terms and conditions set out in this RFP document and all other terms and conditions subject to which such information is provided in writing.

This RFP document is intended to be and is hereby issued only to the prospective Applicants. The purpose of this RFP document is to provide the Applicant(s) with information to assist the formulation of their Proposals. This RFP document does not purport to contain all the information that each Applicant may require. This RFP document may not be appropriate for all persons, and it is not possible for the NDMC, its employees or advisors to consider the investment objectives, financial situation and particular needs of each Applicant who reads or uses this RFP document. The assumptions, assessments, statements and information contained in the RFP document may not be complete, accurate, adequate or correct. Each Applicant should, therefore, conduct its own investigations and analysis and should check the accuracy, adequacy, correctness, reliability and completeness of the assumptions, assessments, statements and information contained in this RFP document and where necessary obtain independent advice from appropriate sources. The NDMC, its employees and advisors make no representation or warranty and shall incur no liability under any law, statute, rules or regulations as to the accuracy, adequacy, correctness, reliability or completeness of the RFP document.

Information provided in this RFP document to the Applicant(s) is on a wide range of matters, some of which may depend upon interpretation of law. The information given is not intended to be an exhaustive account of statutory requirements and should not be regarded as a complete or authoritative statement of law. The NDMC accepts no responsibility for the accuracy or otherwise for any interpretation or opinion on law expressed herein.

The NDMC, its employees and advisors make no representation or warranty and shall have no liability to any person, including any Applicant under any law, statute, rules or regulations or tort, principles of restitution or unjust enrichment or otherwise for any loss, damages, cost or expense which may arise from or be incurred or suffered on account of anything contained in this RFP document or otherwise, including the accuracy, adequacy, correctness, completeness or reliability of the RFP document and any assessment, assumption, statement or information contained therein or deemed to form part of this RFP document or arising in any way for participation.

The NDMC also accepts no liability of any nature whether resulting from negligence or otherwise howsoever caused arising from reliance of any Applicant upon the statements contained in this RFP document.

The NDMC may in its absolute discretion, but without being under any obligation to do so, update, amend or supplement the information, assessment or assumptions contained in this RFP document before the last date of bid submission.

The issue of this RFP document does not imply that the NDMC is bound to select an Applicant or to appoint the selected Applicant or SI, as the case may be, for the Project and the NDMC reserves the right to reject all or any of the Applicants or Bids without assigning any reason whatsoever.

The Applicant shall bear all its costs associated with or relating to the preparation and submission of its Bid including but not limited to preparation, copying, postage, delivery fees, expenses associated with any demonstrations or presentations which may be required by the NDMC or any other costs incurred in connection with or relating to its Bid. All such costs and expenses will remain with the Applicant and the NDMC shall not be liable in any manner whatsoever for the same or for any other costs or other expenses incurred by an Applicant in preparation or submission of the Bid, regardless of the conduct or outcome of the Bidding Process.

Table of Contents

Abbreviations & Definitions

Procuring Entity	New Delhi Municipal Council (NDMC)
Act	The New Delhi Municipal Council Act, 1994 (44 of 1994)
Applicant/Supplier/Seller	A company registered under the Companies Act, 1956/2013.
Bidding Document	Documents issued by the procuring entity, including any amendments thereto, that set out the terms and conditions of the given procurement and includes the invitation to bid
Authorized Signatory	The Applicant's representative/ officer vested (explicitly, implicitly, or Signatory through conduct) with the powers to commit the authorizing Organization to a binding agreement. Also called signing officer/authority having the Power of Attorney (PoA) from the competent authority of the respective Bidding firm.
Bid	A formal offer made in pursuance of an invitation by a procuring entity and includes any tender, proposal or quotation in electronic format
Security Deposit	A security provided to the procuring entity by a Applicant for securing the fulfillment of any obligation in terms of the provisions of the bidding documents
BOQ	Bill of Quantity
SI	System Integrator
ICCC	Integrated Command and Control Centre
DC`	Data Centre
BG	Bank Guarantee
PAN	Permanent Account Number
PBG	Performance Bank Guarantee
SLA	Service Level Agreement is a negotiated agreement between two parties wherein one is the procuring entity and the other is the service provider. It is a service contract where the level of service is formally defined. In practice, the term SLA is sometimes used to refer to the contracted delivery time (of

	the service) or performance.
GO-LIVE	GO-LIVE means 100% supply, installation and commissioning of IT hardware and software, development of ERP solution, implementation of RFID based Solid Waste Management System, and integration with ICCC of all the services defined in this RFP.
VAT	Value Added Tax / Central VAT / GST
EMD	Earnest Money Deposit
LOA	Letter of Acceptance
O&M	Operation & Maintenance
FMS	Facility Management Service
ICT	Information and Communication Technologies
QCBS	Quality & Cost based Selection
SLA	Service Level Agreement

1. Invitation for Proposal

1.1 **Name of the Work**: Request for Proposal for Selection of System Integrator for NDMC Smarty City Project “Design, Development, Implementation, Operation and Maintenance of Command and Control Centre & Data Center, Collaboration solution for meetings and integration with various ERP & smart city & NDMC Applications”.

NDMC hereby invites online bids for Selection of a System Integrator (SI) for the following works:

(i) Design, built, supply and Installation, operation & maintenance of Central Command & Control Centre (ICCC) and Data Centre with appropriate hardware and software, networking for viewing, analyzing, storing and retrieval of the data for various Application and services defined in this RFP. Integration of ICCC software with various ERP & Smart City &NDMC Applications, sensor data and GIS platform;

(ii) For design, supply and Installation, operation & maintenance of civil, interior decoration, furniture, electrical, air-conditioning works for setting up of Command & Control Centre and Data Center;

(iii) Collaboration Solution for meetings

(iv) Development of ERP applications as explained in the RFP;

(v) Providing and installation of 500 surveillance cameras at outdoor locations in NDMC area.

(vi) Helpdesk service and call centre for public complaint redressal throughout contract period on 24X7X365.

(vii) RFID based Solid waste management system for 75000 households.

The detailed scope of work is set out in the RFP document Volume-II.

1.2 Applicants are advised to study this RFP document carefully before submitting their bid/proposals in response to the RFP document. Submission of bid in response to this notice shall be deemed to have been done after careful study and examination of this document with full understanding of its terms, conditions, implications and after assessment of the project viability.

1.3 Evaluation of the Bids will be done on the Quality cum Cost based (QCBS) in proportion of 70: 30 (70% technical and 30% Financial weightage).

1.4 The RFP document can be downloaded from NDMC's website (www.ndmc.gov.in) and Delhi Government's website (https://govtprocurement.delhi.gov.in) and the Applicant is required to deposit a Demand Draft of Rs. 25,000 (Rupees Twenty five Thousand only) drawn in favour of "Secretary NDMC" payable at Delhi/New Delhi with submission of bid.

Office of the Executive Engineer,
Room No.1503, 15th Floor,
New Delhi Municipal Council
Palika Kendra, Sansad Marg,
New Delhi – 110001
Tel No:- 011-23348418

All subsequent notifications, changes and amendments will be uploaded on the NDMC's website www.ndmc.gov.in and Delhi Government's website https://govtprocurement.delhi.gov.in.

1.5 Applicant (authorized signatory) shall submit its offer for preliminary qualification, technical and financial proposal through e-procurement system. However, Tender Document Fees, and Earnest Money Deposit (EMD) should be deposited as per details provided in the bid document. The bid document complete in all respect is to be submitted on or before the time of last date of submission of bid through e-procurement system. NDMC will not be responsible for delay in submission due to any reason.

1.6 Key Events and Dates

S. No.	Information	Details
1.	Advertising Date	27.04.2017
2.	Last date to send in requests for clarifications	Till 04:00pm on 04.05.2017
3.	Date, Time and Place of Pre-Bid conference	05.05.2017 at 03:00pm in NDMC Conference Hall, 3rd Floor, Palika Kendra, Sansad Marg, New Delhi-110001
4.	Release of response to clarifications would be available at	www.ndmc.gov.in and https://govtprocurement.delhi.gov.in
5.	Last date and time for submission of	03:00pm on 19.05.2017

	bids (Bid Due Date)	
6.	Technical Bid Opening Date & Time	03:30pm on 19.05.2017
7.	Date for Presentation	To be informed
8.	Financial Bid Opening Date &Time	To be informed
9.	Address for communication and hard copy submission of documents / correspondence	Executive Engineer (S/P) Civil Engineering Department, 15th floor, Room No. 1503, Palika Kendra, New Delhi-110001 Phone:- 011-23348418

1.7 Other Important Information Related to Bid

S. No.	Item	Description
1.	Earnest Money Deposit (EMD) – Online	Rs. 1.00 Cr. (Rupees One Crore Only)
2	RFP document fee	Rs. 25,000 (Rupees Twenty five Thousand Only)
3.	Bid Validity Period	(180) One-hundred-and eighty days from the date of opening of Bids.
4.	Last date for furnishing Performance Bank Guarantee to NDMC (By preferred Applicant)	Within Fifteen (15) days of the date of issue of Letter of Acceptance (LOA).
5.	Performance Bank Guarantee value (Performance Bank Guarantee)	10% of the tender value.
6.	Performance Bank Guarantee (PBG) validity period	PBG shall be valid till for 180 days beyond the term of the contract period of five years from the date of GO-LIVE.
7.	Last date for signing the Contract Agreement	15 days from the date of issue of Letter of Acceptance.

2. NDMC'S OVERVIEW

2.1 About New Delhi Municipal Council (NDMC)

NDMC is one of the five urban local body in National Capital Territory of Delhi. It has its origins in the Imperial Delhi Committee, which was constituted on 25 March 1913 to overlook the construction of the new capital of India. The administrative area under the New Delhi Municipal Council comprises of 42.7 sq. km. The NDMC is governed by a 13 member Council. The Council Members includes the Member of Parliament of New Delhi Parliamentary Constituency, the Member of Legislative Assembly of New Delhi and Delhi Cantonment Assembly Constituency.

NDMC consists of nearly 3% of the area and 2.5 lakh of the resident population of National Capital Territory of Delhi. However, there is about 16-20 lakhs floating population in daytime which possess challenges for managing the civil services in NDMC area.

NDMC is a seat of the head of the Federal Legislature, Executive and the Judiciary. NDMC region comprises of Lutyen's Delhi, the area which was historically come was regarded as the centre of Central in Union of India. It also consists of important buildings such as Rashtrapati Bhawan, Parliament House, Supreme Court, North and South Blocks and others. In addition to this, NDMC area also comprises of the embassy area. The strategic geo-political location of the NDMC area and its history makes the area extremely important for the country. Efficient functioning of the municipal body is, thus, extremely important for the country.

2.2 NDMC's main responsibilities are –

- Providing basic civic amenities
- To manage its own assets and collection of Property Tax
- Building Regulation
- Registration of Birth and Death
- Construction, and maintenance of municipal markets and regulation of trades
- Sanitation & Public Health
- Maintenance of public parks, gardens or recreational centres

NDMC is one of the few local bodies in the country who is financial self-reliant. It is also a distribution company for water and electricity and its municipal solid waste is 100% scientifically disposed of.

2.3 NDMC's TRANSFORMING INTO A SMART CITY

NDMC has been one of the first city to initiate Smart City projects which inter-alia include city-wide Wi-Fi services in the Connaught Place and Khan Market area, Multi-tier automatic parking system at Sarojini Nagar and Baba Kharak Singh Marg, a multi utility (Service corridor) duct of about 1.2 km in the Connaught Place area and e-governance initiatives such as on-line payments for electricity-water bills, property taxes and other online services such as citizen complaint centers, online data of birth and death, electricity water connections. NDMC is also taking big strides in moving to mobile platform for rendering citizen services.

NDMC has been selected by the Ministry of Urban Development, Government of India as one of the 20 Smart Cities under the Smart City Mission.

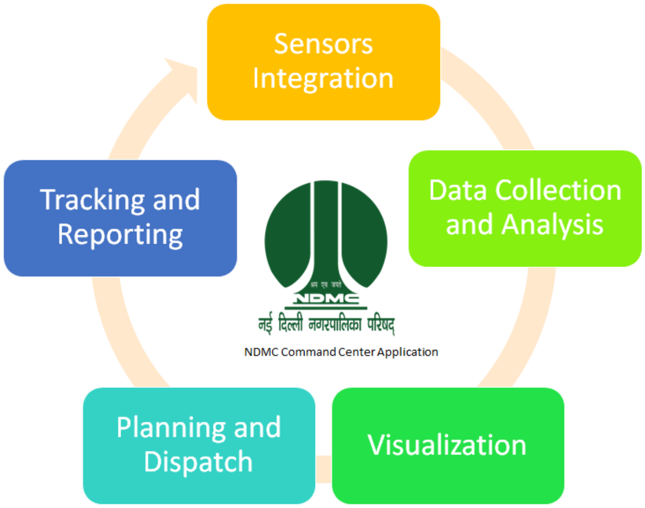
The vision for NDMC Smart City has been formulated based on the strategic blueprint and the needs and aspirations articulated through the stakeholder consultations. NDMC Vision for Smart City is thus:

"To be the Global Benchmark for a Capital City"

3. PROJECT OBJECTIVE & SCOPE

3.1 Project Objective

The vision of the NDMC is to provide Integrated City Operations Platform (ICOP) with combination of Command and Control, Data Visualization and Sensor Integration technologies into a Common Operating Picture that improves whole communities' response to and management of planned and unplanned events, and builds the capability and resiliency of agencies charged with citizen services, safety, infrastructure protection, and relief activities.


Sensors Integration
Data Collection and Analysis
Visualization
Planning and Dispatch
Tracking and Reporting
NDMC
नई दिल्ली नगरपालिका परिषद्
NDMC Command Center Application

The ICOP technology platform and capability enables diverse information sources to be shared and used for accurate and timely decision-making. GIS capability of the integrated command and control center will leveraged the NDMC with Incident Management, Correlation, Alarm Management, Dispatch Capability and tracking of Incidents and level of services. It allows responding agencies to take advantage of detection and prediction technologies that can use all available and relevant data, and support decision-making in the wider context of the situation as it is now and as it might unfold.

The ICOP may be staffed continuously and opened only when required by operational procedures. The latter situation means that the centre and the personnel that will be running it need to be ready at short notice. This in turn implies that the ICOP technology platform will be cost-effective to maintain and the need for complex staff training and retraining kept to a minimum.

The integrated operations centre allows responding agencies to:

- See and make sense of what's happening.
- Utilize a shared platform for collaborative decision-making.
- Cooperatively manage tools and resources, allocate tasks, and issue notifications.

- Performance parameters

The success of an integrated operations centre will be measured by the ability of decision-makers to have access to the information they need to, which will allow them to make decisions in collaboration with other decision-makers and stakeholders. They will be presented with their own tailored views or slices of the common operating picture, updated and refreshed together with the views of other operators throughout the solution. Access to sensitive information will be managed through robust identity management and formal trust relationships that are aligned with legislated powers.

The ICOP shall be working in a fully automated environment for optimized monitoring, regulation and enforcement of traffic with various law enforcement services. Integration with other business systems applications/ modules that provide the transformation capabilities to do whatever is needed. The inherent capability of the same ICOP will provide the middleware to integrate sub system defined, but not limited to, in RFP.

The application specified in this RFP shall be integrated into one functional system and shall be accessible by the operators and concerned agencies with necessary login credentials. The necessary civil, electrical, furniture, IT work including integration with such systems will be in the scope of the SI.

3.2 Project Scope

3.2.1 Centralized Command and Control Center

For centralized monitoring and decision making as per the scope defined below:

3.2.1.1 Components:

i. Network and Security Management Solution

ii. Centralized System for Security Solution

iii. Core Computing and Data Processing infrastructure

iv. Integration with Third Party Shared Services

v. Data Center (DC)

vi. Necessary Civil, Electrical work including furniture, including Air-conditioning for Data Centre, and Command & Control Centre.

vii. ERP Solutions.

viii. Centralised Command and Control System

ix. Help desk service and Call centre for public grievance redressal system on 24X7 basis.

3.2.1.2. In brief the Central command control will be the nodal point of availability of all online data and information related to smart services like LED Street lighting, CCTV surveillance cameras, air quality sensors, Smart Parking system, Wi-Fi, electricity and water SCADA and billing, GIS, Electric and water meters, e-hospitals, property tax management, estate management, engineering system, asset management system, other services defined at 3.2.2. below etc.

3.2.1.3. Command Control Centre will be established with all hardware, software and network infrastructure including switches and routers, Networking racks ,videowall, setting up of workstation consoles, and will be operated and maintained by the system integrator throughout the operation and maintenance period.

3.2.1.4. Necessary Civil, Electrical work including furniture, electrical cabling and network data cabling including Air-conditioning, shall be the responsibility of SI for Data Centre, and Command & Control Centre. DC and ICCC can be in same premises or at different locations.

The system integrator will give the space requirement within fifteen days from the date of signing of the agreement. Accordingly, NDMC will provide the space in Palika Kendra or at any other location, subject to the availability.

The system integrator will give the Architectural Design showing Civil, Electrical, furniture, Air-conditioning and all other work for Data Centre and ICCC within one month from the date of signing of the agreement. Accordingly, NDMC will approve the same or suggest some modifications, if any, and there-after the SI will execute the Civil, Electrical works and provide furniture, including the Air-Conditioning works within prescribed time-limits given in this RFP document.

Detailed functional and technical requirement is mentioned in volume-II of this RFP.

3.2.2 Seamless integration of Command and Control Centre software.

Seamless integration of following smart services and solution is to be done

The Command & Control software offered by SI shall be "commercial off-the-self software" (COST Software) and should provide APIs for the following services for this project. SI will integrate all these modules as per detailed scope given in volume-II of RFP. Integration of following Services and ERP modules should be considered as part of this RFP:

1) Smart LED Street Lights (for 21000 LEDs)
2) Sensor Based & Camera Based Smart Parking for 15000 ECS whole of the NDMC area.
3) Water-SCADA & Smart Water Metering
4) Electricity-SCADA & Smart Electric Metering
5) Property Tax
6) Smart Classroom
7) Surveillance using CCTV (for approximately 2000 camera)
8) NDMC App 311
9) Variable Messaging Sign (VMS)
10) Building Plan Approval
11) Accounts Module (e-fin module)
12) Legal Module
13) e-hospital
14) GPS (Garbage vehicle, C&D waste, municipal vehicles, mechanical sweepers, water tankers etc.)
15) e-office (including e-dak)
16) Public Wi-Fi
17) Estate License/ License fee module
18) Citizen Interactive Kiosks for Urban Service Delivery
19) Environmental Monitoring (sensor based)
20) Smart Waste Management (sensor and GPS based)
21) Billing of Electricity & Water (Commercial Department)
22) Event Management- (Venue Booking, Bharat Ghar Booking and other events)
23) Birth & Death Module
24) Health License
25) Asset Management
26) Material Management and Procurement Management
27) Central Workshop Management
28) HRMS including pay roll and pension, Biometric Attendance
29) Sewage Treatment Plants (STP)

30) Public Bike Sharing
31) ERP modules as given in clause 2.4.13 of volume-II of this RFP.

APIs requirement for initiatives/services proposed in future by the NDMC, which are not mentioned above will be dealt as per Clause 3.5.6, if required by the NDMC.

3.2.3. Collaboration solution for Administrative Meeting

3.2.3.1 NDMC requires IP based full high definition 1080 pixel video conferencing solution to be implemented in NDMC conference rooms, meeting rooms and executive desktop solutions. The solution shall be used for administrative meetings by NDMC at many instances, which will help NDMC reduce travel, faster decision making, save time.

Detailed scope of work, including functional requirements and technical specifications, has been provided in the volume-II of this RFP document**.**

3.2.4 Helpdesk service and call centre for public complaint redressal throughout contract period. The SI will have to provide the hardware & software for Helpdesk service for public complaint redressal and to depute the required manpower 24 X 7 X 365 to receive the calls, distribute to respective persons, updating the status etc. on Existing Communication channels of NDMC such as 311 App, dedicated toll free numbers, facebook, twitter, Whatsapp etc.

3.2.5 Providing and installation of 500 CCTV surveillance cameras with network switches and other infrastructure like poles, fibre cabling electric cabling at outdoor locations in NDMC area complete in all respect except bandwidth cost..

3.2.6 SI will assess the bandwidth (internet & P2P) requirement at all the proposed locations / cameras for bringing in data to the ICCC.

3.2.7 Development of ERP applications as defined in volume II of RFP

The SI will study the work flow requirements of these modules to be developed as per the P2P Bandwidth existing working in NDMC. SI after studying it may proposes modifications in the processes to bring the efficiency of these works. NDMC will approve the SI's suggestions and SI will develop these finally approved modules under scope of works of this RFP document.

3.2.8 RFID based Solid Waste Management System for 75000 households.

3.3 The Engagement Model is bifurcated into following two stages- (i) Implementation Stage; and (ii) Operation and Maintenance Stage:

S. No.	Stage Name	Description	Period
(I)	Implementation Stage	(a) The system integrator will give the space requirement for ICCC & DC to NDMC .	Up to 15 days from the date of signing of contract agreement.
		(b) The system integrator will give the Architectural Design showing Civil, Electrical, furniture, Air-conditioning and all other work for Data Centre and ICCC	Up to one month from the date of signing of contract agreement.
		(c) Complete System Design and submission of Design Report along with engineering drawings including ICCC building design (using 3D Simulation alongwith physical report). Study of integration requirement of services to be implemented for phase-I and to submit report to NDMC.	Up to 3 months from the date of signing of contract agreement.
		Setting up of Command and Control Centre and Data Centre (All civil, electrical, interior works, air-conditioning works, IT hardware & software, furniture, Video wall etc)	Up to 6 months from the date of signing of contract agreement.
		Design, supply, instillation and commissioning of RFID based Solid	Up to 6 months from the date of signing

		waste management system for 75000 household.	of contract agreement
		Integration and commissioning of Twelve services out of fourteen services to be integrated in phase-I as defined in table-1 below.	Up to 6 months from the date of signing of contract agreement.
		Providing and installation of all 500 Surveillance cameras and integration at ICCC.	Up to 6 months from the date of signing of contract agreement.
		(a) Integration and commissioning of balance services of phase-1 and eight services of phase-II as defined in Table-2 below.	Up to 9 months from the date of signing of contract agreement.
		Study, Design, Development, Deployment Of ERP solution and integration with ICCC.	Up to 9 months from the date of signing of contract agreement.
		integration and commissioning of balance services of phase-I and II, and all services defined in Phase III and completion of all the scope of work defined in RFP, (except O&M) i.e. GO-LIVE of the project.	Up to 12 months from the date of signing of contract agreement.
(II)	Operation and Maintenance Stage (Post Implementation Stage)	Running of Call Centre, ERP solution, RFID based solid waste management system & Comprehensive O&M of all equipments, software and services installed and implemented under this RFP and to meet the desired SLAs.	Period of five (5) years from the date of GO-LIVE. In any case of delay in GO-LIVE, the period of five (5) years of O&M will be counted from the date of actual Go-LIVE date.

Table 1: Services for integration in phase-I (as per scope define in volume II of RFP):

S. No.	List of Services
1.	e-office, including e-dak and Human Resource Management System (HRMS)
2.	Sensor Based & Camera Based Smart Parking (Complete NDMC)
3.	Event Management - (Venue Booking, Bharat Ghar Booking and other events)
4.	Smart Classroom, including MIS and CCTVs
5.	CCTVs
6.	NDMC Mobile App (For Public as well as NDMC internal)
7.	Online Building Plans Approval
8.	Accounts Module (e-fin module)
9.	e-Hospital
10.	Pay roll and Pension and Biometric Attendance
11.	Billing of Electricity & Water (Commercial Department)
12.	Birth & Death Module
13	Smart Solid Waste Management
14	Sewage Treatment Plant (STP)

Table 2: Services for integration in phase-II (as per scope define in volume II of RFP):

S. No.	List of Services
1.	Smart LED Street Lights/Smart Poles
2.	Property Tax Management System [Proposed as part of ERP Solution]
3.	Estate Management System, including license fee module [Proposed as part of ERP Solution]
4.	Variable Messaging Signs (VMS)
5.	Legal Module
6.	GPS based vehicle tracking
7.	Public Bike Sharing
8.	Citizen Interactive Kiosks for Urban Service Delivery

9.	Environmental Monitoring (sensor based)
10.	Health License, Electricity Connection Module, Water Connection Module.
11	Public Wi-Fi Citywide

Table 3: Services for integration in phase-III (as per scope define in volume II of RFP):

S. No.	**List of Services**
1.	Electricity – SCADA & Electricity Meter [Proposed to be procured separately by NDMC]
2	Water- SCADA & Water Meter [Proposed to be procured separately by NDMC]
3.	Asset Management System [Proposed as part of ERP]
4	Material Management& Procurement Management System
5	Central Workshop Management [Proposed as part of ERP]

Note: In case any service for integration is not ready with NDMC, the Concessionaire will integrate the same within two months from the date from which the same will be made available. The detailed phase-wise scope is described in Volume II of the RFP.

3.4 NDMC responsibilities (No charges from system Integrator)

3.4.1 NDMC will bear the cost of consumables like papers, toners etc. at DC and ICCC after GO-LIVE.

3.4.2 NDMC will provide built-up space, and free electricity for setting up of Command and Control Centre and Data Centre Subject to availability of space. Built-up space solely for the purpose of storage of spares will be provided by NDMC Subject to availability of space. All the electricity, water consumed for providing service to NDMC, will be free of cost.

3.4.3 NDMC shall provide single window clearance in area where NDMC has full control to the System Integrator for the purpose of this RFP document.

3.4.4 NDMC will provide the GIS map (Software). It will be responsibility of the System Integrator to integrate various services defined in this RFP on GIS map for proper functioning of all the services in integrated command and control centre.

3.4.5 NDMC will provide necessary bandwidth (internet or P2P) as per the desired requirements between ICCC and other systems for integration

3.4.6 Facilitate interactions with NDMC Departments for getting the required information by S.I.

3.4.7 Review the documents submitted by SI and provide feedback.

3.4.8 Help SI to get necessary feeds for ICCC.

3.4.9 In case of any disaster, facilitate communication from ICCC to field agents (in case of absence of ICT setup with field agents)

3.4.10 NDMC reserves the right to interview the personnel proposed by the SI that shall be deployed as part of the project team. If found unsuitable, the NDMC may reject the deployment of the personnel. But ultimate responsibility of the project implementation shall lie with SI.

3.4.11 NDMC reserves the right to require changes in personnel which shall be communicated to SI. SI with the prior approval of the NDMC may make additions to the project team. SI shall provide the NDMC with the resume of Key Personnel and provide such other information as the NDMC may reasonably require. The NDMC 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, SI shall also ensure that the exiting members are replaced with at least equally qualified and professionally competent members.

3.5 System Integrator Responsibilities

The Responsibilities of the System Integrator throughout the operation and maintenance period shall be as indicated under this RFP document, including:

3.5.1 System Integrator (SI) shall perform for the following works

(i) For state of art design, built, supply and Installation, operation & maintenance of civil, interior decoration, furniture, electrical, air-conditioning works for setting up of Command & Control Centre and Data Center;

(ii) Design, supply and Installation, operation & maintenance of Central Command & Control Centre (ICCC) and Data Centre with appropriate hardware and software for viewing, analyzing, storing and retrieval of the data for various Application and services defined in this RFP. Integration of ICCC software with various Smart City/NDMC Applications;

(iii) Collaboration Solution too meetings;

(iv) Development of ERP applications as defined in volume 2 of this RFP;

(v) Providing and installation of 500 surveillance cameras at outdoor locations in NDMC area.

(vi) Helpdesk service and control centre for public complaint redresal throughout contract period.

(vii) RFID Tag based solid waste management system for NDMC area

The detailed scope of work is set out in the RFP document Volume-II.

3.5.2 (i) Conducting site survey, obtaining necessary permissions, developing system requirements, standard operating procedures etc.

(ii) Operation and maintenance of services under this RFP document over the contract period of five years post GO-LIVE.

(iii) Responsibility of all consumables will be of the system integrator, except the consumables at DC and ICCC (like papers, toners etc.) for which NDMC will bear the cost.

(iv) Any Civil/Electrical work required will be the responsibility of the System Integrator. All the equipments required for Command & Control Centre including fibre POP, FMS Rack etc. will be the responsibility of System Integrator.

(v) In addition to the aforementioned, SI shall provide services to manage and maintain the said system and infrastructure as mentioned in the RFP during entire O&M period of five years from GO-LIVE after GO-LIVE.

3.5.3 Providing physical layout of the ICCC & DC (with 3D simulation) & to get it approved from NDMC.

3.5.4 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 of all locations (including buildings).

3.5.5

(i) Formulation of solution architecture, detailed design of smart city solutions, development of test cases (Unit, System Integration and User Acceptance), SOP documentation.

(ii) SI will define the formats for data exchange between various services and systems in agreement with NDMC

(iii) Physical Setup of ICCC as per the layout in consultation with NDMC.

(iv) Helpdesk and control room setup, procurement of equipment, edge devices, commercial -off-the-self. COTS software (if any), licenses, manpower for helpdesk (for five years after GO-LIVE).

(v) IT and Non-IT Infrastructure installation, development, testing and production environment setup.

(vi) Safety and security of IT and Non IT Infrastructure.

(vii) Software Application customization (if any), development of bespoke (individual or custom-mode) solution (if any), data migration, integration with third party services/application (if any)

(viii) Role based training(s) User Manuals, training curriculum and training materials

(ix) SOP implementation, Integration with GIS Platform, Integration of solutions with Command and Control Centre.

(x) Facilitating User Acceptance Testing (UAT) and conducting the pre-launch security audit of applications.

(xi) User training and roll-out of solution.

(xii) Integration of the various services & solution with ICCC platform.

(xiii) Develop provisions for a scalable system

(xiv) Deploying manpower.

(xv) Security of ICCC premises.

(xvi) Annual technical support.

(xvii) Preventive, repair maintenance and replacement of hardware and software components, IT and non-IT and non ICT components.

(xviii) Provide a centralized Helpdesk and Incident Management Support till the end of contractual period.

(xix) Recurring refresher trainings for the users and Change Management activities.

(xx) Conducting disaster recovery site testing through regular mock drills.

(xxi) Provide required access and information for Audits.

(xxii) Overall maintenance of the ICCC facility and continuity of operations as per SLAs.

(xxiii) Submit daily/weekly/fortnight/monthly/quarterly/annual Reports

3.5.6 For initiatives / services proposed in future by the NDMC which are not covered in this RFP document, if there is any requirement of the additional switches / up-gradation of any hardware/ software / other equipments, the same will be arranged, installed and maintained by the SI on payment basis. NDMC will take competitive rates from third party for such equipments, and the payment will be made to the SI for this additional work by the NDMC at such competitive rates. However, all such installed equipments / switches / routers shall be maintained by the SI as per terms & conditions of the RFP document.

SI Responsibility Matrix

Sr. No.	**Description of Item/service**	**Civil, Electrical, Interior, Air-conditioning, Furniture etc.**	**Supply, installation and commissioning of IT Hardware and Software**	**Comprehensive Operation & Maintenance by the system integrator including replacement of defective parts, spare parts to be provided by the system integrator. For a period of five years from the date of Go-Live**	**Licenses cost for Software including updates to be bear by a system integrator. For a period of five years from the date of Go-Live.**	**Handing over of assets to NDMC by the system integrator in proper working condition. At the end of period of five years from the date of Go-Live or termination of agreement, whichever is earlier.**
1	For design, built, supply and Installation, of civil, interior decoration, furniture, electrical, air-conditioning works for setting up of Command & Control Centre and Data Center& its O & M for 5 years from Go-Live	Yes	Yes	Yes	Yes	Yes
2.	Design, built, supply and Installation, of Central Command & Control Centre (ICCC) and Data Centre with appropriate hardware and software for viewing, analyzing, storing and retrieval of the data for various Application and services defined in this RFP. Integration of	Yes	Yes	Yes	Yes	Yes

	ICCC software with various Smart City/NDMC Applications & its O & M for 5 years from Go-Live					
3.	Collaboration Solution for meetings & its O & M for 5 years from Go-Live;	Not applicable	Yes	Yes	Yes	Yes
4.	Development, deployment of ERP applications & its O & M for 5 years from Go-Live	Not applicable	Yes	Yes	Yes	Yes
5.	Providing and installation of 500 surveillance cameras with complete infrastructure at outdoor locations in NDMC area & its O & M for 5 years from Go-Live	Yes	Yes	Yes	Yes	Yes
6.	Helpdesk service and call centre for public complaint redressal throughout contract period.	Yes	Yes	Yes	Yes	Yes
7	RFID based solid waste management for complete NDMC for 75000 household	Not applicable	Yes	Yes	Yes	Yes

3.5.8 The system integrator is required to provide adequate battery bank to ensure uninterrupted power supply to services provided to the NDMC under this project.

3.5.9 At the end of the O&M period of five years from the date of Go-Live, the system integrator has to hand over all the assets and services belonging to the NDMC in proper working condition. In case of any deficiency noticed at the time of such handing over, the system integrator has to get it rectified at his own cost within 30 days of such handing over, otherwise, NDMC will get it rectified at the risk and cost of the system integrator. Performance guarantee of system integrator will be released only after successful handing over of the all hardware, software, network and services in working conditions to NDMC.

3.5.10 At the time of Go-Live (i.e. completion of implementation period), the system integrator shall inform the NDMC in writing for the same along-with a list of all the assets (details of equipments, software, services etc.) created during the implementation period for the NDMC including their costs. The system integrator shall update such assets list on yearly basis throughout the O&M period.

3.5.11 The system integrator has to take all measures for Cyber security, protection of information and communication technology systems of this project from cyber attacks that are purposeful attempts by unauthorized persons to access ICT systems in order to achieve the target of theft, disturbance, damage, or other illegal actions. The system integrator will detect, analysis and do mitigation of vulnerabilities and protect Data centre, and Command & Control Centre from cyber attacks throughout the O&M period.

3.5.12 All the software licenses to be provided by the SI should be enterprise versions or open source based or open standard based, genuine, perpetual, full use and should provide patches, fixes, security patches and updates directly from the OEM, if applicable. All the licenses and support (updates, patches, bug fixes, etc.) shall be in the name of NDMC.

3.5.13 **Supply of Hardware and associated Software:** All the hardware and software items, peripherals and accessories related to ICCC & DC as per the detailed BOQ are to be supplied as per the specifications and requirement. All cables, connectors and other accessories required to complete the system integration, will be supplied by the

Applicant. Any software (system or otherwise) required to make the system functional will also be provided by the SI. All software with necessary licenses supplied for complete integration and commissioning of the project must be provided in the name of NDMC.

3.5.14 Site Survey: Applicant can inspect proposed site for suitability where all hardware/software under the scope of work are to be installed. Applicant shall come out with details like air-conditioning and UPS requirements for ICCC & DC for all the systems to be supplied in the instant case.

The structured network cabling along with necessary accessories will be carried out at space identified for ICCC, DC, video conferencing locations, (NDMC conference room, meeting rooms and executive desktops), camera and other equipment locations for data sourcing and sending by the SI.

3.5.15 Solution Document: The Applicant has to submit detailed solution document for setting up a ICCC & DC with detailed layout diagrams indicating the complete integration of various components in the system. These details are to be submitted for approval of NDMC before commencement of installation and commissioning, however the overall responsibility of commissioning within prescribed time-limits and its satisfactory performance during O&M period will be of the SI.

3.5.16 Technical Specifications: All the equipments quoted should meet the minimum technical specifications as per tender requirement. Technical specifications of any other hardware/ software not mentioned in the RFP document but required to complete the project should also be given.

3.5.17 Cable Laying: All Fiber cables will be laser optimized MMF (LOMMF) OM3 cable. All passive components shall be from one OEM only. No mix and match is allowed.

3.5.18 Installation and Commissioning: The SI shall undertake installation and commissioning of all the items supplied as per the terms and conditions stipulated in the bid document. The Applicant must provide all the accessories and peripherals viz.

cables, cords, connectors, fittings, fixtures etc. required for successful installation and commissioning of the new setup even if the same are not explicitly spelt out in the bid document.

The SI shall supply and install the entire software stack including Operating System, Parallel File System, Back-up & Network Management Software, Libraries, Compilers, Cluster & System monitoring and management tools and any other software tool required to complete the end-to-end solution.

SI shall undertake Installation, Commissioning strictly in accordance with recommendations and best practices of OEM and by OEM / OEM certified engineers. Any suggestion from NDMC in the overall interest of the project shall be incorporated by the SI.

3.5.19 Integration with Redundancy: The entire solution must be integrated for redundancy so that there is no single point of failure.

3.5.20 System Familiarization: SI shall provide onsite system familiarization to 30 NDMC officers for 15 working days by certified trainer(s) before the acceptance of entire system as well as at least 3 days every year. Familiarization should cover technical details of all the systems hardware, system software, system configuration and operation. Familiarization is an integral part of the scope of work. System familiarization should cover the following:

(i) Installation, configuration and administration of ICCC & DC systems hardware/ software

(ii) Performance analysis & tuning of system

(iii) Operation & Management of the System.

(iv) Maintenance of the system.

(v) Testing of the System

Note: Comprehensive hardcopy and Soft copy of system familiarization course will be provided to NDMC and to all above 30 officers.

3.5.21 Documentation: The Applicant has to provide a Solution Document (both in hardcopy and softcopy) with details of technical specifications, interconnectivity diagrams, physical layouts, configurations details along with maintenance procedures and periodicity of maintenance for the equipment supplied under this tender. This document needs to be provided before the acceptance of the system by the NDMC after its commencement.

3.5.22 Acceptance Testing: The system, after the integration is completed, will be put on Acceptance tests. As a part of Acceptance Testing, all the components would be powered on for a period of 72 hours before initiating the acceptance procedure. In the acceptance procedure the Applicant has to demonstrate full and documented functionalities and throughput of the system to NDMC team. The handling of the system and basic troubleshooting must be elaborated to the NDMC systems team for smooth day-to-day operations. NDMC system team and user groups will test the system over a period of 5 days. On successful completion of the acceptance test after successful completion of the entire scope of work as defined in the RFP to that stage, NDMC will issue Acceptance Certificate.

Note: Performance Throughput of all applications must be demonstrated on desktops as well as on video walls.

The job of Installation, Integration, Commissioning, System Familiarization and Acceptance as detailed in the scope of work should be completed within 150 days from the date of letter of Intimation from NDMC. All the jobs are required to be carried out during regular office hours of NDMC except in exceptional circumstances with the prior apparel of NDMC is writing .

3.5.23 Post-Completion Liabilities during warranty:

a) The System Integrator will provide Post-completion onsite comprehensive Warranty for 5 years.
b) The System Integrator will conduct onsite Major Patch upgrade of Software in consultation with NDMC.

c) The System Integrator should provide On-site minimum 3-day Familiarization /Refresher of hardware/software by OEM-certified Personnel once every year.

d) The System Integrator has to maintain minimum spare in working condition, as recommended by OEM in built-up space provided by the NDMC and manage the same as per the Service Level Agreement (SLA) throughout the contract period.

e) The System Integrator has to depute resident Engineers at ICCC & DC as per the manpower schedule, during 5 years of comprehensive O&M period. Engineer has to be physically available onsite and also on call/mail 24x7. Engineer should be Certified from OEM. In case Engineer is on leave/non-available due to any reason, an alternate resource with similar experience has to be stationed during that time. However, backend support should be available 24 x 7 x 365 days. If the services of the deputed person is not satisfactory, he/she has to be replaced with competent person with immediate effect by the System Integrator.

f) O&M of ERP solution

g) O&M of RFID based solid waste management system for complete NDMC of 75000 households approx.

h) Replacement of any defective item during O&M period of five years from the date of GO-LIVE.

3.5.24 SI shall ensure that none of the Key Personnel (refer Section 5.3.6.2 of the RFP Volume I proposed) and manpower exit from the project during first 6 months of the beginning of the project. In such cases of exit, a penalty of INR 2 lakhs per such replacement shall be imposed on SI.

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

3.5.26 In case of change in its team members, SI 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.

3.5.27 SI shall ensure that SI's Team is competent, professional and possesses the requisite qualifications and experience appropriate to the task they are required to perform under this Contract. SI shall ensure that the services are performed through the efforts of SI's Team, in accordance with the terms hereof and to the satisfaction of the NDMC. Nothing in the Contract relieves SI from its liabilities or obligations under the Contract to provide the Services in accordance with the NDMC's directions and requirements and as stated in this Contract and the Bid to the extent accepted by the NDMC and SI 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.

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

3.5.29 SI shall ensure that the OEMs supply equipment/ components including associated accessories and software required and shall support SI in the installation, commissioning, integration and maintenance of these components during the entire period of contract. SI shall ensure that the COTS OEMs supply the software applications and shall support SI in the installation / deployment, integration, roll-out and maintenance of these applications during the entire period of contract. It must clearly be understood by SI 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. SI 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.

3.5.30 All the software licenses that SI proposes should be perpetual software licenses. The software licenses shall not be restricted based on location and the NDMC should have the flexibility to use the software licenses for other requirements if required.

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

3.5.32 The NDMC reserves the right to review the terms of the Warranty and Annual Maintenance agreements entered into between SI and OEMs and no such agreement/contract shall be executed, amended, modified and/or terminated without the prior written consent of the NDMC. An executed copy of each of such agreements/contracts shall, immediately upon execution be submitted by SI to the NDMC.

3.5.33 SI 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 SI shall ensure that the same is supported by the respective OEM for contract period.

3.5.34 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, SI should replace the products/ solutions with an alternate that is acceptable to the NDMC at no additional cost to the NDMC and without causing any performance degradation.

3.5.35 Further, the SI 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 SI under the Contract shall be acquired in the name of the NDMC and SI shall have the non-exclusive, limited right to use such licenses till the Term on behalf of the NDMC 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 NDMC.

3.5.36 That the SI 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 SI has proposed to supply under the Contract free from all claims, titles, interests and liens thereon;

3.5.37 SI shall ensure that the OEMs provide the support and assistance to SI 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, SI shall replace the required component(s) with an equivalent or better substitute that is acceptable to NDMC without any additional cost to the NDMC and without impacting the performance of the solution in any manner whatsoever.

3.5.38 SI 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 NDMC.

3.5.39 SI 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.SI 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 NDMC.

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

3.5.41 SI and their personnel/representative shall not alter / change / replace any hardware component proprietary to the NDMC and/or under warranty or AMC of third party without prior written consent of the NDMC.

3.5.42 SI shall provision the required critical spares/ components at the designated Datacenter Sites / office locations of the NDMC for meeting the uptime commitment of the components supplied by him.

3.5.43 SI's representative(s) shall have all the powers requisite for the execution of Scope of Work and performance of services under the Contract. SI's representative(s) shall liaise with the NDMC's Representative for the proper coordination and timely completion of the works and on any other matters pertaining to the works. SI shall extend full co-operation to NDMC'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 SI'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 NDMC working at the NDMC's office locations & field locations and DC sites. Such Bidder's representative(s) shall be available to the NDMC's Representative at respective Datacenter during the execution of works.

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

3.5.45 SI will replicate all the Data of all the existing IT systems in NDMC and proposed IPDS and SCADA system into the Data storage System of ICCC to be created in this RFP. After successful GO-Live, the Data Centre of ICCC will become the main Data centre for all the Applications of NDMC.

3.6 <u>Warranty</u>

3.6.1 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.

3.6.2 A comprehensive warranty applicable on goods/solutions supplied under the Contract by the respective OEMs and the warranties shall be passed on to the NDMC. The SI shall be responsible for making any and all claims under the warranty on behalf of the NDMC till the expiry of the agreement.

3.6.3 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.

3.6.4 The SI 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 SI and respective OEM along with service and spares support to ensure its efficient and effective operation for the entire duration of the contract.

3.6.5 The SI 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.

3.6.6 The SI 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 NDMC's Specifications) or from any act or omission of the SI, that may develop under normal use of the supplied Goods in the conditions prevailing at the respective Datacenter / Server Room Sites.

3.6.7 Warranty for Services – The SI 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 SI represents that it shall use adequate numbers of qualified individuals with suitable training, education, experience and skill to perform the Services hereunder.

3.6.8 The NDMC shall promptly notify the SI in writing of any claims arising under this warranty.

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

3.6.10 If the SI, having been notified, fails to remedy the defect(s) within a reasonable period, the NDMC may proceed to take such remedial action as may be necessary, at the SI's risk and expense and without prejudice to any other rights which the NDMC may have against the SI under the Contract.

3.6.11 Any OEM specific warranty terms that do not conform to conditions under this Contract shall not be acceptable.

3.6.12 The representations, warranties and covenants provided by the SI under the Contract will not be affected by NDMC's modification of any portion of the software so long as the SI can discharge its obligations despite such modifications, or following their removal by the NDMC.

3.6.13 Notwithstanding anything contained in the Contract, unless the NDMC has otherwise agreed in writing, the NDMC reserves the right to reject Goods which do not conform to the specifications provided in the RFP.

3.7 Term and Extension of the Contract

3.7.1 The Contract period shall come into effect. from the date of signing of agreement (hereinafter the "Effective Date"), and shall remain valid for 60 Months (05 years) from the date of Go Live of the system ("Term").

3.7.2 If the delay occurs due to any Force Majeure event, a reasonable extension of time shall be granted by the NDMC.

3.7.3 SI do not have any right for seeking extension to the term mentioned above.

3.7.4 The NDMC shall reserve the sole right to grant any extension to the Term abovementioned and shall notify in writing to SI, preferably at least 3 (three) months before the expiration of the Term hereof, whether it shall grant SI an extension of the Term. The decision to grant or refuse the extension shall be at the NDMC's discretion and such extension of the contract, if any, shall be as per terms and condition of this agreement and at the rate of 'immediately preceding year rate with 7% enhancement'.

4 INSTRUCTIONS TO THE APPLICANTS

This section includes all the important information related to RFP document required to bid for this project.

A. GENERAL

4.1 General Information and Guidelines

4.1.1 NDMC invites bids to this Request for Proposals ("**RFP document**") from eligible Applicants as per the scope of work defined in this RFP document. RFP document means this RFP document, Contract Agreement, supporting annexure / appendices / formats etc., any addenda to this RFP document and all other such documents.

4.1.2 Any contract that may result from this bidding process will be effective from the date of Signing of the Contract Agreement and shall, unless terminated earlier in accordance with its terms, continue for a period of five years from date of GO-LIVE.

4.1.3 The assumptions, assessments, statements and information provided in this RFP document is for the assistance to the Applicants who are expected to carry out their own surveys, investigations and other detailed examination of the Project before submitting their Bids. The Applicant shall visit the site and examine the project in detail for execution of the work and deployment of equipment. Nothing contained in this RFP document shall be binding on the NDMC nor confer any right on the Applicants, and the NDMC shall have no liability whatsoever in relation to or arising out of any or all contents of the RFP document.

4.1.4 Applicants may carry out Project Site visits/ inspections at their own cost.

4.1.5 The Applicant has to ensure that the general public/ tourist/ visitors are not hindered in any manner while survey, execution, operations and maintenance of the project.

4.1.6 All information supplied by Applicants may be treated as contractually binding on the Applicants on successful award of the assignment by NDMC on the basis of this RFP document.

4.1.7 No commitment of any kind, contractual or otherwise shall exist unless and until a formal written Contract Agreement has been executed by or on behalf of NDMC.

Any notification of Preferred Applicant status (including issue of a Letter of Acceptance) by NDMC shall not give rise to any enforceable rights by the Applicant. NDMC may cancel this public procurement at any time prior to a formal written Contract Agreement being executed by or on behalf of NDMC.

4.1.8 This RFP document supersedes and replaces any previous public documentation and communications, and Applicants should place no reliance on such communications.

4.1.9 The Bid should be furnished clearly indicating the bid amount in both figures and words, in Indian Rupees, and signed by the Applicant's authorized signatory. Bids to be submitted online on Delhi Govt. e-procurement website. In the event of any difference between figures and words, the amount indicated in words shall be taken into account.

4.1.10 The Applicant shall deposit an Earnest Money Deposit (EMD) of Rs.1.00 crore (Rupees One Crore only) in accordance with the provisions of this RFP document. The Applicant has the option to provide the EMD either as a Demand Draft/Pay order/Bankers Cheque/FDR/TDR/BG in favour of "Secretary, NDMC" payable at Delhi/New Delhi. Bank Guarantee shall be, as per format at Annexure–5.

4.1.11 The validity period of the Bank Guarantee for EMD shall not be less than 180 (one hundred and eighty) days from the Bid Due Date, inclusive of a claim period of 60 (sixty) days, and may be extended as may be mutually agreed between the NDMC and the Applicant. Where a demand draft is provided, its validity shall not be less than 120 (one hundred and twenty) days from the Bid Due Date, for the purposes of encashment by the NDMC. The Bid shall be summarily rejected if it is not accompanied by the Earnest Money Deposit (EMD). The EMD shall be refundable no later than 60 (sixty) days from the date of issuance of Letter of Acceptance to the other Applicant(s) except in the case of the Preferred Applicant whose Bid Security shall be retained till it has provided a Performance Security under the Contract Agreement.

4.1.12 No Applicant shall submit more than one Application for the Project. An Applicant applying individually or as a member of Consortium shall not be entitled to submit another Application either individually or as a member of any Consortium, as the case may be.

4.1.13 The Applicant shall acquaint himself with the proposed site of work, its approach roads, working space available before submitting the bid.

4.1.14 The Applicant should submit a Power of Attorney authorizing the signatory of the Application to commit the Applicant.

4.1.15 In the case of a Consortium, the Members should submit a Power of Attorney in favour of the Lead Member.

4.1.16 If for any reason, any area in whole or part is not available for work, the agreed execution schedule shall be suitably modified. However, under no circumstances the system integrator shall be entitled to any relaxation, whatsoever, on this ground and he shall re-organize his resources to suit the modified schedule.

4.1.17 The system integrator shall abide by and comply with all the Applicable Laws and statutory requirements, including New Delhi Municipal Council Act, 1994, Minimum Wages Act 1948, Payment of Wages Act 1936, Contract Labour (Regulation & Abolition) Act 1970, Employees' Provident Funds and Miscellaneous Provisions Act 1952, etc.

4.1.18 The project cost on the part of the Applicant would include the cost of hardware, software, civil, electrical works, manpower and other costs. There will be recurring annual cost associated with operation and maintenance of these facilities as per the scope of the work defined in the RFP document.

4.1.19 Organizational Structure during Implementation and Operation: The Applicant shall submit its proposed organizational structure during implementation, operation and maintenance stages commensurate with targeted Project Completion Schedule, which will form the basis of Employment Schedule. The Applicant shall also enclose CV's of the key persons including tasks assigned to them.

4.1.20 The system integrator shall be responsible for the operations and maintenance as per the terms set out in the RFP document.

4.1.21 An Applicant shall be liable for disqualification and forfeiture of Earnest Money Deposit if any legal, financial or technical adviser of the NDMC in relation to the Project is engaged by the Applicant, its Members or any Associate thereof, as the case may be, in any manner for matters related to or incidental to the Project during the Bidding Process or subsequent to the (i) issue of the Letter of Acceptance or (ii) execution of the Contract Agreement. In the event any such adviser is engaged by the Preferred Applicant or system integrator, as the case may be, after issue of the incidental to Project, then notwithstanding anything to the contrary contained herein or in the Letter of Acceptance or the Contract Agreement and without prejudice to any other right or remedy of the NDMC, including the forfeiture and appropriation of the Earnest Money Deposit or Performance Security, as the case may be, which the NDMC may have there under or otherwise, the Letter of Acceptance or the Contract Agreement, as the case may be, shall be liable to be terminated without the NDMC being liable in any manner whatsoever to the Preferred Applicant or system integrator for the same. For the avoidance of doubt, this disqualification shall not apply where such adviser was engaged by the Applicant, its Member or Associate in the past but its assignment expired or was terminated prior to the Application Due Date. Nor will this disqualification apply where such adviser is engaged after a period of 3 (three) years from the date of commercial operation of the project.

4.2 Change in Ownership

Lead Member will hold more than 50% holding in the consortium throughout the O&M period. The Applicant further acknowledges and agrees that the aforesaid obligation shall be the minimum, and shall be in addition to such other obligations as may be contained in the RFP document / Contract Agreement, and a breach hereof shall, notwithstanding anything to the contrary contained in the RFP document / Contract Agreement, be deemed to be a breach of the RFP document / Contract Agreement and dealt with as such there under. For the avoidance of doubt, the provisions of this Clause shall apply only when the Applicant is a Consortium.

4.3 Cost of Bidding

The Applicants shall be responsible for all of the costs associated with the preparation of their Bids and their participation in the Bidding Process. The NDMC will not be responsible or in any way liable for such costs, regardless of the conduct or outcome of the Bidding Process.

4.4 Site visit and verification of information

4.4.1 Applicants are encouraged to submit their respective Bids after visiting the Project site and ascertaining for themselves the site conditions, traffic, location, surroundings, climate, availability of power, water and other utilities for construction, access to site, handling and storage of materials, weather data, Applicable Laws & regulations, & any other matter considered relevant by them.

4.4.2 It shall be deemed that by submitting a Bid, the Applicant has:

(i) made a complete and careful examination of this RFP Document and unconditionally and irrevocably accepted the terms thereof;

(ii) received all relevant information requested from the NDMC;

(iii) made a complete and careful examination of the various aspects of the Project including but not limited to:

(a) existing facilities and structures;

(b) conditions of the access roads, street light poles and utilities, buildings in the vicinity of the Project Site;

(c) conditions affecting transportation, access, disposal, handling and storage of materials;

(d) all other matters that might affect the Applicant's performance under this RFP document;

(iv) accepted the risk of inadequacy, error or mistake in the information provided in the RFP document furnished by or on behalf of the NDMC relating to any of the matters referred to in this RFP document;

(v) satisfied itself about all matters, things and information, including matters referred to in Clause 4.4.1 hereinabove, necessary and required for submitting an informed Bid, execution of the Project in accordance with this RFP Document and performance of all of its obligations there under;

(vi) acknowledged and agreed that inadequacy, lack of completeness or incorrectness of information provided in this RFP Document or ignorance of any of the matters referred to in Clause 4.4.1 hereinabove shall not be a basis for any claim for compensation, damages, extension of time for performance of its obligations, loss of profits etc. from the NDMC, or a ground for termination of the Contract Agreement by the system integrator;

(vii) acknowledged that it does not have a Conflict of Interest; and

(viii) agreed to be bound by the undertakings provided by it under and in terms hereof.

4.4.3 NDMC shall not be liable for any omission, mistake or error in respect of any of the above or on account of any matter or thing arising out of or concerning or relating to RFP Document or the Bidding Process, including any error or mistake therein or in any information or data given by the NDMC.

4.5 Verification and Disqualification

4.5.1 The NDMC reserves the right to verify all statements, information and documents submitted by the Applicant in response to the RFP document and the Applicant shall, when so required by the NDMC, make available all such information, evidence and documents as may be necessary for such verification. Any such verification, or lack of such verification, by the NDMC shall not relieve the Applicant of its obligations or liabilities hereunder nor will it affect any rights of the NDMC there under.

4.5.2 The NDMC reserves the right to reject any Bid and appropriate the Earnest Money Deposit if:

(a) at any time, a material misrepresentation is made or uncovered, or

(b) the Applicant does not provide, within the time specified by the NDMC, the supplemental information sought by the NDMC for evaluation of the Bid, or

(c) any act or omission of the Applicant results in violation of or non-compliance with this RFP document or any Applicable Laws (Clause No. 8.10).

Such misrepresentation/ improper response shall lead to the disqualification of the Applicant. If the Applicant is a Consortium, then the entire Consortium and each Member may be disqualified / rejected. If such disqualification / rejection occurs after the Bids have been opened and the Preferred Applicant gets disqualified / rejected, then the NDMC reserves the right to take any such measure as may be deemed fit in the sole discretion of the NDMC, including annulment of the Bidding Process.

4.5.3 In case it is found during the evaluation or at any time before signing of the Contract Agreement or after its execution and during the period of subsistence thereof granted by the NDMC, that one or more of the qualification conditions have not been met by the Applicant, or the Applicant has made material mis-representation or has given any materially incorrect or false information, the Applicant shall be disqualified forthwith if not yet appointed as the system integrator either by issue of the Letter of Acceptance or entering into of the Contract Agreement, and if the Preferred Applicant has already been issued the Letter of Acceptance or has entered into the Contract Agreement, as the case may be, the same shall, notwithstanding anything to the contrary contained therein or in this RFP document, be liable to be terminated void ab initio, by a communication in writing by the NDMC to the Preferred Applicant or the system integrator, as the case may be, without the NDMC being liable in any manner whatsoever to the Preferred Applicant or system integrator. In such an event, the NDMC shall be entitled to forfeit and appropriate the Earnest Money Deposit or Performance Security, as the case may be, as Damages, without prejudice to any other right or remedy that may be available to the NDMC under the RFP document and/ or the Contract Agreement, or otherwise.

B. DOCUMENT

4.6 Contents of the RFP Document

4.6.1 This RFP document comprises the disclaimer set forth hereinabove, the contents as listed below, and will additionally include any Addenda issued in accordance with Clause 4.8.

Invitation for Bids

Section 1. Invitation for Proposal

Section 2. Project Overview

Section 3. Project Objective and Scope

Section 4. Instructions to the Applicants

Section 5. Evaluation of Bids

Section 6. Appointment of system integrator

Section 7. Fraud and Corrupt Practices

Section 8. Miscellaneous

Section 9. Punitive Clause

Section 10. Force Majeure

Section 11. Event of Default and Termination

Section 12. Dispute Resolution

Section 13. Liquidated Damages

Section 14. Exit Management Schedule

Section 15. General Conditions of Contract

Annexures:

1. Letter comprising the application for Bid submission.
2. Pre contract Integrity Pact
3. Power of Attorney for Lead Member of Consortium
4. Joint Bidding Agreement
5. Bank Guarantee Format
6. Format for financial bid
7. Power of attorney for signing of Application
8. Statement of legal Capacity

9. Declaration of Non-Blacklisting
10. No Deviation Certificate
11. Manufacturers'/Producers' Authorization Form
12. Formats for submission of the Pre-Qualification Bid
13. Total Responsibility Certificate
14. Self-certificate for project execution experience (In Bidding Entity's Letter Head)
15. Overview of proposed solution
16. Project Plan
17. Manpower Plan
18. Curriculum Viate (CV) of Team Members
19. Compliance to Requirement (Technical/Functional Specifications)
20. Non-Disclosure Agreement
21. Proposed Bill of Material

4.7 Clarifications

4.7.1 Applicants requiring any clarification on the RFP document may notify the NDMC in writing by speed post/ courier/ special messenger and by e-mail and should send in their queries so as to reach the officer designated in Clause 1.4 by the date specified in Clause 1.6 (Key Events and Dates). NDMC shall endeavour to respond to the queries within the period specified therein, but no later than 7 (seven) days prior to the Bid Due Date. The responses will be sent by e-mail. The NDMC will upload clarifications, if any, on its website (www.ndmc.gov.in). The envelopes/ communication shall clearly bear the following identification/ title:

"Queries/Request for Additional Information: RFP for SI for Command Control Centre"

Email: seph.civil@ndmc.gov.in, secretary@ndmc.gov.in
juhi.mukharjee@gmail.com and cee1@ndmc.gov.in

4.7.2 The NDMC shall endeavour to respond to the questions raised or clarifications sought by the Applicants. However, the NDMC reserves the right not to respond to any question or provide any clarification, in its sole discretion, and nothing in this Clause shall be taken or read as compelling or requiring the NDMC to respond to any question or to provide any clarification.

4.7.3 The NDMC may also on its own motion, if deemed necessary, issue interpretations and clarifications to all Applicants through its website. All clarifications and interpretations issued by the NDMC shall be deemed to be part of the RFP document. Verbal clarifications and information given by NDMC or its employees or representatives shall not in any way or manner be binding on the NDMC.

4.8 Modification in the RFP Document

4.8.1 At any time prior to the Bid Due Date, the NDMC may, for any reason, whether at its own initiative or in response to clarifications requested by an Applicant, modify the RFP document by the issuance of Addendum.

4.8.2 Any Addendum / clarification issued hereunder will be in writing and will be published on the NDMC's website (www.ndmc.gov.in) and Delhi Government's website https://govtprocurement.delhi.gov.in to make it accessible to all Applicants, and shall be deemed to be a part of this RFP document.

4.8.3 In order to afford the Applicants a reasonable time for taking an Addendum into account, or for any other reason, the NDMC may, in its sole discretion, extend the Bid Due Date.

C. PREPARATION AND SUBMISSION OF BIDS

4.9 Format and Signing of Bid

4.9.1 Bidders who wish to participate in this proposal will have to register on e-procurement system of Delhi Government to participate in online proposals, bidders will have to procure Digital Signature Certificate (Type II or Type III) as per Information Technology Act, 2000 using which they can sign their electronic bids. Bidders may contact NCT of IT Department, NDMC and e-procurement cell, Government of Delhi for further assistance. Bidders who already have a Valid Digital Certificate need not procure a new digital certificate. Before electronic submission of proposal, it should be ensured that all the proposal papers including conditions of contract are read, understood by the Applicant. The uploaded document of the bid shall contain no alteration, or additions, unless notified. In case, the bidder makes addition and/or correction, the provision written in the original document, read with the addendum or corrigendum issued shall prevail. Scanned copy or proposals technical eligibility document and financial eligibility documents and all original papers related to Bank Guarantee, Power Attorney etc. should be uploaded with the technical bid. The Applicant shall provide all the information sought under this RFP document. The NDMC will evaluate only those Bids that are received in the required formats and complete in all respects.

4.9.2 The hard copy of the Bid shall be typed or written in indelible ink and signed by the authorised signatory of the Applicant who shall also initial each page, in blue ink. All the alterations, omissions, additions or any other amendments made to the Bid shall be initialled by the person(s) signing the Bid.

Applicant shall submit their offer only in online electronic format both for technical and financial proposal and all documents should be digitally signed. Scanned copy of Proposal fees, EMD and all original papers related to Bank guarantee, power of attorney etc. as mentioned in Table 5.2.3 & 5.3.2 should be uploaded along with the technical bid.

4.9.3 It is expected that Applicants have read and understood the RFP document along with clarification / addenda (if any) before the proposal submission. As a matter of confirmation of the same, a copy of the RFP document including other documents like clarification & addendum, if any, duly signed by the authorized signatory shall be submitted alongwith the bid. The bid documents shall have an index page with page numbers specified for all the key information/headers. Scanned copy of all the document to be uploaded on Delhi Government's website https://govtprocurement.delhi.gov.in

4.10 Sealing and Marking of Bids

4.10.1 A two envelope/cover system shall be followed for the bid. The Applicant shall upload the bid on e-procurement website of Delhi government and also submit the hard copy of Bid and seal it in the following two envelopes:

(a) Envelope A: (i) Earnest Money Deposit; (ii) Cost of RFP document (in case of downloaded RFP document), if any; and (iii) Eligibility Criteria including the following:

(i) Power of Attorney for signing of Bid, Authority Letter after the Resolution passed by the board of directors.

(ii) If applicable, the Power of Attorney for Lead Member of Consortium in the format of Annexure-3 ; and

(iii) A copy of the Contract Agreement with each page initialled by the person signing the Bid in pursuance of the Power of Attorney referred to in Clause (i) hereinabove.

(b) Envelope B: Technical Bid (as per Clause 5.3.2). All the relevant Documents of Envelope A & B to be scanned & uploaded on Delhi Government's website https://govtprocurement.delhi.gov.in

(c) Financial bid to be submitted in e-procurement website https://govtprocurement.delhi.gov.in only.

4.10.2 The Bid shall include the following documents: -

Envelope A: Hard copy as well as Uploading of scanned copies on e-tender website (https://govtprocurement.delhi.gov.in)

Sl. No.	Documents Type	Document Format
1.	Earnest Money Deposit (EMD)	EMD – Rs.1.00 Crore to be deposited in the form of Demand Draft/Pay order/Bankers Cheque/FDR/TDR in favour of "**Secretary, NDMC**" Payable at Delhi/New Delhi.
2.	Cost of RFP document, if applicable	Cost of RFP document (in case of RFP document downloaded from website) – Rs.25,000/- to be deposited in the form of Demand Draft/Bankers Cheque in favour of "**Secretary, NDMC**" Payable at Delhi/New Delhi.
3	Eligibility Criteria	The Eligibility Criteria shall be prepared in accordance with the requirements specified in RFP document.

Envelope B: Hard copy as well as Uploading of scanned copies on e-tender (https://govtprocurement.delhi.gov.in)

1 Technical Bid The Technical Bid shall be prepared in accordance with the requirements specified in this RFP document and in the formats prescribed. This Envelope should also mandatorily include un-priced Bill-of-Material (BOM).

To be uploaded Online on e-procurement portal

https://govtprocurement.delhi.gov.in

1 Financial Bid The Financial Bid proposal shall be submitted online **ONLY** on the https://govtprocurement.delhi.gov.in as per Annexure-6.

4.10.2 The two envelopes A & B specified in Clauses 4.10.1 shall be placed in an outer envelope, which shall be sealed. Each of the three envelopes shall clearly bear the following identification:

"Bid for the SI for ICCC"

and shall clearly indicate the name and address of the Applicant. In addition, the Bid Due Date should be indicated on the right hand top corner of each of the envelopes.

4.10.3 Each of the envelopes shall be addressed to the officer designated in Clause 1.4.

4.10.4 If the envelopes are not sealed and marked as instructed above, the NDMC assumes no responsibility for the misplacement or premature opening of the contents of the Bid submitted and consequent losses, if any, suffered by the Applicant.

4.10.5 Bids submitted by fax, telex, telegram or e-mail shall not be entertained and shall be rejected.

4.10.6 Bids not submitted online on e-tender (https://govtprocurement.delhi.gov.in) will not be considered for evaluation

4.11 Bid Due Date

4.11.1 Bids should be submitted before the Bid Due Date (Last date and time for submission of bids) at the address provided in Clause 1.4 in the manner and form as detailed in this RFP document.

4.11.2 The NDMC may, in its sole discretion, extend the Bid Due Date by issuing an Addendum in accordance with Clause 4.8 uniformly accessible for all Applicants.

4.12 Late Bids

Bids received by the NDMC after the specified time on the Bid Due Date (including the extended period if any) shall not be eligible for consideration and shall be summarily rejected.

4.13 Contents of the Bid

4.13.1 The Project will be awarded to the Preferred Applicant on completion of laid down process/formalities.

4.13.2 The opening of Bids and acceptance thereof shall be substantially in accordance with this RFP document.

4.13.3 The proposed Contract Agreement shall be deemed to be part of the Bid.

4.14 Modifications/ Substitution/ Withdrawal of Bids

4.14.1 The Applicant may modify, substitute or withdraw its Bid after submission, provided that written notice of the modification, substitution or withdrawal is received by the NDMC prior to the Bid Due Date. No Bid shall be modified, substituted or withdrawn by the Applicant on or after the Bid Due Date.

4.14.2 The modification, substitution or withdrawal notice shall be prepared, sealed, marked, and delivered in accordance with Clause 4.10, with the envelopes being additionally marked "MODIFICATION", "SUBSTITUTION" or "WITHDRAWAL", as appropriate.

4.14.3 Any alteration/ modification in the Bid or additional information supplied subsequent to the Bid Due Date, unless the same has been expressly sought for by the NDMC, shall be disregarded.

4.15 Opening of Bids

4.15.1 The NDMC shall open the Bids (Envelope A and B) received within the specified time, on the Bid Due Date as specified in Clause 1.6 at the place specified in Clause 1.4 and in the presence of the Applicants who choose to attend.

4.15.2 The representatives of the Applicants should carry the identity card or a letter of authority from the Applicant to identify their bonafides for attending the Technical Bid opening.

4.15.3 The NDMC will subsequently examine and evaluate the Bids in accordance with the provisions set out in this RFP document.

4.15.4 To facilitate evaluation of Bids, the NDMC may, at its sole discretion, seek clarifications in writing from any Applicant regarding its Bid.

4.15.5 The technical evaluation of only those Applicants will be done who will found eligible in terms of Clause 5.2.3

4.15.6 NDMC shall invite the Technically Qualified Applicants as declared in terms of clause 5.3.9.3 for the opening of the Financial Proposals. The date, time, and location of the opening of Financial Proposals will be informed by NDMC separately and individually to such Technically Qualified Applicants.

4.16 Rejection of Bids

4.16.1 Notwithstanding anything contained in this RFP document, the NDMC reserves the right to reject any Bid and to annul the Bidding Process and reject all Bids at any time without any liability or any obligation for such acceptance, rejection or annulment, and without assigning any reasons therefore. In the event that the NDMC rejects or annuls all the Bids, it may, in its discretion, invite all eligible Applicants to submit fresh Bids hereunder.

4.16.2 The NDMC reserves the right not to proceed with the Bidding Process at any time, without notice or liability, and to reject any Bid without assigning any reasons.

4.17 Validity of Bids

The Bids shall be valid for a period of not less than 180 (one hundred and eighty) days from the Bid Due Date. The validity of Bids may be extended by mutual consent of the respective Applicants and the NDMC.

4.18 Confidentiality

4.18.1 Information relating to the examination, clarification, evaluation and recommendation for the Applicants shall not be disclosed to any person who is not officially concerned with the process or is not a retained professional advisor advising the NDMC in relation to, or matters arising out of, or concerning the Bidding Process. The NDMC will treat all information, submitted as part of the Bid, in confidence and will require all those who have access to such material to treat the same in confidence. The NDMC may not divulge any such information unless it is directed to do so by any statutory entity that has the power under law to require its disclosure or is to enforce or assert any right or privilege of the statutory entity and/ or the NDMC or as may be required by law or in connection with any legal process.

4.18.2 The system integrator shall keep confidential all the details and information with regard to the Project, including systems, facilities, operations, management and maintenance of the systems/facilities.

4.18.3 The NDMC or its nominated agencies shall retain all rights to prevent, stop and if required take the necessary punitive action against the system integrator regarding any forbidden disclosure.

4.18.4 For the avoidance of doubt, it is expressly clarified that the aforesaid provisions shall not apply to the following information:

(i) information already available in the public domain;

(ii) information which has been developed independently by the Applicant / system integrator not affecting any interest of the NDMC;

(iii) information which has been received from a third party who had the right to disclose the aforesaid information;

(iv) information which has been disclosed to the public pursuant to a court order.

4.18.5 To the extent the system integrators are confidential or proprietary information with NDMC for effective performance of the Services, the provisions of the Clause 4.18.1 to 4.18.4 shall apply *mutatis-mutandis* on the NDMC.

4.19 Correspondence with the Applicant

Save and except as provided in this RFP document, the NDMC shall not entertain any correspondence with any Applicant in relation to acceptance or rejection of any Bid.

4.20 Contacts during Bid Evaluation

Bids shall be deemed to be under consideration immediately after they are opened on the Bid Due Date and until such time the NDMC makes official intimation of award through issuance of Letter to Acceptance to the Preferred Applicant/ rejection to the Applicants. While the Bids are under consideration, Applicants and/ or their representatives or other interested parties are advised to refrain, save and except as required under the RFP document, from contacting by any means, the NDMC and/ or their employees/ representatives on matters related to the Bids under consideration.

4.21 Deviation Statement

Applicants will note that NDMC will not entertain any deviations to the RFP document whatsoever may be including compliance to the technical specifications defined in the document at the time of submission of the Proposal or thereafter. The Proposal to be submitted by the Applicants would have to be unconditional and unqualified and the Applicants would be deemed to have accepted the terms and conditions of the RFP document with all its contents. Any deviation from the notified RFP document including compliance to the technical specifications will lead to disqualification of the applicant.

4.22 Bid Submission Format

The Applicant should ensure that all the required documents, as mentioned in this RFP document, are submitted alongwith the bid and in the prescribed format only. NDMC will not accept delivery of Proposal in any manner other than that specified in this RFP document. Proposal delivered in any other manner shall be treated as defective, invalid and rejected. Non-submission of the required documents or submission of the documents in a different format /contents may lead to the rejections of the bid proposal submitted by the Applicant.

4.23 Earnest Money Deposit (EMD)

4.23.1 The Applicant shall furnish as part of its Bid, an Earnest Money Deposit (EMD) of Rs.1.00 Crore (Rs. One Crore only) in the form of Demand Draft/ Pay Order/ Bankers Cheque/ FDR/ TDR in favour of “Secretary, NDMC” payable at Delhi/ New Delhi or in the form of a Bank Guarantee issued by a nationalized bank, or a Scheduled Bank in India, in favour of the “Secretary NDMC” in the format at Annexure–5 (the “Bank Guarantee”) and having a validity period of not less than 180 (one hundred eighty) days from the Bid Due Date, inclusive of a claim period of 60 (sixty) days, and may be extended as may be mutually agreed between the NDMC and the Applicant from time to time. In case the Bank Guarantee is issued by a foreign bank outside India, confirmation of the same by any nationalized bank in India is required. For the avoidance of doubt, Scheduled

Bank shall mean a bank as defined under Section 2(e) of the Reserve Bank of India Act, 1934.

4.23.2 The NDMC shall not be liable to pay any interest on the Earnest Money Deposit so made and the same shall be interest free.

4.23.3 Any Bid not accompanied by the Earnest Money Deposit shall be summarily rejected by the NDMC as non-responsive.

4.23.4 The Earnest Money Deposit of unsuccessful Applicants will be returned by the NDMC, without any interest, as promptly as possible on issuance of the Letter of Acceptance to the Preferred Applicant or when the Bidding process is cancelled by the NDMC.

4.23.5 The Preferred Applicant's EMD will be returned, without any interest, upon the system integrator signing the Contract Agreement after furnishing the Performance Security in accordance with the provisions thereof.

4.23.6 The NDMC shall be entitled to forfeit and appropriate the EMD as Damages *inter alia* in any of the events specified in Clause 4.23.7 herein below. The Applicant, by submitting its Bid pursuant to this RFP document, shall be deemed to have acknowledged and confirmed that the NDMC will suffer loss and damage on account of withdrawal of its Bid or for any other default by the Applicant during the period of Bid validity as specified in this RFP document. No relaxation of any kind on EMD shall be given to any Applicant.

4.23.7 The EMD shall be forfeited as Damages without prejudice to any other right or remedy that may be available to the NDMC under the RFP document and/ or under the Contract Agreement, or otherwise, if-

(i) An Applicant submits a non-responsive Bid;

(ii) An Applicant engages in a corrupt practice, fraudulent practice, coercive practice, undesirable practice or restrictive practice as specified in **Clause-7** of this RFP document;

(iii) an Applicant withdraws its Bid during the period of Bid validity as specified in this RFP document and as extended by mutual consent of the respective Applicant(s) and the NDMC;

(iv) The Preferred Applicant fails within the specified time limit -

(a) to sign and return the duplicate copy of Letter of Agreement; or

(b) to sign the Contract Agreement; or

(c) to furnish the Performance Security within the period prescribed therefore in the Contract Agreement.

In such an event, the decision of the NDMC regarding forfeiture of the EMD shall be final and binding upon Applicants.

4.23.8 Applicants should mention the beneficiary account details for EMD refund in the Earnest Money Deposit Form as required for Refund. The beneficiary account provided for EMD refund should remain active for successful EMD refund. The earnest money deposit of unsuccessful Applicants will be refunded through RTGS / NEFT mode. Applicants should submit canned copy of cancelled cheque of the beneficiary account for EMD refund.

4.23.9 In case of forfeiture of EMD as prescribed in as above, the Applicant shall not be allowed to participate in the rebidding process of the same project.

4.24 Pre-Bid Meeting

4.24.1 Pre-Bid Meeting will be convened at the designated date as mentioned in Clause 1.6 at a time and place specified by the NDMC.

4.24.2 Only those persons who have purchased this RFP document shall be allowed to participate in the pre-bid conference.

4.24.3 A maximum of three representatives of each person who has purchased this RFP document shall be allowed to participate on production of duly issued authority letter from such person and identity documents.

4.24.4 During the course of Pre-Bid Conference(s), the Applicants may seek clarifications and make suggestions for consideration of the NDMC.

4.24.5 The NDMC shall endeavour to provide clarifications and such further information as it may, in its sole discretion, consider appropriate for facilitating a fair, transparent and competitive Bidding Process.

4.24.6 All enquiries from the Applicants relating to this RFP document must be submitted in writing only to NDMC at the time of pre-bid meeting (Key Events and Dates – Clause 1.6).**The queries of applicants, who have purchased this RFP document, may be emailed to seph.civil@ ndmc.gov.in, cee1@ndmc.gov.in, secretary@ndmc.gov.in and juhi.mukharjee@gmail.com**

4.25 Deleted

4.26 Administrative Guidelines

4.26 This section describes the administrative guidelines, policies and procedures to be followed by the system integrator while undertaking operational activities. NDMC is particular about safeguarding the aesthetics and regulatory norms of NDMC and expects the system integrator to strictly abide to the same. This includes, but is not limited to, approach related to operational activities, safety and security aspects, repair and maintenance, vandalism, damage to public property, misuse of public amenities, misuse of public space and other key NDMC requirements. The system integrator is responsible for adhering to the following administrative guidelines:

(i) NDMC reserves the right to intervene at any point throughout the Contract Agreement for all administrative, operation and maintenance activities.

(ii) Any civil and architectural work or structural changes required while implementation should go through proper approvals from NDMC. Every plan that is submitted would be reviewed and approved with necessary amendments (if any) by the NDMC based on the project plan. The system integrator is responsible for incorporating the amendments proposed by the NDMC, and submit the revised plan for approval to NDMC. All civil and architectural changes are to be implemented by the system integrator only after the plans are approved by NDMC.

(iii) All regulatory approvals required for executing this project, acquired from concerned parties (Public and Private) should be planned and arranged by the system integrator. NDMC will extend assistance in getting the requisite permission from statutory bodies in this regard.

For permissions other than in purview of NDMC, the SI has to arrange such permissions at their own. NDMC may act as a facilitator for obtaining such permissions by the system integrator. However, this will not create any right in favour of the system integrator for getting such permission through NDMC.

(iv) NDMC will hold ownership of all hardware equipment and software components, including but not limited to all active and passive devices, sensors, servers, computer systems, solutions, applications, reports, software and licenses etc.

(v) The system integrator shall be responsible to keep all the tangible and intangible assets under this Agreement in good, operational and serviceable conditions at all times. Timelines have been defined in the RFP document.

(vi) The system integrator shall not cause any damage to Government buildings / other premises / property/ public places etc. If any damage occurs, the system integrator will perform necessary restoration at its own cost.

(vii) The work of system integrator shall be subject to inspection at various stages. The system integrator shall abide and follow all Safety and Security Regulations and practices at all times. The system integrator should use products only as per technical specifications defined in RFP document.

(viii) The system integrator would also be required to maintain a centralized Helpdesk monitoring system at the Centralized Command and Control Center, which will track new installations, complaints, issues logged by the O& M team.

(ix) All the hardware and software supplied and replaced should be new and from reputed OEMs as per the RFP document. The system integrator shall ensure that the products procured are of the OEM proposed in the bid. The material shall be checked/ validated/ audited through agency identified by NDMC, along with

Quality tests before dispatching to site or thereafter. The system integrator is responsible to check and validate all material including hardware, software and peripherals and provide the list of the same to NDMC before installation.

4.27 Operation and Maintenance (O&M) Guidelines

4.27 The system integrator shall follow the following Operation and Maintenance guidelines:

(i) The system integrator has to adhere to the operation and maintenance policies and procedures, as applicable from time to time, for managing and operating the Project. This includes (but not limited to) approach related to manpower, resources, vendor management, security, customer service, repair and maintenance and other primary functions, training programs to staff, user manuals, technical manuals, financial management, risk management, life/safety management, employee management and administrative policies and procedures for customer service improvement.

(ii) system integrator will be responsible to deploy on-field and off-field (but on-site at NDMC) resources for appropriate up-keeping, maintenance, and operation of all network, hardware, and software components, and ensure smooth functioning of the project throughout the entire O&M period of five years (60 months) from the date of Go-Live.

(iii) The Command and Control Center will be hosted and operated at NDMC premises. System Integrator will operate and maintain all equipments installed at Command Control Centre of Data Centre. Day to day operations at Command and Control Center will be monitored and operated by NDMC. All the hardware and software issues will be the responsibility of the system integrator.

(iv) After implementation period, the Operations and Maintenance (O&M) period shall be upto a period of five years (60 months) from the date of GO-LIVE.

(v) The system integrator shall provide comprehensive on-site warranty for all the hardware items, softwares and peripherals, supplied under this RFP.

(vi) The system integrator shall provide comprehensive Facility Management Service (**FMS**) for all devices, equipment and its related hardware, software, electrical and network infrastructure components supplied for the this project. This involves comprehensive maintenance of all component covered under the Contract Agreement, including configuration of servers, desktops, routers, switches, firewall, CCTVs, and various other active and passive components along with repair, replacement of parts, sensors, providing spare parts, updating, security alerts and patch updating, regular backup of the data etc.

(vii) The system integrator shall depute adequate manpower as full time dedicated onsite FMS team. The FMS team shall be deputed to identify, acknowledge, troubleshoot, manage, replace and repair the hardware/ system software. The FMS team shall undertake day-to-day troubleshooting and maintenance requirements for this project.

(viii) The FMS team shall be also be responsible for regular monitoring of all the equipment, proactively perform warranty checks, and generate SLA reports from the SLA monitoring tool.

(ix) The FMS team shall be required to take regular backup of the application data as per the frequency defined by NDMC. Security and safety arrangements for safe custody of the backup data shall also be the responsibility of system integrator upto O&M period.

Time frame for regular data backup will be provided by the applicant in its proposed architecture of the system. NDMC reserves its right to ask the SI to do modification in such time-frame, if required, at any time upto a period upto O&M period.

(x) The system integrator shall ensure that the FMS team has appropriate skill-sets for managing data center, networking, hardware and application software tools & ICCC.

(xi) The system integrator shall ensure that the instruction manuals, technical manuals and user manuals supplied by the manufacturer/ OEMs/ system integrator are referred, referenced, reviewed and maintained up-to-date at all times.

(xii) All patches and updates to any software and hardware devices shall be provided by the system integrator without any additional costs during O&M period.

(xiii) NDMC reserves the right to ask for replacement of any hardware, software and network components if it is not from approved OEM and does not conform to the specification/requirements specified in the RFP document.

(xiv) During the maintenance period, if any hardware or software needs to be replaced, the same will be replaced with same OEM and with same or higher configuration free of cost.

4.28 Passive Cabling Guidelines

4.28.1 The system integrator is required to carry out all work related to passive cabling under the scope of setting up the command center. All work under passive cabling should be governed by a set of standards that specify wiring data centers, offices, and other buildings for data or voice communications, using fibre cables. The category 7 (CAT 7) and modular sockets will only be used when requirement of data transfer is very low. For high data transfer fiber cable will be used. All materials used shall be conforming to relevant standard and as per ISO.

4.28.2 The system integrator should ensure that appropriate communication channels are setup for data, voice along with wireless compatibility. The system integrator should ensure that the cable layouts are neat and distinguishable. The termination of cables needs to be planned for future expansion of scope.

5 EVALUATION OF BIDS

5.1 BID EVALUATION

5.1.1 NDMC will evaluate the bids.

5.1.2 The NDMC may seek clarifications in writing from the Applicants on their proposals and may visit Applicant's client site to validate the credentials/ citations claimed by the Applicant.

5.1.3 Each of the responses shall be evaluated as per the criterions and requirements specified in this RFP document. NDMC reserves the right to reject any or all proposals on the basis of any deviations from this RFP document.

5.1.4 This is a Lowest Price Bid based selection. Only those applicants who achieve minimum technical criteria would be eligible for financial bid opening

5.1.5 Technical Score for being eligible for financial bid opening is 75 marks out of 100.

5.1A Tests of responsiveness

5.1A.1 Prior to evaluation of Bids, the NDMC shall determine whether each Bid is responsive to the requirements of this RFP document. A Bid shall be considered responsive if:

(i) it is received as per the format defined in RFP document.

(ii) it is received by the Bid Due Date including any extension thereof pursuant to Clause 4.11;

(iii) it is signed, sealed, bound together in hard cover and marked as stipulated in Clauses 4.9 and 4.10;

(iv) it is accompanied by the Earnest Money Deposit;

(v) it is accompanied by the Power(s) of Attorney, if applicable;

(vi) it contains all the information (complete in all respects) as requested in this RFP document (in formats same as those specified);

(vii) it quotes complete scope of Work as indicated in the RFP documents, addendum (if any) and any subsequent information given to the Applicant;

(viii) it does comply with all the Technical specifications and General Terms and conditions;

(ix) it does not contain any condition or qualification;

(x) the Applicant has submitted all additional information or clarification as sought by NDMC within the prescribed period;

(xi) Bids with duly signed integrity pact; and

(xii) it is not non-responsive in terms hereof.

5.1A.2 The NDMC reserves the right to reject any Bid which is non-responsive and no request for alteration, modification, substitution or withdrawal shall be entertained by the NDMC in respect of such Bid. Provided, however, that the NDMC may, in its discretion, allow the Applicant to rectify any infirmities or omissions if the same do not constitute a material modification of the Bid.

5.2 Earnest Money Deposit, RFP Document Cost (if applicable) and Eligibility Criteria (Envelope A)

5.2.1 The bids without Earnest Money Deposit will be summarily rejected.

5.2.2 In case, the Applicant has downloaded the RFP document from the NDMC’s website, then the Applicant is required to pay the cost of RFP document along with the EMD, failing which its bid will be rejected.

5.2.3 The bid of the Applicant shall be evaluated on the basis of the following Eligibility Criteria:

Pre-Qualification Criteria

S. No.	Eligibility Criteria	Document Proof	Scanned copy to be uploaded
1.	A Company Registered under the Companies Act 1956/2013; OR A Consortium of registered agencies consisting of: (i) Maximum 3 companies; and (ii) One of the consortium member should lead the consortium. Lead member should have more that 50% stake in the consortium and should be registered in India under the Companies Act 1956/2013; and (iii) Lead Member should be registered in India for atleast three completed financial years i.e. should be registered on or before 01/04/2014; and (iv) All the consortium members are equally responsible and jointly & severally liable under this RFP, including: • The delivery of products & services. • Successful completion of this entire Project • Meeting the SLAs; and (v) Other consortium members should be a legal entity; and (vi) Technical and financial experience of members of the consortium having more than 26% stake in the consortium will only be considered for the purpose of this RFP.	• Copy of Certificate of Incorporation/ Registration under Companies Act, 1956/2013. • Consortium agreement clearly stating the roles and responsibilities of each member.	**PQ-1**
2.	The average annual Turnover (TO) in Indian Rupees for last 3 audited financial years (2014-15, 2015-16, 2016-17) in the field of (a) ICT infrastructure	• Certificate from the Statutory auditor/CA clearly specifying the annual turnover for the specified years. • In case, audited report for F.A. 2016-17 is not available,	**PQ-2**

	(b) IT system integration services (c) IT hardware manufacturer/ software developer • For Sole Applicant or , lead member (in case of Consortium) shall have average annual turnover of Rs. 100 Cr.	certificate from Statutory Auditor / CA to this effect of fulfill this requirement be provided, and the audited report be provided within 30 days of its availability.	
3.	The Sole Applicant or lead member (in case of Consortium), shall have the Positive Net-Worth (PNW) in Indian Rupees as on end of financial year 2015-16 as Rs. 20 Cr.	• Certificate from the Statutory auditor/CA clearly specifying the net worth of the firm.	**PQ-3**
4.	The Sole Applicant or lead member (in case of Consortium), shall not have incurred losses during last three years.	• Certificate from the Statutory auditor/CA clearly specifying the same has to be submitted.	
5.	Duly signed Integrity Pact **as per Annexure – 2**	• The applicant has to submit duly signed Integrity Pact as per Annexure-2 alongwith its proposal.	**PQ-4**
6.	The sole Applicant or the Lead Applicant in case of a Consortium , should possess the below Certifications which are valid at the time of bid submission: (i) CMMI level 5 and above ; and (ii) ISO 9001:2008 certification for system integration; or ISO 20000:2011 for IT Service Management; or ISO 27001:2005 for Information Security Management System	• Copies of valid certificates in the name of the sole Applicant or the Lead Applicant in case of a Consortium.	**PQ-5**
7.	**Experience in development of Smart City component *** Applicant or any Consortium Partner having more than 26% stake in the consortium, should have experience in implementation and maintenance of following project of value not less than INR 10 Crore in India or abroad	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	

	in last seven years: a)Utility Management (Water OR Electricity SCADA) and or b)Command & Control Centre or c) Network Operations Centre (NOC) in India or abroad in last 7 years. Or Establishment of Command Control Centre with at least 1000 IP based CCTV Cameras successful installation & operations in any govt./semi govt./other agencies. Note: • Bidder can propose separate (one or more) projects for each component for evaluation. Each project should have minimum value of INR 10 Crores	are required: i. Letter from the Company Secretary of the bidder certifying that the entity whose experience is shown is parent/subsidiary Company • Shareholding pattern of the bidding entity as per audit reports	
7.	100% compliance to technical specification and functionality as per this RFP.	Compliance sheet to technical specifications and functionalities.	**PQ-6**
8.	The Applicant or Lead member in case of Consortium, shall have Bank Solvency certificate of not less Rs. 40 Crores (certificate issued within last six months from the date of issue of this RFP document will be considered for this purpose).	Certificate from Bank	**PQ-7**

9.	Registration under Tax, Labour Laws, Electrical Laws, etc.
	.1.1
		The Applicant or the Lead Applicant should have a registered number of:
		(a) VAT/Sales Tax where its business is located;
		(b) Service Tax;
		(c) Income Tax PAN;
		The ESI & EPF registration as per Labour Laws;
			Copies of relevant(s) Certificates of Registration.
			In case of (i) ESI Registration; or/and (ii) EPF registration, if such certificate is not available, and if such ESI and EPF registration will be required as per the

			proposed work then in such case an undertaking on a stamp paper of Rs.10 shall be provided stating that the same will be obtained within a period of two months from the date of signing of the agreement; **PQ-8**
10.	No Barring Certificate	Sole Applicant or in case of consortium all members of the consortium, which has been barred, by the Central Government/ any State Government/ NDMC, or any entity controlled by these, from participating in any project (BOT or otherwise), and the bar subsists as on the date of Application, would not be eligible to submit an Application, either individually or as member of a Consortium.	Undertaking by the authorized signatory as well as all member of consortium as per the form mentioned in Annexure- 9; PQ-9

Note: 1. The System integrator shall comply with all applicable laws, including labour laws, at any point of time throughout the contract period.

2. For Sr. No. 6, (*****) the proposed project will be considered for evaluation only if its scope covers following under the individual component:

- **Utility Management System (Water/Electricity/any other utility SCADA):** Assignment in which Electrical/Water/ other utility city level / township level / campus level distribution system is automated for real time management and operations.
- **Command & Control Centre (ICCC)/ Network Operation Centre (NOC):** Assignment in which ICCC/ NOC comprising of Command

Centre Application, Management (Video wall) room, Operations room, Contact center/helpdesk are built.

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

4. 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 submission of bids under the tender document shall be used for conversion of amount in foreign currency to Indian Rupees equivalent.

5.2.4 The successful applicant will get done provisional registration of GST within 60 days from the date from which it will be applicable.

5.2.5 Consortium as mentioned in clause 5.2.3 above shall be subject to the condition mentioned below in clauses 5.2.7 and 5.2.8.

5.2.6 The Applicant shall submit all the documents in the prescribed formats mentioned in the RFP document.

5.2.7 Consortium

The Applicant for participation in the Selection Process, maybe (a) a single entity or (b) a Consortium, coming together to execute the project. No Member at any given point of time, may assign or delegate its rights, duties or obligations under the Agreement except with prior written consent of the NDMC. The Lead member shall have more than 50% holding in the consortium and cannot assign or delegate its rights, duties or obligation under the Agreement throughout the contract period.

No Applicant applying individually, or as a member of a Consortium, as the case may be, can be member of another consortia bidding for the project.

In the event the Applicant is a Consortium, it shall, comply with the following additional requirements:

1. Number of members in a consortium shall not exceed 03 (three) including the Lead Member.

2. Members of the Consortium shall nominate one member as the Lead Member (the “Lead Member”); who shall have more than 50% holding in the consortium throughout the contract period;

3. The Lead Member will remain responsible for successful delivery of the project at all times throughout the contract period;

4. The Lead Member shall be authorized and shall be fully responsible for the accuracy and veracity of the representations and information submitted by itself and all other Members of the consortium respectively from time to time in response to this RFP.

5. Members of the Consortium shall enter into a binding Joint Bidding Agreement, for the purposes of making the Application and submitting a Bid.

6. Subject to the provisions of sub-clause(5) above, the Joint Bidding Agreement should contain the information required for each member of the Consortium and shall, inter alia:

   i. Undertake that each of the members of the Consortium shall have an independent, definite and separate scope of work which was allocated as per each member’s field of expertise;

   ii. Commit to the profit and loss sharing ratio of each member;

   iii. Commit to the scope of work, rights, obligations and liabilities to be held by each member; specifically commit that the Lead Member shall be answerable on behalf of other members for the performance of obligations and duties under this Agreement,

   iv. provide a brief description of the roles and responsibilities of individual members; and clearly define the proposed administrative arrangements (organization chart) for the management and execution.

   v. Include a statement to the effect that all members of the Consortium shall be severally liable for all obligations in relation to the Assignment until the completion of the Assignment in accordance with the Agreement;

vi. Undertake that all Members shall comply with all lock-in requirements set forth in the RFP.

vii. Commit that each of the members, whose experience will be evaluated for the purposes of this RFP document, shall, for a period of 2 (two) years from the date of commercial operation of the Project, hold 26% or more holding in the consortium at the time of submission of bid and may only be replaced by such other party having same or better technical capabilities as well as eligibility conditions with prior approval of the NDMC;.

viii. Undertake;

a. that notwithstanding anything contrary contained in this RFP or the Agreement, the Lead Member shall always be liable for obligations and duties of all the Consortium Members i.e. for both its own liability as well as the liability of other Members.

b. that the Lead Member shall be liable for the entire scope of work and risks involved and further shall be liable and responsible for ensuring the individual and collective commitment of each of the Members of the Consortium in discharging all of their respective general obligations under this RFP;

c. Each Member further undertakes to be individually liable for the performance of its part of the obligations with out in any way limiting the scope of collective liability envisaged in the RFP

d. that the Members of the Consortium shall alone be liable for all obligations of the identified sub-contractor and clearly indemnify NDMC against any losses or third party claims arising due to the sub-contractor/consortium’s default.

e. that the Lead Member is liable to manage the complete assignment by taking responsibility and maintain transparency around monetary terms.

7. The technical and Net Worth of the Members shall satisfy the conditions of eligibility as prescribed in this RFP;

8. The nomination of the Lead Members hall be supported by a Power of Attorney, as per the format in this RFP signed by the other members of the Consortium. The duties, responsibilities and powers of such Lead Member shall be specifically included in the Consortium Agreement. It is expected that the Lead Member would be authorized to incur liabilities and to receive instructions and payments for and on behalf of the Consortium. The NDMC expects that Lead Member should have complete responsibility pertaining to execution of Assignment;

9. Any change to the composition of the consortium can be done only with the prior approval of the NDMC. The Lead Member will be responsible for the scope of work to be delivered by the exiting member, whether he does it himself or through a new member of the consortium. In case of a new member, the Lead Member will take the prior approval of the NDMC, before on boarding the member, who is expected to possess same or better technical qualifications as well as eligibility criteria that is of the existing member to be replaced by such new member. The Lead Member is also responsible for incorporating relevant changes in the Joint Bidding Agreement, as per Annexure–4.

5.2.8 An Applicant shall not have a conflict of interest (the "**Conflict of Interest**") as provided in Clause 8.14 that affects the Bidding Process. Any Applicant found to have a Conflict of Interest shall be disqualified. In the event of disqualification, the NDMC shall be entitled to forfeit and appropriate the Earnest Money Deposit or Performance Security, as the case may be, as mutually agreed genuine pre-estimated loss and damage likely to be suffered and incurred by the NDMC and not by way of penalty for, inter alia, the time, cost and effort of the NDMC, including consideration of such Applicant's proposal, without prejudice to any other right or remedy that may be available to the NDMC under the RFP Document and/ or the Contract Agreement or otherwise.

5.2.9 The Applicant shall promptly inform the NDMC of any change in the status of the Applicant with reference to any of the eligibility criterion specified in clause 5.2.3 to 5.2.5, and failure to do so shall render the Applicant liable for disqualification from the Bidding Process.

5.2.10 Only those Applicants who meet the eligibility criteria specified in Clauses 5.2.3 to 5.2.5 shall qualify for technical evaluation under Clause 5.3. Applications of firms/ consortia who do not meet these criteria shall be rejected.

5.3 Technical Evaluation (Envelope B)

5.3.1 Applicants, who will found eligible in terms of Clause 5.2 above, would be considered for technical evaluation.

Technical Evaluation Framework

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

Section	Evaluation Criteria	Points
A	Sole Applicant /Consortium Profile	20
B	Sole Applicant /Consortium Project Experience	41
C	OEM Qualification (for Quality of products offered)	14
D	Approach & Methodology & Project Presentation/Demonstration	15
E	Proposed Resources for the Project	10
Technical Score		100

5.3.2 Criteria for Technical Evaluation

<table>
<tr><th>No.</th><th>Technical Evaluation Criteria</th><th>Technical Evaluation parameter</th><th>Points</th><th>Name to be given to the PDF file to be uploaded</th></tr>
<tr><td colspan="5"><b>A. Sole Applicant/Consortium profile Max. Marks : 20</b></td></tr>
<tr><td>A1</td><td><b>Average Annual Turnover of</b>
last 3 audited financial years (2013- 14, 2014-15,
2015-16).in following fields
(i) ICT solution
(ii) Telecom infrastructure
(iii) IT system integration services</td><td><table>
<tr><th>Average Annual Turnover (Indian Rupees)</th><th>Percentage</th></tr>
<tr><td>>= 200 Cr.</td><td>100</td></tr>
<tr><td>>= 175 Cr. and
< 200 Cr.</td><td>90</td></tr>
<tr><td>>= 150 Cr. and <
175 Cr.</td><td>75</td></tr>
<tr><td>>= 100 Cr. and <
150 Cr.</td><td>60</td></tr>
</table></td><td><b>8</b></td><td><b>PQ-10</b></td></tr>
<tr><td>A2</td><td><b>Net worth as on 2015- 16 financial year end</b></td><td><table>
<tr><th>Net Worth
(Indian Rupees)</th><th>Percentage</th></tr>
<tr><td>>= 100 Cr.</td><td>100</td></tr>
<tr><td>>= 75 Cr. and
< 100 Cr.</td><td>90</td></tr>
<tr><td>>= 50 Cr. and <
75 Cr.</td><td>75</td></tr>
<tr><td>>= 20 Cr. and <
50 Cr.</td><td>60</td></tr>
</table></td><td><b>8</b></td><td><b>PQ-10</b></td></tr>
</table>

<table>
<tr>
<td>A3</td>
<td><b>People in organization (Full time Employees –FTE in ICT projects)</b></td>
<td>
<table>
<tr><th>Number of FTE</th><th>Percentage</th></tr>
<tr><td>> 700 FTE</td><td>100</td></tr>
<tr><td>> 600 FTE to =<700 FTE</td><td>90</td></tr>
<tr><td>> 500 FTE to =<600 FTE</td><td>75</td></tr>
<tr><td>=< 500 FTE</td><td>60</td></tr>
</table>
</td>
<td><b>4</b></td>
<td><b>PQ-10</b></td>
</tr>
<tr>
<td colspan="5"><b>B. Project Experience of Sole Applicant/ any consortium member Max. Mark : 41</b></td>
</tr>
<tr>
<td>B1</td>
<td><b>Executing Information and Communications Technology(ICT) Projects</b></td>
<td>• The Applicant should have experience in executing ICT projects.
• Each project work Rs. 50 Cr (Indian Rupees) is considered as one unit.
• Points are allocated based on number of units executed
<table>
<tr><th>Number of units</th><th>Percentage</th></tr>
<tr><td>= 4 or >4</td><td>100</td></tr>
<tr><td>= 3</td><td>90</td></tr>
<tr><td>=2</td><td>75</td></tr>
<tr><td>=1</td><td>60</td></tr>
</table>
</td>
<td><b>8</b></td>
<td><b>PQ-11</b></td>
</tr>
</table>

<table>
<tr>
<td>B2</td>
<td><b>Data Centre</b></td>
<td>
<ul>
<li>The Applicant should have experience in executing projects for setting up, O&M of Data Centre of atleast 500 TB storage</li>
<li>Each project of data centre having 500 TB storage or more will be considered as one unit.</li>
<li>Points are allocated based on number of units executed</li>
</ul>
<table>
<tr><th>Number of units</th><th>Percentage</th></tr>
<tr><td>= 4 or >4</td><td>100</td></tr>
<tr><td>= 3</td><td>90</td></tr>
<tr><td>=2</td><td>75</td></tr>
<tr><td>=1</td><td>60</td></tr>
</table>
</td>
<td><b>8</b></td>
<td><b>PQ-11</b></td>
</tr>
<tr>
<td>B3</td>
<td><b>Integration with Smart Utility Solutions such as</b>
<b>Water -SCADA, Power, ITMS, Smart SWM, Smart Sewerage/Drainage</b></td>
<td>
<ul>
<li>The Applicant should have experience in projects of integration with Smart Utility Solutions such as Water -SCADA, Power, ITMS, Smart SWM, Smart Sewerage/ Drainage</li>
<li>Each project of Indian Rupees 2 Cr. Or more for integration with Smart Utility solutions will be considered as one unit.</li>
<li>Points are allocated based on
number of units executed</li>
</ul>
<table>
<tr><th>Number of units</th><th>Percentage</th></tr>
<tr><td>= 4 or >4</td><td>100</td></tr>
<tr><td>= 3</td><td>90</td></tr>
<tr><td>=2</td><td>75</td></tr>
<tr><td>=1</td><td>60</td></tr>
</table>
</td>
<td><b>6</b></td>
<td><b>PQ-11</b></td>
</tr>
</table>

<table>
<tr>
<td>B4</td>
<td><b>Command and Control Center installations</b></td>
<td>
• The Applicant should have experience in executing projects for operationalization of Command and Control/Communications Centre (covering surveillance/ traffic/ disaster management/ city
operations functions).
• Each executed project of Rs. 10 Crore value will be considered as one unit.
• Points are allocated based on number of units executed
<table>
<tr><th>Number of units</th><th>Percentage</th></tr>
<tr><td>= 4 or >4</td><td>100</td></tr>
<tr><td>= 3</td><td>90</td></tr>
<tr><td>=2</td><td>75</td></tr>
<tr><td>=1</td><td>60</td></tr>
</table>
</td>
<td><b>12</b></td>
<td><b>PQ-11</b></td>
</tr>
<tr>
<td>B5</td>
<td><b>ERP System</b></td>
<td>
• The Applicant should have experience in executing projects for customization/ configuration and installation of ERP system for an urban local body (Municipal Corporation / municipal council /
Development authority).
• Each executed project worth Indian Rupees Two Crores will be considered as one unit.
• Points are allocated based on number of units executed
<table>
<tr><th>Number of units</th><th>Percentage</th></tr>
<tr><td>= 4 or >4</td><td>100</td></tr>
<tr><td>= 3</td><td>90</td></tr>
<tr><td>=2</td><td>75</td></tr>
<tr><td>=1</td><td>60</td></tr>
</table>
</td>
<td><b>7</b></td>
<td><b>PQ-11</b></td>
</tr>
</table>

<table>
<tr><th colspan="5"><b>C.</b> OEM Qualification (for Quality of products offered) Max. Marks : 14</th></tr>
<tr>
<td>C1</td>
<td>Evaluation of the products offered on the basis of Original Equipment Manufacturer (<b>OEM</b>)</td>
<td>The products offered by the Applicant in its bid for this project will be evaluated on the basis of manufacturer of the products as per Gartner Magic Quadrant. OEM Qualification for the following categories of the products/ equipment will be evaluated as per Gartner Magic Quadrant:
<table>
<tr><th>Parameters</th><th>Max. Marks</th></tr>
<tr><td>Magic Quadrant for Data Center Networking (Datacenter Switches)</td><td>3</td></tr>
<tr><td>Magic Quadrant for Enterprise Network Firewalls or Intrusion Prevention Systems</td><td>3</td></tr>
<tr><td>Magic Quadrant for Servers</td><td>3</td></tr>
</table>
In terms of Gartner Magic Quadrant, marks would be awarded as per the following criteria:
OEM prescribed as Leaders (3 Marks)
OEM prescribed as Challengers (2 Marks)
OEM prescribed as Visionaries (1 Marks)
OEM prescribed as Niche Players, (0 Marks) or OEM not listed in Gartner magic Quadrant</td>
<td><b>9</b></td>
<td><b>PQ-12</b></td>
</tr>
<tr>
<td>C2</td>
<td>Evaluation of the products offered on the basis of Original Equipment Manufacturer (OEM)</td>
<td>The smart city central control application offered by the Applicant in its bid for this project will be evaluated on the basis of manufacturer of the products as per Navigant Research Leader board. OEM Qualification for the following categories of the products/ equipment will be evaluated as per <b>Navigant Research Leader boar</b>d:
In terms of Navigant Research Leader board, marks would be awarded as per the following criteria:</td>
<td><b>5</b></td>
<td><b>PQ-12</b></td>
</tr>
</table>

<table>
<tr><td></td><td></td><td>OEM prescribed as Leaders (5 Marks)
OEM prescribed as Contenders (3 Marks)
OEM prescribed as Challengers (1 Marks)
OEM prescribed as Followers, or
OEM not listed in Navigant Research Leader board (0 Marks)</td><td></td><td></td></tr>
<tr><td colspan="5"><b>D. Approach & Methodology & Project Presentation/Demonstration Max. Marks : 15</b></td></tr>
<tr><td>D1</td><td><b>Approach &
Methodology</b></td><td><table><tr><th>Parameters</th><th>Percentage</th></tr><tr><td>As per details mentioned in clause 5.3.6.3</td><td>80</td></tr><tr><td>Presentation</td><td>20</td></tr></table></td><td><b>7.5</b></td><td><b>PQ-13</b></td></tr>
<tr><td>D2</td><td><b>Project Presentation/ Demonstration</b></td><td>Following parameters will be evaluated during live demonstration<b>:</b><table><tr><th>Parameters</th><th>Percentage</th></tr><tr><td>Demonstration of ICCC & ERP, live projects/ projects executed and claimed in the project experience</td><td>70</td></tr><tr><td>Demonstration of ICCC & ERP, projects under implementation.</td><td>30</td></tr></table></td><td><b>7.5</b></td><td><b>PQ-13</b></td></tr>
<tr><td colspan="5"><b>E. Proposed Resources for the Project Max. Marks : 10</b></td></tr>
<tr><td>E1</td><td><b>People on project</b></td><td>Marking as per Clause 5.3.6.2</td><td><b>10</b></td><td><b>PQ-14</b></td></tr>
</table>

Note: (i) Work Orders and Client Certificates for successful completion of such work confirming period and area of activities for the purpose of clause 5.3.2 should be enclosed. Self-certification shall be submitted by the Applicant for works executed for internal purposes. NDMC can verify such submissions / work orders / client certificates submitted by the Applicant through any means, including site visits.

ii) If the applicant is a l00% subsidiary of any legal entity, then the financial and technical capabilities of such parent legal entity may be considered for purpose of Technical and Financial eligibility of Clause 5.2.3 and 5.3.2, subject to the condition that the parent company will own the responsibility of its subsidiary company.

iii) System Integrator has to ensure that proposed OEM should not have been blacklisted by any sovereign government and barred from participating in government projects due to security reasons in the last five years.

iv) The value of executed works shall be brought to current costing level by enhancing the actual value of work at simple rate of 7% per annum, calculated from the date of completion to the last date of submission of bid.

5.3.3 The Technical Evaluation of Applicant's proposals (Envelope B) shall be based on:

(i) Technical Proposal Evaluation;

(ii) Technical Presentation; and

(iii) Demonstration.

5.3.4 Technical Presentation

The Applicants, who will found eligible in terms of Clause 5 above, will be asked to give a presentation on its proposal on date, time and place as communicated to the Applicant by the NDMC in writing before the Bid Evaluation Committee.

5.3.5 Demonstration and Client Visit

5.3.5.1 The Demonstration will be evaluated as per the following procedure:

(i) Each shortlisted Applicant shall demonstrate the solution offered.

(ii) The Applicant is expected to demonstrate the complete proposal as per RFP document;

a. Integration of hardware and software and functioning of the same simultaneously;

b. Interface in between various components of the projects on a common communication platform;

c. All equipments / applications can communicate back and forthwith the centralized Command and Control Centre, and comply to all the Scope, Requirements, Standards etc. mentioned in the RFP document.

(iii) The demonstration should provide representative solution to integrate various aspects of the project as per the scope of the project.

5.3.5.2 Demonstration shall be in English.

5.3.5.3 NDMC may visit various client sites national or global to validate the project citations and implementation experience quoted by the Applicant. The NDMC will bear the expenses on the NDMC officers/officials tour and the Applicant shall facilitate the same.

5.3.5.4 All the expenses incurred by the Applicant for the purposes mentioned in the clause 5.3.4 and clause 5.3.5 will be borne by the Applicant.

5.3.6 Manpower deployment

NDMC would like to give emphasis on the suitable technical staff proposed for the contract period. Applicant may propose personnel for different skill-sets required for different responsibilities during Project Implementation (upto GO-LIVE) & Post-Implementation (after GO-LIVE) periods. Following documentation is expected in this section:

(i) Overall Project Team (for both Project Implementation & Maintenance phases), consists of Top Management Team and Core Delivery Team (Implementation, O&M and On-Premise Teams) as per requirement.

(ii) Escalation Chart for the entire Project Duration

(iii) Summary Table giving Qualification, Experiences, Certifications, Relevance to the project, including detail CVs.

(iv) Undertaking stating that deployed manpower will be exactly same as that proposed in the Bid for Technical Evaluation.

5.3.6.1 Key Personnel criteria

SI shall provide adequate number of personnel, each responsible for a specific role within the project. SI shall provide clear definition of the role and responsibility of each individual personnel.

SI shall have a defined hierarchy and reporting structure for various teams that shall be part of the project. SI has to provide the list of proposed Resources for the Project. Any changes in Resource deployment will have to be approved by the NDMC.

Following table indicates the minimum qualification required for Key Positions identified for this project. However, SI shall independently estimate the teams size required to meet the requirements of Service Levels as specified as part of this tender.

Except for Project Director, all other proposed positions shall be Onsite throughout the entire project implementation phase.

5.3.6.2 Resource Planning (Total Marks-10)

#	Criteria	Criteria Details	Marks Allotted in %
1.	Resource Deployment Plan & Governance structure	Bidder would be evaluated for Resource Deployment Plan & Governance Structure	30
2.	Program Manager	Refer to Team Evaluation Matrix Below	10
3.	Citizen Service/Municipal Domain expert	Refer to Team Evaluation Matrix Below	5
4.	Water SCADA or Electrical SCADA expert	Refer to Team Evaluation Matrix Below	5
5.	IBMS expert	Refer to Team Evaluation Matrix Below	5
6.	Command Center Design Expert (Civil)	Refer to Team Evaluation Matrix Below	5

7.	ITMS Expert	Refer to Team Evaluation Matrix Below	5
8.	Solution Architect	Refer to Team Evaluation Matrix Below	5
9.	Project Manager-Software	Refer to Team Evaluation Matrix Below	5
10.	Project Manager-Infrastructure	Refer to Team Evaluation Matrix Below	5
11.	Database Architect	Refer to Team Evaluation Matrix Below	5
12.	Security Expert	Refer to Team Evaluation Matrix Below	5
13.	Command and Control Centre management Expert	Refer to Team Evaluation Matrix Below	5
14.	Mobile App development Expert	Refer to Team Evaluation Matrix Below	5
		Total	**100**

Team Evaluation Matrix

Program Manager = 10 points

a)Educational Qualification:

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

b)Certification :

- PMP / Prince 2 Certification = 2 Points

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

- >=10 years = 3 points
- >=8 and <10 year =2 Points
- >=5 and <8 year =1 Points
- Else 0

d)Project/Program management Experience in ICT implementation Project of

value > 100 crores:

- >= 3 Projects= 1.5 Points
- 2 Projects = 1 points
- Else 0

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

- 1 Project= 1.5 Points
- Else 0

Citizen Service/Municipal Domain expert= 5 Points

a) Educational Qualification:

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

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

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

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

- At least 1 Project = 2 point
- Else 0

Electrical or Water or utility SCADA expert = 5 Points

a) Educational Qualification:

- Bachelor's Degree in Engineering/MCA = 1 Points
- Else 0 Points

b) Work experience in Implementation of SCADA Projects:

- >=9 years = 3 points
- >=6 and <9 year =1.5 Points
- Else 0

c) International work experience in Implementation of SCADA Projects:

- At least 1 Project = 1 point
- Else 0

IBMS expert = 5 Points

a) Educational Qualification:

- Bachelor's Degree in Engineering/MCA = 1 Points
- Else 0 Points

b) Work experience in Implementation of IBMS Projects:

- >=9 years = 3 points
- >=6 and <9 year =1.5 Points
- Else 0

c) International work experience in Implementation of IBMS Projects:

- At least 1 Project = 1 point
- Else 0

Command Center Design Expert (Civil)=5 Points

a) Educational Qualification:

- Bachelor's Degree in Engineering/ Architect = 1 Points
- Else 0 Points

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

- >=9 years = 3 points
- >=6 and <9 year =1.5 Points
- Else 0

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

- At least 1 Project = 1 point
- Else 0

Intelligent Transport Management System (ITMS) Expert= 5 Points

a) Educational Qualification:

- Bachelor's Degree in Engineering/MCA = 1 Points
- Else 0 Points

b) Work experience in Implementation of ITMS Projects:

- >=9 years = 3 points
- >=6 and <9 year = 1.5 Points
- Else 0

c) International work experience in Implementation of ITMS Projects:

- At least 1 Project = 1 point
- Else 0

Solution Architect=5 Points

a) Educational Qualification:

- Bachelor's Degree in Engineering/MCA = 1 Points
- Else 0 Points

b) Work experience as IT/ICT solution architect:

- >=9 years = 3 points
- >=6 and <9 year = 1.5 Points
- Else 0

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

- At least 1 Project = 1 point
- Else 0

Project Manager-Software = 5 Points

a) Educational Qualification:

- Bachelor's Degree in Engineering/MCA = 1 Points
- Else 0 Points

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

- >=9 years = 3 Points

- >=6 and <9 year = 1.5 Points
- Else 0

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

- At least 1 Project = 1 Points
- Else 0

Project Manager – IT/ICT Infrastructure=5 Points

a) Educational Qualification:

- Bachelor's Degree in Engineering/MCA = 1 Points
- Else 0 Points

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

- >=9 years = 3 Points
- >=6 and <9 year =1.5 Points
- Else 0

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

- At least 1 Project = 1 Points
- Else 0

Database Architect= 5 Points

a) Educational Qualification:

- Bachelor's Degree in Engineering/MCA = 1 Points
- Else 0 Points

b) Work experience as Database architect:

- >=9 years = 3 Points
- >=6 and <9 year =1.5 Points
- Else 0

c) International work experience as Database architect:

- At least 1 Project = 1 Points
- Else 0

IT Security Expert= 5 Points

a) Educational Qualification:

- Bachelor's Degree in Engineering/MCA = 0.5 Points
- Else 0 Points

i. Certification

- CISA= 1 Point

c) Work experience as IT Security Expert:

- >=9 years = 3 Points
- >=6 and <9 year = 1.5 Points
- Else 0

d) International work experience as IT Security Expert:

- At least 1 Project = 0.5Points
- Else 0

Command and Control Centre (ICCC) Expert = 5 Points

a) Educational Qualification:

- Bachelor’s Degree in Engineering/MCA = 1 Points
- Else 0 Points

b) Work experience as ICCC Expert:

- >=9 years = 3 Points
- >=6 and <9 year =1.5 Points
- Else 0

c) International work experience as ICCC Expert:

- At least 1 Project = 1 Point
- Else 0

Mobile App development Expert= 5 Points

a) Educational Qualification:

- Bachelor’s Degree in Engineering/MCA = 1 Points
- Else 0 Points

b) Work experience as Mobile App development Expert:

- >=5 years = 3 Points
- >=3 and <5 year =1.5 Points
- Else 0

c) International work experience as Mobile App development Expert:

- Atleast 1 Project = 1 Points
- Else 0

Note: The Presentation has to delivered by proposed Program Manager

5.3.6.3 Approach and Methodology

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 No.	Details
1.	Please explain your understanding of the project.
2.	Please provide the proposed solution and network architecture of NDMC Smart City
3.	Please explain how would you ensure that the implementation phase is completed within stipulated timeframe of 6 months
4.	What will be the 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 NDMC as well as new applications or systems that may be envisaged / developed in the future by NDMC.
5.	Please identify major risks for the project and also propose suitable mitigation plan for each of these risks.
6.	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
7.	What have been your key learnings from the similar projects and how do you propose to incorporate them in executing this assignment
8.	How SLAs mentioned under this RFP will be measured? What tools will be used for SLA measurement?
9.	What should be the Cloud Strategy of NDMC with respect to scope of this RFP? Please elaborate on pros and cons of this strategy.
10.	Please explain your detailed approach and methodology for executing this project
11.	Innovation in ICCC solution.
	Total

5.3.7 Technical Solution Proposed for the Project (Approach, Methodology, Project Management, Execution Methodology, SLA Management)

Broad areas to be covered in the Technical Solution documentation are given below:

(i) Bill of Material (i.e. un-priced Financial Bid format): This document should give indication of all the proposed cost components, without specifying the costs. **<u>Applicant should note that the bid shall get disqualified if Applicant gives price details in the technical document.</u>**

(ii) Describe the proposed Technical Solution for each of the initiative, namely Command and Control Centre including Data Centre, integration with other applications and other scope defined in the RFP. Following should be captured in the same:

a. Detailed description of the design and technical solution and various applications and components including make of equipment or sizing of infrastructure (including diagrams and calculations wherever applicable);
b. Compliance to technical requirements specified in the scope of work;
c. Technical Design and clear articulation of benefits to NDMC of various components of the solution
d. Strength of the Applicant to provide services including examples or case studies of similar solutions deployed for other clients;
e. Any other parameter.

(iii) Provide detailed Approach and Methodology for Implementation and Post-Implementation periods.

(iv) Approach & Methodology for Management of SLA Requirements specified in the RFP document. Applicant is required to clearly articulate how each of the SLA requirements would be adhered in a table format.

(v) Detailed Project Plan with timelines, resource allocation, milestones etc. in for supply, installation and commissioning of the physical and IT components for the Command and Control Centre including data centre and networking.

(vi) Insights into Best and latest Industry practices and standards.

5.3.8 Compliance Table to the IT/ Non-IT Components

The RFP document has specified the minimum specifications in clause of volume II of the RFP for various components. Applicant has to give a comprehensive compliance sheet for the equipment/software proposed by them including make and model number.

5.3.9 Technical Scoring and Evaluation

5.3.9.1 For the purpose of arriving at Technical Score, the bid shall be evaluated against the Technical Parameters, with respective weightage, as given in RFP document.

5.3.9.2 The Total Technical Score will be calculated out of 100 Marks. The Applicant has to score the following minimum Qualifying Marks to qualify in the Technical Evaluation Criteria:

- 60% marks in individual Technical Evaluation Criteria; and
- 75% marks out of total 100 Marks of Technical Evaluation criteria.

5.3.9.3 The Applicants scoring marks less than the minimum qualifying marks as mentioned above shall be disqualified for Financial Bid Opening. The Applicants scoring marks equal to or more than the minimum qualifying marks as mentioned above shall be declared as Technically Qualified Applicants.

5.4 FINANCIAL BID

5.4.1 Submission of Financial Bids

5.4.1.1 The Applicant shall quote the unit rate and total amount of equipment to be supplied as per the bill of material table

5.4.1.2 The information regarding cost of equipments, cost of installations, manpower costs and O&M costs throughout the O&M period should be provided as per the financial bid format given in the RFP document (Annexure-6).

5.4.1.3 Any bid which does not conform to the formats prescribed above in clause 5.4.1.1 and 5.4.1.2 will be disqualified.

All bids which are technically qualified shall be invited for financial bid opening.

5.4.2 Financial Evaluation

5.4.2.1 The Financial Bids of Technically Qualified Applicants will be opened on date, time and place as communicated to the Applicant by the NDMC in writing in the presence of Applicants who choose to attend.

5.4.2.2 The Financial Bids shall be evaluated on the basis of the total amount quoted by the applicant as per financial bid in the prescribed Performa given in the RFP and QCBS formula Giving 70% weightage to technical evaluation and 30% weightage to financial quote of Applicant.

5.4.2.3 The Applicant whose Financial Bid has the lowest total quoted amount for the Project ("L1 Applicant") shall be given a Financial Score of 100 marks. The financial scores of other Technically Qualified Applicants shall be computed as follows:

Financial Score of Applicant for the Project (Y) = 100 x total amount quoted by the L1 Applicant (in INR) / total amount quoted by the Applicant (in INR)

5.4.2.4 The marks secured based on evaluation of the Financial Bid as per Clause 5.4.2.3 above shall be the financial score of the Applicant for the Project ("Financial Score")

5.5 Composite Score of the Applicants

Composite Score of the Applicants shall be worked out as under:

	Applicant's Scores (A)	Weightage (B)	Weighted Score [(C) = (A) x (B)]
Technical Score	X	70%	(0.7)(X)
Financial Score	Y	30%	(0.3)(Y)
Composite Score of the Applicant			(0.7)(X) + (0.3)(Y)

5.6 Evaluation for Preferred Applicant

5.6.1 The Applicant who has secured the **highest Composite Score** as calculated under clause 5.5 shall be declared the Preferred Applicant for the Project.

5.6.2 In the event that two or more Applicants secure exactly the same Composite Score in respect of the Project, then the Preferred Applicant will be selected in the following manner:

(a) The Applicant whose Financial Score is highest for the Project among such Applicants having same Composite Score will be declared as Preferred Applicant;

(b) In case, Applicants having same Composite Score also have same Financial Score, then the Applicant having more Technical score will be declared as Preferred Applicant;

(c) In case, Applicants having same Composite Score, Financial score and Technical score, then the Applicant having more Financial networth at the end of financial year 2015-16 will be declared as Preferred Applicant

(d) If none of the above resolves the tie, a simple draw method will be used for tie-breaking. The Preferred Applicant will be selected only from such Applicants having same Composite Score, Financial score and Technical score by draw on date, time and place as communicated to all such Applicants by the NDMC in writing in presence of such Applicants who choose to attend.

6 Appointment of System Integrator

6.1 Selection of Applicant

6.1.1 After selection of Preferred Applicant in terms of Clause 5.6, a Letter of Acceptance (the "LOA") shall be issued, in duplicate, by the NDMC to the Preferred Applicant and the Preferred Applicant shall, within 7 (seven) days of the receipt of the LOA, sign and return the duplicate copy of the LOA in acknowledgement thereof. In the event the duplicate copy of the LOA duly signed by the Preferred Applicant is not received by the stipulated date, the NDMC may, unless it consents to extension of time for submission thereof, appropriate the Earnest Money Deposit of such Applicant as Damages on account of failure of the Preferred Applicant to acknowledge the LOA.

6.1.2 Issue of Letter of Acceptance (LOA) shall not be construed as any right given in favour of the Preferred Applicant, and NDMC reserves the right to annul the process of award, including signing of Contract Agreement, of this project without any liability or any obligation for such annulment, and without assigning any reasons there for.

6.1.3 Upon issue of LOA to the Preferred Applicant, NDMC will release the EMD of all Applicants, except the Preferred Applicant.

6.1.4 After acknowledgement of the LOA as aforesaid by the Preferred Applicant, it shall cause the Preferred Applicant to execute the Contract Agreement within the period prescribed in Clause 1.7(i.e. 15 days from the date of issue of LOA). The Preferred Applicant shall not be entitled to seek any deviation, modification or amendment in the Contract Agreement.

6.2 Deleted.

6.3 Performance Bank Guarantee

6.3.1 The Preferred Applicant will be required to submit a Performance Bank Guarantee (PBG) equivalent to 10% of the total contract amount quoted by the preferred bidder to the NDMC within 15(fifteen) days from the date of receipt of Letter of Acceptance. In case of a Consortium, the Lead Applicant of Consortium shall be liable to pay Performance Bank Guarantee

6.3.2 Performance Bank Guarantee shall be valid for 180 days beyond the term of the Contract Agreement. The Performance Guarantee shall contain a claim period of three months from the last date of validity.

6.3.3 In case, the Preferred Applicant fails to submit performance bank guarantee within the time stipulated, the NDMC at its discretion may cancel the Letter of Acceptance issued to the Preferred Applicant without giving any notice and may invoke the EMD of such Preferred Applicant.

6.3.4 NDMC shall invoke the Performance Bank Guarantee in case the selected SI fails to discharge their contractual obligations during the Contract Agreement period or NDMC incurs any loss due to SI’s negligence in carrying out the project implementation as per the agreed terms and conditions.

6.4 Release of Performance Bank Guarantee

The Performance Bank Guarantee will be released only after meeting all of the following conditions:

(i) After successful implementation of this project;

(ii) Successful operation and maintenance of all the services under this agreement;

(iii) Payment of all the penalties throughout implementation, operation and maintenance period;

(iv) Payment of all contract fees as per agreement alongwith penalties, if any;

(v) At the end of the contract period, Performance Bank Guarantee of SI will be released after successful handing over all the assets and services, including all hardware, software, network and services in working conditions. If any deficiency noticed at the time of handing over the SI has to get rectified/replaced the same at his own cost within 15 days otherwise NDMC will get it rectified at the risk and cost of the SI.

(vi) On production of clearance for all applicable dues, if any.

6.5 Signing of Contract Agreement

6.5.1 Subsequent to NDMC's issuing Letter of Acceptance to the Preferred Applicant, the Preferred Applicant shall execute the Contract Agreement with the NDMC within a period of 15 days from the date of issue of the Letter of Acceptance subject to the condition that the Performance Bank Guarantee has been deposited by the Preferred Applicant within the prescribed period.

6.5.2 Failure of the Preferred Applicant to furnish the Performance Bank Guarantee or execute the Agreement within the prescribed time shall cause the EMD of the Preferred Applicant to be liquidated. The Preferred Applicant will be liable to indemnify NDMC for any additional cost or expense, incurred on account of failure of the Preferred Applicant to execute the Agreement.

6.5.3 Notwithstanding anything to the contrary mentioned above, NDMC at its sole discretion shall have the right to extend the time lines for execution of Agreement on the request of the Preferred Applicant, provided the same is bona-fide.

6.6 TAX LIABILITY

6.6.1 The System Integrator shall be responsible for all the statutory taxes, statutory dues, local levies, Service tax, GST, etc. to be paid to Government / Statutory bodies / Authorities etc. for the services rendered by it. There will be no tax liability upon the NDMC whatsoever on any account.

6.6.2 The System Integrator indemnifies NDMC from any claims that may arise from the statutory authorities in connection with this License.

6.6.3 The System Integrator should ensure enforcement of Applicable Laws including Labour Laws, Minimum Wages Laws etc. and at no point of time should the NDMC be drawn into litigation on these counts.

6.7 Failure to Agree with the Terms and Conditions of the RFP document

6.7.1 The performance of Applicant will be continuously reviewed by NDMC to maintain the terms & conditions as specified in this RFP document. Based on the review, if the System Integrator fails to satisfy / maintain their commitment with respect to SLAs, Performance, Timely Implementation of the Project etc defined in the RFP document. the Contract Agreement may be terminated by giving 30 days notice as cure period and if it is not cured within 30 days then NDMC will terminate the Contract Agreement by giving further notice of 30 days for termination of Contract Agreement. NDMC's decision in this regard will be final. In case of termination of this Contract Agreement, NDMC shall have the right to avail services of any other Applicant / agency to continue the project without any let or hindrance from Applicant and the Applicant has to provide all necessary assistance for smooth switch over. NDMC will not pay any charges to the Applicant. Failure of the Preferred Applicant / System Integrator to agree with the RFP document shall constitute sufficient grounds for the annulment of the award, in which event NDMC may take a decision to re-issue the RFP document. In such a case, NDMC shall invoke the EMD/PBG of the Preferred Applicant/System Integrator.

6.7.2 In addition, NDMC reserves the right to appropriate the EMD / Performance Bank Guarantee given by the Applicant / System Integrator and black-list the Applicant/ System Integrator.

6.7.3 The SI has to meet the timeline and milestone as per clause 3.3. Failing to adhere to the timelines shall result in imposing liquidated damages and invoking of termination clauses

6.8 Payment Terms

6.8.1 Payments for the Applicant will be done on the basis of the table given below. The various timelines and related milestones have been below and payment will be made as per the achievement of milestones of RFP

S. No.	Milestone	Payment
P1	On Completion of Civil, Electrical, Air-conditioning work of ICCC and DC.	100% of the value of this component subject to submission of BG of equivalent amount.
P2	Upon delivery & inspection of IT	100% of the CAPEX Value of the items delivered (except software and its integration), subject to

	hardware.	submission of BG of equivalent amount.
P3	Integration and commissioning of first 12 services of Phase-I defined in table under Clause 3.3 .	33% of the cost of software and its integration after deducting necessary taxes. 1/3rd of the BG kept against payment released for P1 & P2 will also be released.
P4	Integration and commissioning of balance services of Phase-I and eight services of Phase-2 defined in table under Clause 3.3.	33% of the cost of software and its integration after deducting necessary taxes security deposit @ 10%. 1/3rd of the BG kept against payment released for P1 & P2 will also be released.
P5	supply, installation, commissioning and integration with ICCC of RFID based Solid waste Management System	Payment of RFID based Solid waste Management System
P6	Implementation of ERP Solution.	Payment of ERP Solutions
P7	supply, installation, commissioning and integration with ICCC of all 500 Surveillance cameras	Payment of Surveillance Cameras Solutions
P8	Go-live of complete project for all components and services as per timelines	Balance payment of the CAPEX Value will be released. Balance BG kept against payment released for P1 & P2 will also be released.
P9	Quarterly payments after Go-live of complete project for Operation & Maintenance period of five years.	Quarterly payment of O&M cost will be released at the end of each quarter after deducting penalties, if any.

(i) All payments will be made against invoices raised by the SI with required supporting documents

(ii) Payment to the SI would be on milestone basis for P1, P2, P3, P4,P5,P6,P7 & P8 and on quarterly for P9 in a year based on the invoice submitted in accordance with the payment schedule mentioned above and the deductions based on the performance on the SLAs defined in this RFP. Additionally, all payments to be made by NDMC to the SI shall be inclusive of all statutory levies, duties, taxes and other charges whenever levied / applicable (including Service Tax as applicable). Service Tax and/ or GST will be reimbursed after submission of proof of depositing the service tax and/ or GST.

(iii) Taxes and Statutory Payments will be paid by the SI.

(iv) All payments agreed to be made by NDMC to the SI in accordance with the Bid shall be inclusive of all statutory levies, duties, taxes and other charges, whenever levied/applicable.

(v) The SI shall bear all personal/income taxes levied or imposed on it and its personnel, etc. on account of payment received under this Contract. The SI shall bear all income/corporate taxes, levied or imposed on the SI on account of payments received by it from NDMC for the work done under this Contract. The SI shall bear all other taxes such as sales tax, octroi, VAT, custom duty, service tax, etc..

7. FRAUD AND CORRUPT PRACTICES

7.1 The Applicants and their respective officers, employees, agents and advisers shall observe the highest standard of ethics during the Bidding Process and subsequent to the issue of the Letter of Acceptance (**LOA**) and during the subsistence of the Contract Agreement. Notwithstanding anything to the contrary contained herein, or in the LOA or the Contract Agreement, the NDMC may reject a Bid, withdraw the LOA, or terminate the Contract Agreement, as the case may be, without being liable in any manner whatsoever to the Applicant or System Integrator, as the case may be, if it determines that the Applicant or System Integrator, as the case may be, has, directly or indirectly or through an agent, engaged in corrupt practice, fraudulent practice, coercive practice, undesirable practice or restrictive practice in the Bidding Process. In such an event, the NDMC shall be entitled to forfeit and appropriate the EMD or Performance Security, as the case may be, as Damages, without prejudice to any other right or remedy that may be available to the NDMC under the RFP document and/ or the Contract Agreement, or otherwise.

7.2 Without prejudice to the rights of the NDMC under Clause 6.1 hereinabove and the rights and remedies which the NDMC may have under the LOA or the Contract Agreement, or otherwise if an Applicant or System Integrator, as the case may be, is found by the NDMC 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 Bidding Process, or after the issue of the LOA or the execution of the Contract Agreement, such Applicant or System Integrator shall not be eligible to participate in any tender or RFP document issued by the NDMC during a period of 2 (two) years from the date such Applicant or System Integrator, as the case may be, is found by the NDMC to have directly or indirectly or through an agent, engaged or indulged in any corrupt practice, fraudulent practice, coercive practice, undesirable practice or restrictive practices, as the case may be.

7.3 For the purposes of this Clause 6, 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 actions of any person connected with the Bidding Process (for avoidance of doubt, offering of employment to or employing or engaging in any manner whatsoever, directly or indirectly, any official of the NDMC who is or has been associated in any manner, directly or indirectly, with the Bidding Process or the LOA or has dealt with matters concerning the Contract 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 the NDMC, shall be deemed to constitute influencing the actions of a person connected with the Bidding Process); or (ii) save and except as permitted under the Clause 4.1.22 of this RFP document, engaging in any manner whatsoever, whether during the Bidding Process or after the issue of the LOA or after the execution of the Contract Agreement, as the case may be, any person in respect of any matter relating to the Project or the LOA or the Contract Agreement, who at any time has been or is a legal, financial or technical adviser of the NDMC in relation to any matter concerning the Project;

(ii) "**fraudulent practice**" means a misrepresentation or omission of facts or suppression of facts or disclosure of incomplete facts, in order to influence the Bidding Process;

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

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

(v) "**Restrictive practice**" means forming a cartel or arriving at any understanding or arrangement among Applicants with the objective of restricting or manipulating a full and fair competition in the Bidding Process.

8. MISCELLANEOUS

8.1 Jurisdiction of Court

The Bidding Process shall be governed by, and construed in accordance with, the laws of India. The courts at Delhi/New Delhi shall have the exclusive jurisdiction over all disputes arising under, pursuant to and/ or in connection with the Bidding Process.

8.2 The NDMC, in its sole discretion and without incurring any obligation or liability, reserves the right, at any time, to;

(i) suspend and/ or cancel the Bidding Process and/ or amend and/ or supplement the Bidding Process or modify the dates or other terms and conditions relating thereto;

(ii) consult with any Applicant in order to receive clarification or further information;

(iii) retain any information and/ or evidence submitted to the NDMC by, on behalf of, and/ or in relation to any Applicant; and/ or

(iv) independently verify, disqualify, reject and/ or accept any and all submissions or other information and/ or evidence submitted by or on behalf of any Applicant.

8.3 It shall be deemed that by submitting the Bid, the Applicant agrees and releases the NDMC, its employees, agents and advisers, irrevocably, unconditionally, fully and finally from any and all liability for claims, losses, damages, costs, expenses or liabilities in any way related to or arising from the exercise of any rights and/ or performance of any obligations hereunder, pursuant hereto and/ or in connection with the Bidding Process and waives, to the fullest extent permitted by applicable laws, any and all rights and/ or claims it may have in this respect, whether actual or contingent, whether present or in future.

8.4 The Applicant shall take all necessary precautions to prevent any nuisance or inconvenience to the owners, tenants or occupiers of adjacent properties during execution of work.

8.5 In the event of any restrictions being imposed by the NDMC, security agencies, traffic agencies, or any other authority in the working area, System Integrator shall strictly follow such restrictions and nothing shall be excused from doing the stipulated work on this account. The loss of time on this account, if any, shall have to be made by deploying additional resources to complete the work in time. Other restrictions are given as under:-

(i) The movement of trucks and vehicles shall be regulated in accordance with rules and regulations as approved by competent authority;

(ii) The System Integrator shall inform in advance, the truck registration numbers, ownerships of the trucks, names and address of the drivers;

(iii) Labour huts of workmen will not be allowed at project area and in NDMC area;

(iv) The System Integrator shall be responsible for behavior and conduct of his staff. The System Integrator shall engage no staff with doubtful integrity or having a bad record;

(v) The workers of the System Integrator should strictly observe code of conduct and manner befitting security. If any employee of the System Integrator fails to absolve proper conduct, the SI shall be liable to remove him from deployment, immediately in receipt of the instructions of the NDMC;

(vi) The System Integrator shall be responsible for the conduct and behavior of its workers employed for the work;

(vii) The NDMC shall have the right, to have any person removed who is considered unacceptable due to the reasons of security, efficiency, etc. Similarly, System Integrator reserves the right to change the staff as per its requirement;

(viii) The NDMC shall not be responsible for any compensation, which may be required to be paid to the worker(s) of the System Integrator consequent upon any injury/ mishap.

8.6 The Applicant has to give the month-wise and quarterly scheduled completion plan along-with the technical bid. However, total implementation will have to be completed in 12(twelve) months. If the targets for each quarter is not completed then necessary penalties will be impose and also no further permission will be given to lay further fibre network or to execute any kind of work.

8.7 Commercial services will only be allowed after completion of target of each quarter for services to be delivered to NDMC.

8.9 Indemnity Clause

The System Integrator shall defend, indemnify, release and hold harmless the NDMC from and against any and all loss, damage, injury, liability, demands and claims for injury to or death of any person (including an employee of the System Integrator or NDMC) or for loss of or damage to property (including System Integrator or NDMC property), in each case whether directly or indirectly resulting from or arising out of System Integrator performance under this RFP document / contract agreement. This indemnity shall apply whether or not NDMC was or is claimed to be passively, concurrently, or actively negligent, and regardless of whether liability without fault is imposed or sought to be imposed on NDMC. Such indemnity shall not apply to the extent that it is void or otherwise unenforceable under applicable law in effect on or validly retroactive to the date of this RFP document / contract agreement and, shall not apply where such loss, damage, injury, liability, death or claim is the result of the sole negligence or willful misconduct of the NDMC.

8.10 Applicable Law(s)

8.10.1 The System Integrator has to follow all the applicable statues, laws, bye-laws, rules, regulations, orders, ordinances, protocols, codes, guidelines, policies, notices, directions, judgments, decrees or other requirements or official directive of any government authority or court or other law, rule or regulation approval from the relevant governmental authority, government resolution, directive, or other government restriction or any similar form of decision of, or determination by, or any interpretation or adjudication having the force of law in India as amended form time to time while providing these services.

8.10.2 Compliance with the labour laws and minimum wages Act

8.11 Integrity Pact

The Applicant shall submit a duly signed integrity pact **as per Annexure-2** along with its proposal as per the RFP document.

8.12 Documents and Information

The documents including this RFP document and all attached documents, provided by the NDMC are and shall remain or become the property of the NDMC and are transmitted to the Applicants solely for the purpose of preparation and the submission of a Bid in accordance herewith. Applicants are to treat all information as strictly confidential and shall not use it for any purpose other than for preparation and submission of their Bid. The provisions of this Clause shall also apply mutatis mutandis to Bids and all other documents submitted by the Applicants, and the NDMC will not return to the Applicants any Bid, document or any information provided along therewith.

8.13 Language

The Bid and all communications in relation to or concerning the RFP Document and the Bid shall be in English language. If any supporting document is in any language other than English, translation of the same in English language duly attested by the Applicant, shall be provided. In case of discrepancy, English translation shall govern.

8.14 Conflict of Interest

An Applicant shall be deemed to have a Conflict of Interest affecting the Bidding Process, if:

(i) the Applicant, its Member or Associate (or any constituent thereof) and any other Applicant, its Member or any Associate thereof (or any constituent thereof) have common controlling shareholders or other ownership interest; provided that this disqualification shall not apply in cases where the direct or indirect shareholding of an Applicant, its Member or an Associate thereof (or any shareholder thereof having a shareholding of more than 5% (five per cent) of the paid up and subscribed share capital of such Applicant, Member or Associate, as the case may be) in the other Applicant, its Member or Associate, is less than 5% (five per cent) of the holding in the consortium thereof; provided further that this disqualification shall not apply to any ownership by a bank, insurance company, pension fund or a public financial institution referred to in sub-section (72) of section 2 of the Companies Act, 2013. For the purposes of this Clause, indirect shareholding held through one or more intermediate persons shall be computed as follows: (aa) where any intermediary is controlled by a person through management control or otherwise, the entire shareholding held by such controlled intermediary in any other person (the "Subject Person") shall be taken into account for computing the shareholding of such controlling person in the Subject Person; and (bb) subject always to sub-clause (aa) above, where a person does not exercise control over an intermediary, which has shareholding in the Subject Person, the computation of indirect shareholding of such person in the Subject Person shall be undertaken on a proportionate basis; provided, however, that no such shareholding shall be reckoned under this sub-clause (bb) if the shareholding of such person in the intermediary is less than 26% of the holding in the consortium of such intermediary; or

(ii) a constituent of such Applicant is also a constituent of another Applicant; or

(iii) such Applicant, its Member or any Associate thereof receives or has received any direct or indirect subsidy, grant, concessional loan or subordinated debt from any other Applicant, its Member or Associate, or has provided any such subsidy, grant, concessional loan or subordinated debt to any other Applicant, its Member or any Associate thereof; or

(iv) such Applicant has the same legal representative for purposes of this Bid as any other Applicant; or

(v) such Applicant, or any Associate thereof, has a relationship with another Applicant, or any Associate thereof, directly or through common third party/ parties, that puts either or both of them in a position to have access to each other's information about, or to influence the Bid of either or each other; or

(vi) such Applicant or any Associate thereof has participated as a consultant to the NDMC in the preparation of any documents, design or technical specifications of the Project.

For purposes of this Clause, Associate means, in relation to the Applicant/ Consortium Member, a person who controls, is controlled by, or is under the common control with such Applicant/ Consortium Member (the "Associate"). As used in this definition, the expression "control" means, with respect to a person which is a company or corporation, the ownership, directly or indirectly, of more than 50% (fifty per cent) of the voting shares of such person, and with respect to a person which is not a company or corporation, the power to direct the management and policies of such person by operation of law.

8.15 Non Transferability of RFP document

This RFP document is non-transferable.

8.16 Severability

If for any reason whatsoever any provision of this Agreement is or becomes invalid, illegal or unenforceable or is declared by any court of competent jurisdiction or any other instrumentality to be invalid, illegal or unenforceable, the validity, legality or enforceability of the remaining provisions shall not be affected in any manner, and the Parties shall negotiate in good faith with a view to agreeing upon one or more provisions which may be substituted for such invalid, unenforceable or illegal provisions, as nearly as is practicable. Provided failure to agree upon any such provisions shall not be subject to dispute resolution under this Agreement or otherwise.

8.18 Notices

Unless otherwise stated, notices to be given under this Agreement including but not limited to a notice of waiver of any term, breach of any term of this Agreement and termination of this Agreement, shall be in writing and shall be given by hand delivery, recognized international courier, mail, telex or facsimile transmission and delivered or transmitted to the Parties at their respective addresses set forth below:

If to NDMC:
__________________________________ (designation of authorized officer)
____
____
Fax No. ___________________________

If to the SI:
The _______________________________ (Designation)
____
____
____
Fax No. ____________________________

Or such address, telex number, or facsimile number as may be duly notified by the respective Parties from time to time, and shall be deemed to have been made or delivered:

(i) in the case of any communication made by letter, when delivered by hand, by recognized international courier or by mail (registered, return receipt requested) at that address, and

(ii) in the case of any communication made by telex or facsimile, when transmitted properly addressed to such telex number or facsimile number.

8.20 Waiver

8.20.1 Waiver by either Party of any default by the other Party in the observance and performance of any provision of or obligations under this Agreement:

i. shall not operate or be construed as a waiver of any other or subsequent default hereof or of other provisions or obligations under this Agreement;

ii. shall not be effective unless it is in writing and executed by a duly authorised representative of such Party; and

iii. shall not affect the validity or enforceability of this Agreement in any manner.

8.20.2 Neither the failure by either Party to insist on any occasion upon the performance of the terms, conditions and provisions of this Agreement or any obligation hereunder nor time or other indulgence granted by a Party to the other Party shall be treated or deemed as waiver/breach of any terms, conditions or provisions of this Agreement.

9 Punitive Clause

9.1 Service Level Agreement (SLAs)

The purpose of this Service Level Agreement (hereinafter referred to as SLA) is to clearly define the levels of service which shall be provided by the SI to NDMC for the duration of this Contract.

The benefits of the SLA are as follows:

(i) Increasing client/ client organization satisfaction with IT services

(ii) Reducing the risk of not meeting business requirements for IT services

(iii) Better communication and information flows between IT staff and customers

(iv) Standards and guidance for IT staff

(v) Greater productivity and better use of skills and experience

(vi) A quality approach to IT services

The NDMC shall regularly review the performance of the services being provided by the SI and the effectiveness of this SLA. It would also form a baseline for the NDMC to compute payment for the SI. The State Designated Agency will also review the SLA periodically.

NDMC will impose a fine on the SI for not meeting the **Implementation Service Level Agreements (SLAs)** and **Post-Implementation SLAs** as detailed below:

9.2 SLAs during Implementation period: These SLAs shall be used to evaluate the timelines for completion of deliverables that are listed in the deliverable. These SLAs will be applicable for commissioning of the project (upto GO-LIVE). For delay of every week in completion & submission of the deliverable mentioned in the proposal, the SI would be charged with penalty as follows:

Implementation phase related performance levels

Measurement	Definition	Target	Penalty
Manpower Deployment			
Team	SI is expected to mobilize project	Within 15 days of	Delay beyond 7

mobilization and commencement of work	team for commencement of work. Commencement of work would mean reporting and availability of SI's resources (90% Key Personnel as per the RFP requirement) at the NDMC office for the project within defined period of 15 days and remaining 10% in next 15 days).	signing of contract agreement.	calendar days = 0.2% of project cost excluding O&M cost of the Delay beyond 8-15 calendar days = 0.5% of the project cost excluding O&M cost. Delay beyond 15 days may lead to Termination of the Contract at the discretion of the NDMC. However, every such delay of 15 days, after first 15 days, a penalty of 1% of the project cost excluding O&M cost. Will be imposed upon the SI.

Delay in execution of work (in Weeks) as per Clause 3.3	**Penalty value**
Per week	0.5% per week of the Project cost excluding O&M cost.
Maximum	10% of the total Project cost excluding O&M cost. In case of delay in execution goes beyond six months from the scheduled date of Go-live then NDMC may terminate the contract.

In case, the SI reaches maximum of penalty at any point of time, NDMC reserves the right to invoke the termination clause.

In case any service for integration is not ready from NDMC, the Concessionaire will integrate the same within three months from the date from which the same will be made available.

9.3 Post-Implementation SLAs

9.3.1 These SLAs shall be used to evaluate the performance of the services on monthly basis but penalties would be levied for cumulative performance for the quarter basis.

9.3.2 Penalty levied for non-performance as per SLA requirements shall be deducted from the payment due to the SI. If the penalties amount exceeds 25% of the OPEX cost in a year then NDMC will have the right to terminate the agreement.

9.3.3 The SLA parameters shall be measured for each of the sub systems' SLA parameter requirements and measurement methods, through appropriate SLA Measurement tools to be provided by the SI and audited by NDMC for accuracy and reliability. The SI would need to configure the SLA Measurement Tools such that all the parameters as defined under SLA matrix given below. Post-implementation SLAs, should be measured and appropriate reports be generated for monitoring the compliance.

9.3.4 In the event of non-compliance to Clause 9.3.3, NDMC reserves the right to invoke the termination clause. All the activities and obligations pursuant to the termination, shall be as per Termination Clause as provided in this RFP document.

9.3.5 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:

(i) **"Total Time"** - Total number of hours in the quarter (or the concerned period) being considered for evaluation of SLA performance.

(ii) **"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*

(iii) **"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.

(iv) **“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 NDMC 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 6 times a year.

(v) **“Incident” -** Any event / abnormalities in the service being rendered, that may lead to disruption in normal operations and services to the end user.

(vi) **“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.

(vii) **“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.

9.3.6 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 SI is linked to the compliance with the SLA metrics. The matrix specifies three levels of performance, namely,

(i) The SI will get 100% of the Contracted value if all the baseline performance metrics are compiled and the cumulative credit points are 100

(ii) The SI will get lesser payment in case of the lower performance. (For e.g. if SLA point score is 80 then the SI will get 20% less on the quarterly payment – The formula calculating the deductions is “(100 – SLA Point Score)%”)

(iii) 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 SI and approved and audited by NDMC or its appointed Consultant for accuracy and reliability.

NDMC 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.

Total liquidated damages to be levied on the SI shall be capped at 10% of the total contract value. However, NDMC 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 25% of the OPEX value. NDMC would also have right to invoke termination of contract in case cumulative debit point (breach points) are above twenty five in two consecutive quarters.

9.3.7 SLA Matrix for Post Implementation SLAs

#	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 - <20 secs High Complexity query - < 40 sec	5	Simple complexity Query = 5.01 – 10 secs Medium complexity query = 20.01 – 40 secs High Complexity query = < 40.1 sec – 80 secs	2.5	Simple complexity Query = > 10 secs Medium complexity query = >40 secs High Complexity query = > 80 secs	0

#	Performance Area	Baseline		Lower Performance		Breach	
		Metric	Points	Metric	Points	Metric	Points
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%	4	>= 98 % to <99.5%	2	< 98 %	0
2	IP Phones	99%	3	>= 96 % to <99%	1.5	< 96 %	0
3. **Underlying IT Infrastructure Uptime/Availability at Data Centers**							
1	Application Servers Uptime	99.98%	18	>= 99.5 % to <99.97%	9	< 99.5%	0
2	Storage System Uptime	99.98%	18	>= 99.5 % to <99.97%	9	< 99.5%	0
4. **Security /Patch Services for IT Infrastructure**							
1	Firewall and any other security appliance Uptime	100%	14	99.5 % to 99.99%	7	< 99.5%	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

#	Performance Area	Baseline		Lower Performance		Breach	
		Metric	Points	Metric	Points	Metric	Points
3	Anti-malware, 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 7 days of patch release.	Up-to 1 violations of service parameters	1	2 – 5 violations	0.5	> 5 violations	0
6	Resolution of Issue	<4 Hrs (for Critical issue) <8 Hrs (for Medium issue) <2 days (for Low issue)	4	<8 Hrs and >=4 hrs(for Critical issue) <16 Hrs and >=8 (for Medium issue) <4 days and >=2 (for Low issue)	0.5	>8 Hrs (for Critical issue) >16 Hrs (for Medium issue) >4 days (for Low issue)	0
7	CCTV Cameras	>=99.5% uptime	5	98%=<uptime<99.5%	2.5	Uptime<98%	0
	Total Score		**100**		**50**		**0**

9.3.8 General Instructions related to SLAs mentioned above

(i) Theft cases by default would not be considered as “beyond the control of Bidder”.

(ii) Power shut down would not be considered as “beyond the control of Bidder”.

(iii) Damages due to Road Accident / Mishap shall not be considered as “beyond the control of Bidder”.

(iv) Deliberate damage to field devices: camera, Pole etc. would not be considered as “beyond the control of Bidder”. Bidder is advised to have stronger poles & proper housing to protect from such damages.

9.3.9 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 SI 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 NDMC/End user department and provided passwords • Availability of any report / data to any other user than those authorized by NDMC/End user department, and provided passwords • 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 INR 5,00,000/- or lead to termination of contract

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><b>Definition</b></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 NDMC/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><b>Service Level Requirement</b></td><td>Availability of the required man-power should be 100%. SI to implement the biometric attendance system and share the attendance report of each person proposed as part of team on monthly basis with NDMC.</td></tr>
<tr><td><b>Measurement of Service Level Parameter</b></td><td>Following instances would be considered as SLA non-compliances:<ul><li>Replacement of a profile by the Bidder (only one replacement per profile – with equal or higher qualification and experience – would be permitted per year)</li><li>Non-deployment of the profile for more than 1 month. Authority reserves the right to ask SI to replace (with equal or higher qualification and experience) the profile if the performance / commitment are not up to the mark</li></ul></td></tr>
<tr><td><b>Penalty for non-achievement of SLA Requirement</b></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>Programme Manager</td><td><ul><li>Penalty of Rs 25,000 in 1st week of non-availability</li><li>Penalty of Rs. 50,000 in 2nd week of non-availability and Rs.50,000 each week thereafter.</li></ul></td></tr>
<tr><td>For Technical Experts Clause No.5.3.6.2 (S.No.3 to 14)</td><td><ul><li>Penalty of Rs 2,500 per day of non-availability for 7 days</li><li>Penalty of Rs. 5,000 per day of non-availability after 7 days</li></ul></td></tr>
<tr><td>For all other team members</td><td><ul><li>Penalty of Rs 1,500 per day of non-availability</li></ul></td></tr>
</table></td></tr>
</table>

9.3.10 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

Issue Resolution

Explanation	Issue Resolution SLA shall monitor the time taken to resolve a complaint / query after it has been reported by NDMC/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.

9.3.11 Rate of Penalties prescribed in Clause 9.3.8 and 9.3.9 will increase @10% per annum on compounding basis from the date of signing of the agreement.

9.3.12 Penalties shall not be levied on the SI in the following cases

9.3.12.1 In case of a force majeure event affecting the SLA which is beyond the control of the SI. Force Majeure events shall be considered in line with the Force Majeure clause mentioned in this RFP document.

9.3.12.2 Theft cases by default/ vandalism would not be considered as "beyond the control of SI". Hence, the SI should be taking adequate anti-theft measures, spares strategy, Insurance as required to maintain the desired required SLA.

10 FORCE MAJEURE

10.1 Definition of Force Majeure

The SI or the NDMC, as the case may be, shall be entitled to suspend or excuse performance of its respective obligations under this RFP document to the extent that such performance is impeded by an event of force majeure ('Force Majeure').

10.2 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 may be classified as all or any of the following events:

(i) Act of God, including earthquake, flood, Inundation, landslide, exceptionally adverse weather conditions, storm, tempest, hurricane, cyclone, lightning, thunder, volcanic eruption, fire or other extreme atmospheric conditions;

(ii) Radioactive contamination or ionizing radiation or biological contamination;

(iii) A strike or strikes or other industrial action or blockade or embargo or any other form of civil disturbance(whether lawful or not), in each case affecting on a general basis the industry related to the affected Services and which is not attributable to any unreasonable action or inaction on the part of the SI or any of its Subcontractors or suppliers and the settlement of which is beyond the reasonable control of all such persons;

(iv) general strikes, lockouts, boycotts, labor disruptions or any other industrial disturbances as the case may be not arising on account of the acts or omissions of the SI and which affect the timely implementation and continued operation of the Project;

(v) 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.

For the avoidance of doubt, it is clarified that any negligence in performance of Services which directly causes any breach like hacking, theft, vandalism, etc. aren’t the forces of nature and hence wouldn’t be qualified under the definition of “Force Majeure”. In so far as applicable to the performance of Services, Service Provider 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 there from(wherever applicable).

10.3 Notification procedure for Force Majeure

10.3.1 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 within accordance with the dispute resolution mechanism in accordance with Clause.

10.3.2 Upon cessation of the situation which led the Party claiming Force Majeure, the claiming Party shall within seven(7) days here of notify the other Party in writing of the cessation and the Parties shall as soon as practicable thereafter continue performance of all obligations under this RFP document.

10.4 Allocation of costs arising out of Force Majeure

10.4.1 Upon the occurrence of any Force Majeure Event, the Parties shall bear their respective costs and no Party shall be required to pay to the other Party any costs thereof.

10.4.2 For the avoidance of doubt, Force Majeure Costs may include interest payments on debt, operation and maintenance expenses, any increase in the cost of the Services on account of inflation and all other costs directly attributable to the Force Majeure Event.

10.5 Save and except as expressly provided in this Clause, neither Party shall be liable in any manner what so ever 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.

10.6 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 this RFP document 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 Parties 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.

11 EVENTS OF DEFAULT AND TERMINATION

11.1 Events of Default

Any of the following events shall constitute an event of default unless such event has occurred as a result of one or more reasons set out in clause 11.2;

(i) The SI has failed to adhere to the project execution requirements and the Implementation Schedule and such failure, in the reasonable estimation of the NDMC, is likely to delay achievement of GO-LIVE beyond 30 weeks of the Scheduled GO-LIVE Date, which is one year from the date of signing of Contract Agreement;

(ii) The SI has failed to achieve GO-LIVE within 30 weeks from the Scheduled GO-LIVE Date;

(iii) The SI is in Material Breach of O&M Requirements;

(iv) Any representation made or warranties given by the SI under this RFP document is found to be false or misleading;

(v) The SI has created any Encumbrance on the Project Site in favour of any Person save as otherwise expressly permitted under this RFP document;

(vi) The SI has failed to ensure minimum shareholding requirements specified in clause 5.2;

(vii) A resolution has been passed by the shareholders of the SI for the voluntary winding up of the SI;

(viii) Any petition for winding up of the SI has been admitted and liquidator or provisional liquidator has been appointed or the SI has been ordered to be wound up by Court of competent jurisdiction except for the purpose of amalgamation or reconstruction with the prior consent of NDMC, provided that, as part of such amalgamation or reconstruction, the property, assets and undertaking of the SI are transferred to the amalgamated or reconstructed entity and that the amalgamated or reconstructed entity has unconditionally assumed the obligations of the SI under this RFP document, and provided further that:

a) the amalgamated or reconstructed entity has the technical capability and operating experience necessary for the performance of its obligations under this RFP document;

b) the amalgamated or reconstructed entity has the financial standing to perform its obligations under this RFP document and has a credit worthiness at least as good as that of the SI as at Commencement Date; and

c) RFP document remains in full force and effect.

(ix) The SI has abandoned the Project Facilities.

(x) The SI has repudiated this RFP document or has otherwise expressed an intention not to be bound by this RFP document.

(xi) The SI has suffered an attachment levied on any of the assets located or comprised in the Project Site/Project Facilities, causing a Material Adverse Affect on the Project and such attachment has continued for a period exceeding 90 days.

(xii) The SI has otherwise been in Material Breach of any of its other obligations and terms and conditions under this RFP document.

(xiii) The SI is not able to meet the SLAs minimum requirements at all the times or otherwise.

(xiv) The SI reporting bankruptcy to the NDMC, or any appropriate statutory forum.

(xv) As otherwise provided in this RFP document.

11.2 No Breach of Obligations

The SI shall not be considered to be in breach of its obligations under this RFP document nor shall it incur or suffer any liability if and to the extent performance of any of its obligations under this RFP document is affected by or on account of any of the following:

(i) Force Majeure Event as provided under clause 10;

(ii) Compliance with written instructions of the NDMC or the directions of any Government Agency in writing, other than instructions issued as a consequence of a breach by the SI of any of its obligations hereunder or any applicable law;

11.3 Termination due to Events of Default

11.3.1 Without prejudice to any other right or remedy which the NDMC may have in respect thereof under this RFP document, upon the occurrence of a Event of Default, the NDMC shall be entitled to terminate this Agreement as hereinafter provided.

11.3.2 If NDMC decides to terminate this Agreement pursuant to preceding clause 11.3.1, it shall in the first instance issue Preliminary Notice to the SI. Within 30 days of receipt of the Preliminary Notice, the SI shall submit to NDMC in sufficient detail, the manner in which it proposes to cure the underlying Event of Default (the **"SI's Proposal to Rectify"**). In case of non-submission of the SI's Proposal to Rectify within the said period of 30 days, NDMC shall be entitled to terminate this Agreement by issuing Termination Notice, and to appropriate the Performance Security.

11.3.3 If the SI's Proposal to Rectify is submitted within the period stipulated there for, the SI shall have further period of 30 days to remedy / cure the underlying Event of Default (Cure Period). If, however the SI fails to remedy/cure the underlying Event of Default within such further period allowed, NDMC shall be entitled to terminate this Agreement by issue of Termination Notice and to appropriate the Performance Security if subsisting.

11.4 Termination Notice

If NDMC, having become entitled to do so decides to terminate this Agreement pursuant to the preceding clause 11.3, it shall issue Termination Notice setting out:

(i) in sufficient detail the underlying Event of Default;

(ii) the Termination Date which shall be a date occurring not earlier than 30 days from the date of Termination Notice;

(iii) the estimated Termination Payment including the details of computation thereof and;

(iv) any other relevant information.

11.5 Obligation of Parties

Following issue of Termination Notice by NDMC in accordance with clause 11.4, the Parties (i.e. the SI and the NDMC) shall promptly take all such steps as may be necessary or required to ensure that:

(i) until Termination the Parties shall, to the fullest extent possible, discharge their respective obligations so as to maintain the continuity of service to the users of the Project Facilities,

(ii) the Termination Payment, if any, payable by the SI is paid to the NDMC before the Termination Date; and

(iii) the Project Facilities are handed over to NDMC by the SI on the Termination Date, free from any Encumbrance, under this Agreement.

11.6 Withdrawal of Termination Notice

Notwithstanding anything inconsistent contained in this RFP document, if the SI cures the underlying Event of Default to the satisfaction of the NDMC at any time before the Termination occurs, the Termination Notice may be withdrawn by the NDMC.

Provided that the SI shall compensate the NDMC for any direct costs/ consequences occasioned by the Event of Default which caused the issue of Termination Notice.

11.7 Termination Payments

11.7.1 Upon Termination of this Agreement, the NDMC shall be entitled to receive Termination Payment as under:

(i) Prior to GO-LIVE

If the Agreement is terminated due to Event of Default, NDMC shall forfeit all the Performance Bank Guarantee(s) furnished by the SI, and all the assets and services created under this project will become the property of NDMC. The SI shall pay all fees/ dues, if any, to the NDMC before the date of termination. NDMC may also recover dues, if any, against the SI, and may take any other action as its deem fit.

(ii) After GO-LIVE

If the Agreement is terminated due to Event of Default, NDMC shall forfeit the Performance Bank Guarantee furnished by the SI, and all the assets and services created under this project will become the property of NDMC. The SI shall pay all fees/ dues, if any, to the NDMC before the date of termination. NDMC may also recover due, if any, against the SI, and may take any other action as its deem fit.

11.7.2 The SI shall pay all fees/ dues, if any, to the NDMC before the date of termination.

11.7.3 The SI may terminate the agreement by giving a notice of 60 days to the NDMC. Such termination is subject to the fulfillment of the conditions, as prescribed under clause 11.7.1, 11.7.2 and 11.8, by the SI.

11.8 Rights of NDMC on Termination

Upon Termination of this Agreement for any reason whatsoever, NDMC shall have the power and authority to:

(i) Enter upon the Project Site and take over the Project Facilities without any hindrance.

(ii) prohibit the SI or any Person claiming through or under the SI from entering upon/dealing with the Project Site / Project Facilities;

(iii) step in or nominate any person to step in without the necessity of any further action by the SI, to the interests of the SI under such of the Project Agreements, as NDMC may in its discretion deem appropriate with effect from such date as NDMC may specify:

Provided any sums claimed by counter party to any such Project Agreements as being due and owing for work or services performed or accruing on account of any act, omission or event prior to such date specified by NDMC for step in shall and shall always constitute debt between the SI and such counter party and NDMC shall in no way or manner be liable or responsible for such sums. The SI shall ensure that the Project Agreements contain provisions necessary to give effect to the provisions of this clause 11;

(iv) Notwithstanding anything contained in this Agreement, NDMC shall not, as a consequence of Termination or otherwise, have any obligation whatsoever including but not limited to obligations as to compensation for loss of employment, continuance or regularization of employment, absorption or re-employment on any ground, in relation to any person in the employment of or engaged by the SI in connection with the Project, and the handback of the Project

Site/facilities by the SI to NDMC shall be free from any such obligation.

(v) Notwithstanding anything contained in this Agreement, the right of NDMC to vacant and peaceful possession of the Project Facilities, upon Termination is absolute. If the SI fails to deliver vacant and peaceful possession of the Project Facilities as contemplated in this provision, the SI shall be liable to pay to NDMC and NDMC shall be entitled to recover from the SI, an amount that represents a genuine estimate of the losses, damages and costs suffered by NDMC by way of liquidated damages. The parties agree that the said liquidated damages shall be calculated at the rate applicable for the year when the Contract is Terminated plus the costs incurred by NDMC for recovery of the Project Facilities. Such liquidated damages shall be recoverable from the Termination Date to the date when NDMC receives vacant and peaceful possession of the Project Facilities. Provided, the recovery of liquidated damages shall be without prejudice to the rights and remedies available to NDMC against the SI who shall be deemed to be a trespasser in illegal and unauthorized possession and occupation of the Project Site and Project Facilities, upon Termination.

11.9 Rights of Parties

Notwithstanding anything to the contrary contained in this Agreement, Termination pursuant to any of the provisions of this Agreement shall be without prejudice to accrued rights of either Party including its right to claim and recover money damages and other rights and remedies which it may have in law or Contract Agreement. The rights and obligations of either Party under this Agreement, including without limitation those relating to Termination Payment, shall survive the Termination but only to the extent such survival is necessary for giving effect to such rights and obligations.

11.10 Early Determination

Notwithstanding anything inconsistent contained anywhere in this agreement, in the event of early determination of this Agreement by NDMC without the consent of the SI or in the absence of any default by the SI, the procedure for Termination will be as prescribed under Clause 12 (Dispute Resolution).

12 DISPUTE RESOLUTION

12.1 Any disputes and or difference relating to this agreement or claims arising out of or relating to this agreement or breach, termination or the invalidity thereof or on any issue whether arising during the progress of the services or after the completion or abandonment thereof or any matter directly or indirectly connected with this agreement will be resolved through joint discussion of the authorized representatives of both the parties (NDMC and SI). If the dispute is not resolved by joint discussion, then the matter will be referred for adjudication to a sole Arbitrator appointed by the Chairman, NDMC on receipt of written notice / demand of appointment of Arbitrator from either party.

12.2 The award of the sole Arbitrator shall be final and binding on all the parties. The cost of Arbitration shall be borne by the respective parties equally. Arbitration proceedings will be held at premises of NDMC, New Delhi only.

12.3 Rules governing Arbitration Proceedings: The Arbitration Proceedings shall be governed by Indian Arbitration and Conciliation Act 1996, as amended from time to time including provisions in force at the time the references made. During the pendency of arbitration proceedings and currency of the Contract Agreement, the SI shall continue to perform and make due payments to NDMC as per the Contract Agreement.

13 LIQUIDATED DAMAGES

Time is the essence of the Agreement and the delivery dates are binding on the SI. In the event of delay or any gross negligence, for causes attributable to the SI, in meeting the deliverables, the NDMC shall be entitled at its option to recover from the SI as agreed, liquidated damages, as per the rates mentioned in Clause 9 **“Punitive Clauses**” as mentioned in this RFP document. The Liquidated Damages shall be capped at 10% of the total CAPEX before Go-Live and 25% of the OPEX per year after Go-Live, and in the event of Liquidated Damages exceeding this capping, the NDMC has a right to invoke “Termination Clause”. The activities pursuant to the termination of the Contract Agreement shall be in-line with the conditions of the RFP document.

14 EXIT MANAGEMENT SCHEDULE

14.1 Purpose: This Clause sets out the provisions, which will on expiry or termination of the Contract Agreement.

14.2 Transfer of assets:

14.2.1 The SI shall within fifteen (15) days of the expiry of the Contract Agreement or termination of the Contract Agreement, whichever is earlier, hand over all the assets and services belonging to the NDMC, as per the Assets List made under the provisions of Clause 3.5.28, in proper working condition to the NDMC.

14.2.2 In case of any deficiency noticed at the time of such handing over, the SI has to get it rectified at his own cost within 45 days of such handing over otherwise NDMC will get it rectified at the risk and cost of the SI.

14.2.3 Performance Bank Guarantee of the SI will be released only after successful handing over of the all the assets and services, including hardware, software, network and services in working conditions to NDMC, and after adjustments of any amount due and recoverable from the SI under this Agreement by NDMC, if any.

14.2.4 Upon service of a notice under this Clause the following provisions shall apply:

(a) The SI shall ensure that all liabilities have been cleared beyond doubt, prior to transfer/all fungible/non-fungible assets to NDMC . All documents regarding the discharge of such liabilities shall be furnished to the NDMC.

(b) All title to the Assets and Services to be transferred to the NDMC pursuant to this Clause shall be transferred to NDMC, within the time period as mentioned in clause 14.2.1.

14.2.5 The outgoing SI will pass on to NDMC, the subsisting rights in any licensed products on terms not less favorable to NDMC, than that enjoyed by the outgoing SI.

14.3 Cooperation and Provision of Information

During the Exit Management Period:

(i) the SI will allow the NDMC access to information reasonably required to define the then current mode of operation associated with the provision of the services to enable the NDMC to assess the existing services being delivered;

(ii) promptly on reasonable request by the NDMC, the SI 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 SI). The NDMC shall be entitled to copy of all such information. Such information shall include details pertaining to the services rendered and other performance data. The SI shall permit the NDMC or its nominated agencies to have reasonable access to its employees and facilities as reasonably required by the NDMC to understand the methods of delivery of the services employed by the SI and to assist appropriate knowledge transfer.

15. General Conditions of Contract (GCC)

15.1 Definition of Terms

15.1.1 **“Acceptance of System”:** The system including the hardware, software, solution or any deliverable shall be considered to have been accepted by the procuring entity, 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 SI to the satisfaction of procuring entity and the Purchaser has indicated its acceptance by signing the Acceptance Certificate.

15.1.2 **“Acceptance Certificate”** - means that document issued by the procuring entity signifying Acceptance of a hardware, software, solution, or any other deliverable pursuant to the successful completion of the acceptance test of the System.

15.1.3 **“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 rele**vant 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.

15.1.4 **“Bidder”** shall mean organization/ consortium submitting the proposal in response to this RFP.

15.1.5 **“**Procuring entity**”** means the New Delhi Municipal Council (NDMC). The project shall be executed in NDMC and shall be owned by NDMC.

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

15.1.7 ‘**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 Purchaser which is disclosed to or otherwise learned by SI in the course of or in connection with the Contract but does not include information which is available lawfully in the public domain

15.1.8 "**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 Purchaser, the acceptance of Letter of Award from the SI together with all Annexures, Schedules, referenced documents and all amendments, corrigendum, addendums and changes thereto.

15.1.9 **"Contract Value"** means the amount quoted by the SI in its commercial bid.

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

15.1.11 **"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.

15.1.12 **"Effective Date"** means the date on which this Contract is signed by procuring entity.

15.1.13 **"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 SI is required to supply, install and maintain under the contract.

15.1.14 **"Command and Control Center"** means the integrated/centralized operation center from where any agency control their operations for the entire city.

15.1.15 **"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 Purchaser's Representative.

15.1.16 **“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.

15.1.17 **“Notice”** means: a notice; or a consent, approval or other communication required to be in writing under this Contract.

15.1.18 **“OEM”** means the **Original Equipment Manufacturer of any equipment / system / software / product** which are providing such goods to the Purchaser under the scope of this RFP**.**

15.1.19 “**Project**” or “**Engagement**” means Appointment of Master System Integrator for Integrated Control and Command Centre (ICCC) and Data Centre (DC) for Smart City NDMC.

15.1.20 ‘Procuring entity **Representative / Project Coordinator**’ means the person or the persons appointed by the Purchaser from time to time to act on its behalf for overall coordination, supervision and project management.

15.1.21 “**Scope of Work**” means all Goods and Services, and any other deliverables as required to be provided by the SI under the RFP.

15.1.22 **“SI’s Team”** means SI who along with all of its Consortium Members who have to provide Goods & Services to the Procuring entity 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 SI for the purposes of this Contract.

15.1.23 ‘**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;

15.1.24 ‘**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 SI to meet the design criteria.

15.1.25 ‘**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 Purchaser.

15.1.26 “**Purchase Order**’ means the purchase order(s) issued from time to time by the Procuring entity to the SI to provide Goods and Services as per the terms and conditions of this Contract.

15.1.27 “**Consortium**” means Legal firms (not more than 3 in total)entering into the Contract with the Procuring entity and includes their respective successors and assignees.

15.1.28 “**Replacement Service Provider**” means the organization replacing SI in case of contract termination for any reasons

15.1.29 “**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 Purchaser and the heirs, legal representatives, successors and assignees of such person.

15.1.30 **“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 Purchaser. 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.

15.1.31 ‘**Timelines’** means the project milestones for performance of the Scope of Work and delivery of the Services as described in the RFP;

15.2 Interpretation

15.2.1 In this Contract unless a contrary intention is evident:

(i) the clause headings are for convenient reference only and do not form part of this Contract;

(ii) unless otherwise specified a reference to a clause number is a reference to all of its sub-clauses;

(iii) 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;

(iv) 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;

(v) a word in the singular includes the plural and a word in the plural includes the singular;

(vi) a word importing a gender includes any other gender;

(vii) a reference to a person includes a partnership and a body corporate;

(viii) a reference to legislation includes legislation repealing, replacing or amending that legislation;

(ix) 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.

15.3 Documents forming part of Agreement

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

(i) The Contract;

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

(iii) The Proposal of the SI as accepted by the Purchaser along with any related documentation

(iv) The Procuring Entity 's Letter of Award;

(v) The SI’s Acceptance of Letter of Award, if any;

(vi) The tripartite agreement to be entered into between the ISPs for provision of bandwidth services, if any; and

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

15.4 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.

15.5 The Goods supplied under this Agreement shall conform to the minimum 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 SI in accordance with the Agreement and the terms specified by the Procuring Entity in Purchaser Order. In case if it is found that the Goods provided by SI do not meet one/ more criteria, the SI shall remain liable to provide a replacement for the same which meets all the required specifications and as per choice of Procuring Entity, at no additional cost to Procuring Entity.

15.6 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 NDMC.

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.

NDMC 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 NDMC and within time specified and acceptable to NDMC.

If the successful bidder, having been notified, fails to remedy the defect(s) within the period specified in the contract, NDMC 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 NDMC 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 NDMC.

The successful bidder hereby warrants NDMC 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.

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

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

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

15.7 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 NDMC may call for new bids. In such a case, NDMC shall invoke the PBG and/or forfeit the EMD.

15.8 Reporting Progress

15.8.1 SI shall monitor progress of all the activities related to the execution of the Contract and shall submit to the Procuring Entity, progress reports with reference to all related work, milestones and their progress during the implementation phase.

15.8.2 Formats for all above mentioned reports and their dissemination mechanism shall be discussed and finalized with the Purchaser along with project plan. The Procuring Entity on mutual agreement between both parties may change the formats, periodicity and dissemination mechanism for such reports.

15.8.3 Periodic meetings shall be held between the representatives of the Procuring Entity and SI 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 Procuring Entity, to discuss the performance of the contract.

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

15.8.5 Several review committees involving representative of the Procuring Entity and senior officials of SI shall be formed for the purpose of this project. These committees shall meet at intervals, as decided by the Procuring Entity later, to oversee the progress of the implementation.

15.8.6 All the Goods, Services and manpower to be provided / deployed by SI 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 Procuring Entity's Representative in accordance with the Contract.

15.8.7 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 Procuring Entity's Representative shall so notify SI in writing.

15.8.8 SI 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. SI shall not be entitled to any additional payment for taking such steps. If at any time it should appear to the Procuring Entity or Procuring Entity's Representative that the actual progress of work does not conform to the approved plan SI shall produce at the request of the Procuring Entity'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

15.8.9 The submission seeking approval by the Procuring Entity or Procuring Entity's Representative of such plan shall not relieve SI of any of his duties or responsibilities under the Contract.

15.8.10 In case during execution of works, the progress falls behind schedule or does not meet the Tender requirements, SI 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 Procuring Entity for its review and approval. All time and cost effect in this respect shall be borne, by SI within the Contract Value

15.8.11 The Procuring Entity 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 SI. The Procuring Entity may demand and upon such demand being made, SI shall provide documents, data, material or any other information pertaining to the Project which the Procuring Entity may require, to enable it to assess the progress/ performance of the work / service under the Contract.

15.8.12 At any time during the course of the Contract, the Procuring Entity 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 SI of its obligations/ functions in accordance with the standards committed to or required by the Procuring Entity and SI undertakes to cooperate with and provide to the Procuring Entity/ any other agency appointed by the Procuring Entity, 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 SI failing which the Procuring Entity may, without prejudice to any other rights that it may have issue a notice of default. Cost of acquisition of deliverables by the SI and other Sub-Contractors is out of the purview of audit/inspections.

15.8.13 Without prejudice to the foregoing, the SI shall allow access to the Procuring Entity or its nominated agencies to all information which is in the possession or control of the SI 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 Procuring Entity to comply with the terms of the Audit, Access and Reporting provision set out in this Contract.

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

15.8.15 SI 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 Procuring Entity before commencement of installation of integrated command and control center. The plan shall be drawn mutually at a later stage.

15.8.16 SI shall be deemed to have knowledge of the 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, SI detects physical conditions and/or obstructions affecting the work, SI shall take all measures to overcome them.

15.9 Project Plan

15.9.1 Within 15 calendar days of Effective Date of the contract/ Issuance of LoI/LOA, SI shall submit to the Procuring Entity 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 SI shall conform to the requirements and timelines specified in the Contract. The Procuring Entity and SI shall discuss and agree upon the work procedures to be followed for effective execution of the works, which SI 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 Procuring Entity's Representative of the Project Plan shall not relieve SI of any of his duties or responsibilities under the Contract.

15.9.2 If SI's work plans necessitate a disruption/ shutdown in Procuring Entity'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 SI to develop/adhere such a work plan shall be to his account.

15.10 Warranty

15.10.1 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.

15.10.2 A comprehensive warranty applicable on goods/solutions supplied under the Contract by the respective OEMs and the warranties shall be passed on to the Procuring Entity. The SI shall be responsible for making any and all claims under the warranty on behalf of the Procuring Entity. 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 Procuring Entity. The AMC / ATS shall commence from the date of expiry of the warranty period of the respective goods and solutions.

15.10.3 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.

15.10.4 The SI 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 SI and respective OEM along with service and spares support to ensure its efficient and effective operation for the entire duration of the contract.

15.10.5 The SI 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.

15.10.5 The SI 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 Procuring Entity's Specifications) or from any act or omission of the SI, that may develop under normal use of the supplied Goods in the conditions prevailing at the respective Datacenter / Server Room Sites.

15.10.6 Warranty for Services – The SI 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 SI represents that it shall use adequate numbers of qualified individuals with suitable training, education, experience and skill to perform the Services hereunder.

15.10.7 The Procuring Entity shall promptly notify the SI in writing of any claims arising under this warranty.

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

15.10.9 If the SI, having been notified, fails to remedy the defect(s) within a reasonable period, the Procuring Entity may proceed to take such remedial action as may be necessary, at the SI’s risk and expense and without prejudice to any other rights which the Procuring Entity may have against the SI under the Contract.

15.10.10 Any OEM specific warranty terms that do not conform to conditions under this Contract shall not be acceptable.

15.10.11 Any OEM specific warranty terms that do not conform to conditions under this Contract shall not be acceptable.

15.10.12 The representations, warranties and covenants provided by the SI under the Contract will not be affected by Procuring Entity’s modification of any portion of the software so long as the SI can discharge its obligations despite such modifications, or following their removal by the Procuring Entity.

15.10.13 Notwithstanding anything contained in the Contract, unless the Procuring Entity has otherwise agreed in writing, the Procuring Entity reserves the right to reject Goods which do not conform to the specifications provided in the RFP.

15.11 Change Control Note (CCN)/change requests

15.11.1 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 SI and changes to the terms of payment.

15.11.2 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 (Annex I, Section C 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 Authority.

15.11.3 SI 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.

15.11.4 SI 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:

(i) a description of the change;

(ii) a list of deliverables required for implementing the change;

(iii) a timetable for implementation;

(iv) an estimate of any proposed change; or any relevant acceptance criteria;

(v) an assessment of the value of the proposed change;

(vi) Material evidence to prove that the proposed change is not already covered within the scope of the RFP, Agreement and Service Levels.

15.11.5 Prior to submission of the completed CCN to the Authority or its nominated agencies, SI shall undertake its own internal review of the proposal and obtain all necessary internal approvals. As a part of this internal review process, SI 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.

15.11.6 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 SI meets the obligations as set in the CCN. In the event SI 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 SI. Change requests and CCNs shall be reported monthly to each Party's representative who shall prioritize and review progress.

15.11.7 Cost for CCN

SI 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: oa
description of the change;

(i) a list of deliverables required for implementing the change;
or timetable for implementation;

(ii) an estimate of any proposed change; or
any relevant acceptance criteria;

(iii) an assessment of the value of the proposed change;

(iv) Material evidence to prove that the proposed change is not already covered within the scope of the RFP, Agreement and Service Levels.

Prior to submission of the completed CCN to the NDMC or its nominated agencies, SI shall undertake its own internal review of the proposal and obtain all necessary internal approvals. As a part of this internal review process, SI 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 SI meets the obligations as set in the CCN. In the event SI 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 SI. Change requests and CCNs shall be reported monthly to each Party's representative who shall prioritize and review progress.

Annexure-1

Letter Comprising the Application for Bid Submission

Dated:

To,
Executive Engineer
NDMC
Palika Kendra,
New Delhi

Sub: Application for "Request for Proposal for Selection of System Integrator for NDMC Smarty City Project "Design, Development, built, Implementation, Operation and Maintenance of Command and Control Centre & Data Center, ERP Solution and integration with various Smart City/NDMC Applications".

Dear Sir,

With reference to your RFP document dated ……….., I/we, having examined the RFP Document and understood its contents, hereby submit my proposal for the aforesaid project. The Application is unconditional and unqualified.

2. I/ We acknowledge that the NDMC will be relying on the information provided in the Application and the documents accompanying such Application for Technical and Financial qualification for the aforesaid project, and we certify that all information provided in the Application and in Annexure 1 to 21 is true and correct; nothing has been omitted which renders such information misleading; and all documents accompanying such Application are true copies of their respective originals.

3. This statement is made for the express purpose of selection of preferred applicant for the aforesaid Project.

4. I/ We shall make available to the NDMC any additional information it may find necessary or require to supplement or authenticate the Qualification statement.

5. I/ We acknowledge the right of the NDMC to reject our Application without assigning any reason or otherwise and hereby waive, to the fullest extent permitted by applicable law, our right to challenge the same on any account whatsoever.

6. I/ We certify that in the last three years, we/ any of the Consortium Members or our/their Associates have neither failed to perform on any contract, as evidenced by imposition of a penalty by an arbitral or judicial authority or a judicial pronouncement or arbitration award, nor been expelled from any project or contract by any public authority nor have had any contract terminated by any public authority for breach on our part.

7. I/ We declare that:

(a) I/ We have examined and have no reservations to the RFP document, including any Addendum issued by the Authority;

(b) I/ We do not have any conflict of interest in accordance with Clauses of the RFP document;

(c) I/We have not directly or indirectly or through an agent engaged or indulged in any corrupt practice, fraudulent practice, coercive practice, undesirable practice or restrictive practice, as defined in Clause 7.3 of the RFP document, in respect of any tender or request for proposal issued by or any agreement entered into with the NDMC or any other public sector enterprise or any government, Central or State; and

(d) I/ We hereby certify that we have taken steps to ensure that in conformity with the provisions of the RFP document, no person acting for us or on our behalf has engaged or will engage in any corrupt practice, fraudulent practice, coercive practice, undesirable practice or restrictive practice.

8. I/ We understand that you may cancel the Bidding Process at any time and that you are neither bound to accept any Application that you may receive nor to invite the Applicants to Bid for the Project, without incurring any liability to the Applicants, in accordance with Clauses of the RFP document.

9. I/ We believe that we/ our Consortium/ proposed Consortium satisfy(s) the Net Worth criteria and meet(s) all the requirements as specified in the RFP document and are/ is qualified to submit a Bid.

10. I/ We declare that we/ any Member of the Consortium, or our/ its Associates are not a Member of a/ any other Consortium applying for this RFP process.

11. I/ We certify that in regard to matters other than security and integrity of the country, we/ any Member of the Consortium or any of our/ their Associates have not been convicted by a Court of Law or indicted or adverse orders passed by a regulatory authority which could cast a doubt on our ability to undertake the Project or which relates to a grave offence that outrages the moral sense of the community.

12. I/ We further certify that in regard to matters relating to security and integrity of the country, we/ any Member of the Consortium or any of our/ their Associates have not been charge-sheeted by any agency of the Government or convicted by a Court of Law.

13. I/ We further certify that no investigation by a regulatory authority is pending either against us/ any Member of the Consortium or against our/ their Associates or against our CEO or any of our directors/ managers/ employees.

14. [I/ We further certify that we are qualified to submit a Bid in accordance with the guidelines for qualification of Applicants seeking to acquire stakes in Public Sector Enterprises through the process of disinvestment issued by the GOI vide Department of Disinvestment OM No. 6/4/2001-DD-II dated 13th July, 2001 which guidelines apply *mutatis mutandis* to the Bidding Process.

15. I/ We undertake that in case due to any change in facts or circumstances during the Bidding Process, we are attracted by the provisions of disqualification in terms of the provisions of this RFP document, we shall intimate the NDMC of the same immediately.

16. The Statement of Legal Capacity as per format provided at Annexure-8 of the RFP document, and duly signed, is enclosed. The power of attorney for signing of application and the power of attorney for Lead Member of consortium, as per format provided at Annexure-7 and Annexure-3 respectively of the RFP, are also enclosed.

17. I/ We understand that the selected Applicant shall either be an existing Company incorporated under the Indian Companies Act, 1956, or shall incorporate as such prior to execution of the Contract Agreement.

18. I/ We hereby irrevocably waive any right or remedy which we may have at any stage at law or howsoever otherwise arising to challenge or question any decision taken by the Authority in connection with the selection of Applicants, selection of the Applicant, or in connection with the selection/ Bidding Process itself, in respect of the above mentioned Project and the terms and implementation thereof.

19. I/ We agree and undertake to abide by all the terms and conditions of the RFP document.

20. I/ We certify that in terms of the RFP document, my/our Net worth is Rs.……………….. (Rupees in words) and the Aggregate Experience Score is ………………….. (number in words).

21. We agree and undertake to be jointly and severally liable for all the obligations of the SI under the Contract Agreement till occurrence of Financial Close in accordance with the Contract Agreement.

In witness thereof, I/ we submit this application under and in accordance with the terms of the RFP document.

Yours faithfully,

Date: (Signature, name and designation of the Authorised Signatory)

Place: Name and seal of the Applicant/ Lead Member

Details of Applicant

1. (a) Name:

(b) Country of incorporation:

(c) Address of the corporate headquarters and its branch office(s), if any, in India:

(d) Date of incorporation and/ or commencement of business:

1. Brief description of the Company including details of its main lines of business and proposed role and responsibilities in this Project:

3. Details of individual(s) who will serve as the point of contact/ communication for the Authority:

(a) Name:

(b) Designation:

(c) Company:

(d) Address:

(e) Telephone Number:

(f) E-Mail Address:

(g) Fax Number:

4. Particulars of the Authorised Signatory of the Applicant:

(a) Name:

(b) Designation:

(c) Address:

(d) Phone Number:

(e) Fax Number:

5. In case of a Consortium:

(a) The information above (1-4) should be provided for all the Members of the Consortium.

(b) A copy of the Jt. Bidding Agreement, as envisaged in Clause __ should be attached to the Application.

(c) Information regarding the role of each Member should be provided as per table below:

Sl. No.	**Name of Member**	**Role and responsibilities**	**Percentage of holding in Consortium**

* The role of each Member, as may be determined by the Applicant, should be indicated in accordance with instructions of RFP document.

(d) The following information shall also be provided for each Member of the Consortium:

Name of Applicant/ member of Consortium:

No.	**Criteria**	**Yes**	**No.**
1	Has the Applicant/ constituent of the Consortium been barred by the [Central/ State] Government, or any entity controlled by it, from participating in any project (BOT or otherwise)?		
2	If the answer to 1 is yes, does the bar subsist as on the date of Application?		
3	Has the Applicant/ constituent of the Consortium paid liquidated damages of more than 5% (five per cent) of the contract value in a contract due to delay or has been penalised due to any other reason in relation to execution of a contract, in the last three years?		

6. A statement by the Applicant and each of the Members of its Consortium (where applicable) or any of their Associates disclosing material non-performance or contractual non-compliance in past projects, contractual disputes and litigation/ arbitration in the recent past is given below (Attach extra sheets, if necessary):

Technical Capacity of the Applicant@

Applicant type*	**Member Code***	**Project Code****	**Category***	**Experience of Projects as per Clause 5.3.2 S.N.2 (a) to (d)**	**Experience score***
(1)	(2)	(3)	(4)	(5)	(8)
Single Entity Applicant		A			
		B			
		C			
		D			
Consortium		1a			

		1b			
		1c			
		1d			
Consortium Member 2		2a			
		2b			
		2c			
		2d			
Consortium Member 3		3a			
		3b			
		3c			
		3d			
				Aggregate Experience Score	

@ *Provide details of only those projects that have been undertaken by the Applicant under its own name.*

# *An Applicant consisting of a single entity should fill in details as per the row titled Single entity Applicant and ignore the rows titled Consortium Member. In case of a Consortium, the row titled Single entity Applicant may be ignored.*

* *Member Code shall indicate NA for Not Applicable in case of a single entity Applicant. For other Members, the following abbreviations are suggested viz. LM means Lead Member, OM means Other Member.*

Add more rows if necessary.

Financial Capacity of the Applicant

(*Refer to Clauses 5.2.3 and 5.3.2 of the RFP*)

(In Rs. crore)

Applicant Member (1)	**Member Code£ (2)**	**Turnover**					**Net Worth•**
		Year 16-17 (3)	**Year 15-16 (4)**	**Year14-15 (5)**			**Year 15-16 (8)**
Single entity Applicant							
Consortium Member 1							
Consortium Member 2							

Consortium Member 3							

Name & address of Applicant's Bankers:

- An Applicant consisting of a single entity should fill in details as per the row titled Single entity Applicant and ignore the rows titled Consortium Members. In case of a Consortium, row titled Single entity Applicant may be ignored.
- For Member Code, see instructions at of this Annexure-3.
- The Applicant should provide details of its own Financial Capacity.

Instructions:

1. The Applicant/ its constituent Consortium Members shall attach copies of the balance sheets, financial statements and Annual Reports for 3 (three) years preceding the Application Due Date. The financial statements shall:

   (a) reflect the financial situation of the Applicant or Consortium Members and its/their Associates where the Applicant is relying on its Associate's financials;

   (b) be audited by a statutory auditor;

   (c) be complete, including all notes to the financial statements; and

   (d) correspond to accounting periods already completed and audited (no statements for partial periods shall be requested or accepted).

2. Net Cash Accruals shall mean Profit After Tax + Depreciation.

3. Net Worth shall mean (Subscribed and Paid-up Equity + Reserves) less (Revaluation reserves + miscellaneous expenditure not written off + reserves not available for distribution to equity shareholders).

5. In the case of a Consortium, a copy of the Jt. Bidding Agreement shall be submitted in accordance with Clause 5.2.3 of the RFP document.

6. The applicant shall also provide the name and address of the Bankers to the Applicant.

7. The Applicant shall provide an Auditor’s Certificate specifying the net worth of the Applicant and also specifying the methodology adopted for calculating such net worth in accordance with the RFP document.

Details of Eligible Projects

(*Refer to Clauses 5.3.2 of the RFP document*)

Project Code: **Member Code:**

Item **(1)**	**Refer Instruction** **(2)**	**Particulars of the Project** **(3)**
Title & nature of the project		
Category	5	
Year-wise (a) payments received/made for construction, (b) payments made for development of PPP projects and /or (c) revenues appropriated	6	
Location	7	
Project Cost	8	
Date of commencement of project/contract	9	
Equity shareholding(with period during which equity was held	10	
Whether credit is being taken for the Eligible Experience of an Associate (Yes/No)	11	

Instructions:

1. Applicants are expected to provide information in respect of each Eligible Projects in this Annex. The projects cited must comply with the eligibility& technical criteria specified in Clause 5.2.3 and 5.3.2 of the RFP document, as the case may be. Information provided in this section is intended to serve as a backup for information provided in the Application. Applicants should also refer to the Instructions below.

2. For a single entity Applicant, the Project Codes would be a, b, c, d etc. In case the Applicant is a Consortium then for Member 1, the Project Codes would be 1a, 1b, 1c, 1d etc., for Member 2 the Project Codes shall be 2a, 2b, 2c, 2d etc., and so on.

3. A separate sheet should be filled for each Eligible Project.

4. Member Code shall indicate NA for Not Applicable in case of a single entity Applicant. For other Members, the following abbreviations are suggested viz. LM means Lead Member, and OM means Other Member.

5. Refer to Clause 5.3.2 of the RFP for category number.

6. The total payments received/ made and/or revenues appropriated for each Eligible Project are to be stated in Annex-II of this Appendix-I. The figures to be provided here should indicate the break-up for the past 5 (five) financial years. Year 1 refers to the financial year immediately preceding the Application Due Date; Year 2 refers

to the year before Year 1, Year 3 refers to the year before Year 2, and so on (Refer Clause 2.2.12). For Categories 1 and 2, expenditure on development of the project and/or revenues appropriated, as the case may be, should be provided, but only in respect of projects having an estimated capital cost exceeding the amount specified in Clause 3.2.3 (c). In case of Categories 3 and 4, payments made/ received only in respect of construction should be provided, but only if the amount paid/received exceeds the minimum specified in Clause 3.2.4. Payment for construction works should only include capital expenditure, and should not include expenditure on repairs and maintenance.

7. In case of projects in Categories 1 and 2, particulars such as name, address and contact details of owner/ Authority/ Agency (i.e. contract grantor, counter party to PPA, etc.) may be provided. In case of projects in Categories 3 and 4, similar particulars of the client need to be provided.

8. Provide the estimated capital cost of Eligible Project. Refer to Clauses 3.2.3 and 3.2.4

9. For Categories 1 and 2, the date of commissioning of the project, upon completion, should be indicated. In case of Categories 3 and 4, date of completion of construction should be indicated. In the case of projects under construction, the likely date of completion or commissioning, as the case may be, shall be indicated.

10. For Categories 1 and 2, the equity shareholding of the Applicant, in the company owning the Eligible Project, held continuously during the period for which Eligible Experience is claimed, needs to be given (Refer Clause 3.2.3).

11. Experience for any activity relating to an Eligible Project shall not be claimed by two or more Members of the Consortium. In other words, no double counting by a consortium in respect of the same experience shall be permitted in any manner whatsoever.

12. Certificate from the Applicant's statutory auditor$ or its respective clients must be furnished as per formats below for each Eligible Project. In jurisdictions that do not have statutory auditors, the auditors who audit the annual accounts of the Applicant/ Member/Associate may provide the requisite certification.

13. If the Applicant is claiming experience under Categories 1 & 2, it should provide a certificate from its statutory auditor in the format below:

Annexure- 2

PRE-CONTRACT INTEGRITY PACT

General

This pre–bid pre–contact Agreement (hereinafter called the Integrity Pact) is made on _____________ day of the month of _____________20…….., between on one hand the New Delhi Municipal Council acting through Shri ________________ , The Executive Engineer (hereinafter called the "Principal/Owner", which expression shall mean and include, unless the context otherwise requires, his successors in office and assigns) of the First Part and M/s __________________ represented by Shri _______________ (hereinafter called the "Applicant(s)/Contractor(s) which expression shall mean and include, unless the context otherwise requires, his successors and permitted assigns) of the Second Part.

Whereas the Principal/Owner proposes to procure (Name of work the Store/Equipment/Item) through the Applicant(s)/Contractor(s) and the Applicant(s)/Contractor(s) is willing to offer / has offered the same.

Whereas the Applicant(s)/Contractor(s) is a private company/public company/ Government undertaking/ partnership/ registered export agency, constituted in accordance with the relevant law in the matter and the Principal/Owner is the municipal government of New Delhi established as per NDMC act 1994 performing its functions on behalf of the Council.

Now, therefore,

To avoid all forms of corruption by following a system that is fair, transparent and free from any influence/prejudiced dealings prior to, during and subsequent to the currency of the contract to be entered into with a view to:

Enabling the Principal/Owner to procure the desired said work/ Services/ Stores / Equipments at a competitive price in conformity with the defined specifications by avoiding the high cost and the distortionary impact of corruption during bidding, execution & public procurement,

And

Enabling Applicant(s)/Contractor(s) to abstain from bribing or indulging in any corrupt practice in order to secure the contract by providing assurance to them that their competitors will also abstain from bribing and other corrupt practices and the Principal/Owner will commit to prevent corruption, in any form, by its officials by following transparent procedures.

The parties here to hereby agree to enter into this Integrity Pact and agree as follows:

Commitments of the Principal/Owner

1.1 The Principal/Owner undertakes that no official of the Principal/Owner, connected directly or indirectly with the contract, will demand, take a promise for or accept, directly or through intermediaries, any bribe, consideration, gift, reward, favour or any material or immaterial benefit or any other advantage from the Applicant(s)/Contractor(s), either for themselves or for any person, organization or third party related to the contract in exchange for an advantage in the bidding process, bid evaluation, contracting or implementation process related to the contract.

1.2 The Principal/Owner will, during the pre-contract stage, treat all Applicant(s)/Contractor(s) alike, and will provide to all Applicant(s)/Contractor(s) the same information and will not provide and such information to any particular Applicant(s)/Contractor(s) which could afford an advantage to that particular Applicant(s)/Contractor(s) in comparison to other Applicant(s)/Contractor(s).

1.3 All the officials of the Principal/Owner will report to the CVO, NDMC any attempted or completed breaches of the above commitments as well as any substantial suspicion of such a breach.

2. In case any such preceding misconduct on the part of such official(s) is reported by the Applicant(s)/Contractor(s) to the CVO, NDMC with full and verifiable facts and the same is prima facie found to be correct by the NDMC, necessary disciplinary proceedings, or any other action as deemed fit, including criminal proceedings may be initiated by the NDMC and such a person shall be debarred from further dealings related to the contract process. In such a case while an enquiry is being conducted by the NDMC the proceedings under the contract would not be stalled.

Commitments of Applicant(s)/Contractor(s)

3. The Applicant(s)/Contractor(s) commits itself to take all measures necessary to prevent corrupt practices, unfair means and illegal activities during any stage of its bid or during any pre-contract or post-contract stage in order to secure the contract or in furtherance to secure it and in particular commit itself to the following:

3.1 The Applicant(s)/Contractor(s) will not offer, directly or through intermediaries, any bribe, gift, consideration, reward, favour, any material or immaterial benefit or other advantage, commission, fees, brokerage or inducement to any official of the Principal/Owner, connected directly or indirectly with the bidding process, or to any person, organization or third part related to the contract in exchange for any advantage in the bidding, evaluation, contracting and implementation of the contract.

3.2 The Applicant(s)/Contractor(s) further undertakes that it has not given, offered or promised to give, directly or indirectly any bribe, gift, consideration, reward, favour, any material or immaterial benefit or other advantage, commission, fees brokerage or inducement to any official of the Principal/Owner or otherwise in executing the contract or forbearing to do or having done any act in relation to the obtaining or execution of the contract or any other contract with the New Delhi Municipal Council for showing or forbearing to show favour or disfavor to any person in relation to the contract or any other contract with the New Delhi Municipal Council.

3.3 Applicant(s)/Contractor(s) shall disclose the name and address of agents/Brokers/ representatives/ Intermediaries and Indian Applicant(s)/Contractor(s) shall disclose their foreign Principals or associates at the time of bidding.

3.4 Applicant(s)/Contractor(s) shall disclose the payments to be made by them to such agents/brokers/representatives/ intermediaries, in connection with this bid/contract at the time of bidding.

3.5 **Deleted.**

3.6 The Applicant(s)/Contractor(s), either while presenting the bid or during pre-contract negotiations or before signing the contract, shall disclose any payments he has made, is committed to or intends to make to agents, brokers or any other intermediaries in Connection with the contract and the details of services agreed upon for such payments. A copy of contract so made with agents /brokers/intermediaries shall be submitted.

3.7 The Applicant(s)/Contractor(s) will not collude with other parties interested in the contract to impair the transparency, fairness and progress of the bidding process, bid evaluation, contracting and implementation of the contract. Applicant shall remain responsible to maintain safety & confidentiality of his bid documents during bid process.

3.8 The Applicant(s)/Contractor(s) will not accept any advantage in exchange for any corrupt practice, unfair means, and illegal activities.

3.9 The Applicant(s)/Contractor(s) shall not use improperly, for purposed of competition or personal gain, or pass on to others, any information provided by the Principal/Owner as part business relationship regarding plans, technical proposals and business details, including information contained in any electronic data carrier. The Applicant(s)/Contractor(s) also undertakes to exercise due and adequate care lest any such information is divulged.

3.10 The Applicant(s)/Contractor(s) commits to refrain from giving any complaint directly or through any other manner without supporting it with full and verifiable facts, either to principal/owner or to IEMs so appointed by NDMC.

3.11 The Applicant(s)/Contractor(s) shall not instigate or cause to instigate any third person to commit any of the actions mentioned above.

3.12 If the Applicant(s)/Contractor(s) or any employee of the Applicant(s)/Contractor(s) or any person acting on behalf of the Applicant(s)/Contractor(s), either directly or indirectly, is a relative of any of the officers of the Principal/Owner, or alternatively, if any relative of an officer of the Principal/Owner has financial interest/ stake in the Applicant(s)/Contractor(s) firm, the same shall be disclosed by the Applicant(s)/Contractor(s) at the time of filing of bid. The term 'relative' for this purpose would be as defined in Section 6 of the Companies Act 1956.

3.13 The Applicant(s)/Contractor(s) shall not lend to or borrow any money form or enter into any monetary dealings or transaction, directly or indirectly, with any employee of the Principal/Owner.

3.14 Deleted

3.15 NDMC has adopted integrity pact for all its contract for 50 lacs and above. It is mandatory for the Applicants/contractors to sign the I.P. The bid of Applicant/contractor to do not sign the I.P. shall not be considered details of IEMs (Independent External Monitor is as under:-

1. Shri V. K. Gupta, IEM, Email: vinod91951@gmail.com

2.

In case of any grievances about the bid the same may be sent to IEM/Vigilance of NDMC with the name address of the sender.

4. <u>Previous Transgression</u>

4.1 The Applicant(s)/Contractor(s) declares that no previous transgression occurred in the last Five years immediately before signing of this Integrity Pact, with any other company in any country in respect of any corrupt practices envisaged here under or with any Public Sector Enterprise in India or New Delhi Municipal Council that could justify Applicant(s)/Contractor(s) exclusion from the bidding process.

4.2 The Applicant(s)/Contractor(s) agrees that if it makes incorrect statement on this subject, Applicant(s)/Contractor(s) can be disqualified from the bidding process or the contract, if already awarded, can be terminated for such reason.

5. Deleted.

6. Sanctions for Violations

6.1 Any breach of the aforesaid provisions by the Applicant(s)/Contractor(s) or any one employed by it or acting on its behalf (whether with or without the knowledge of the Applicant(s)/Contractor(s) shall entitle the Principal/Owner to take all or any one of the following actions, wherever required:-

(i) To immediately call off the pre contract negotiations without assigning any reason or giving any compensation to the Applicant(s)/Contractor(s). However, the proceedings with the other Applicant(s)/Contractor(s) would continue.

(ii) The Earnest Money Deposit (in pre-contract stage) and/or Security Deposit/Performance Bond / Guarantee (after the contract is signed) shall stand forfeited and the Principal/Owner shall not be required to assign any reason therefore.

(iii) To immediately cancel the contract, if already signed, without giving any compensation to the Applicant(s)/Contractor(s).

(iv) To recover all sums already paid by the Principal/Owner, and in case of an Indian Applicant(s)/Contractor(s) with interest thereon at 2% higher than the prevailing Prime Lending Rate of State Bank of India, while in case of a Applicant(s)/Contractor(s) form a country other than India with interest theron at 2% higher than the LIBOR. If any outstanding payment is due to the Applicant(s)/Contractor(s) form the Principal/Owner in connection with any other contract for any other stores, such outstanding payment could also be utilized to recover the aforesaid sum and interest.

(v) To encash the advance bank guarantee and performance bond/warranty bond, if furnished by the Applicant(s)/Contractor(s), in order to recover the payments, already made by the Principal/Owner, along with interest.

(vi) To cancel all or any other contracts with the Applicant(s)/Contractor(s). The Applicant(s)/Contractor(s) shall be liable to pay compensation for any loss or damage to the Principal/Owner resulting from such cancellation/ rescission and the

Principal/Owner shall be entitled to deduct the amount so payable form the money(s) due to the Applicant(s)/Contractor(s).

(vii) To debar the Applicant(s)/Contractor(s) from participation in future bidding processes of the New Delhi Municipal Council for a period ranging from six months to maximum five years. However if the Applicant takes corrective measures against transgressions, subject to satisfaction of Principal/Owner & IEMs, the period of debar can be reviewed.

(viii) To recover all sums paid in violation of this Pact by Applicant(s)/Contractor(s) to any middleman or agent or broker with a view to securing the contract.

(ix) In case where irrevocable Letter of Credit have been received in respect of any contract signed by the Principal/Owner with the Applicant(s)/Contractor(s), the same shall not be opened.

(x) Forfeiture of Performance Bond/Guarantee in case of a decision by the Principal/Owner to forfeit the same without assigning any reason for imposing sanction for violation of this Pact.

6.2 The Principal/Owner will be entitled to take all or any of the actions mentioned at para 6.1 (i) to (x) of this Pact also on the Commission by the Applicant(s)/Contractor(s) or any one employed by it or acting on its behalf (whether with or without the knowledge of the Applicant(s)/Contractor(s), of an offence as defined in Chapter IX of the Indian Penal code, 1860 or Prevention of Corruption Act, 1988 or any other statute enacted for prevention of corruption.

6.3 The decision of the Principal/Owner to the effect that a breach of the provisions of this Pact has been committed by the Applicant(s)/Contractor(s) shall be final and conclusive on the Applicant(s)/Contractor(s). However, the Applicant(s)/Contractor(s) can approach the Independent Monitor(s) appointed for the purposes of this Pact. IEMs shall examine the transgression and its severity and submit the report to Chairman, NDMC for further action after providing an opportunity and hearing to the affected parties.

7. Fall Clause : Deleted

8. Independent External Monitors

8.1 The Principal/Owner has appointed Independent External Monitors (hereinafter referred to as IEMs) for this Pact in consultation with the Central Vigilance Commission whose names and email IDs have been given in the NIT.

8.2 The task of the IEMs shall be to review independently and objectively, whether and to what extent the parties comply with the obligations under this pact.

8.3 The IEMs shall not be subject to instructions by the representatives of the parties and perform their functions neutrally and independently.

8.4 Both the parities accept that the IEMs have the right to access all the documents relating to the project/procurement, including minutes of meetings

8.5 As soon as the IEMs notices, or have reasons to believe a violation of this Pact, they shall so inform to Chairman, NDMC.

8.6 The Applicant(s)/ Contractor(s) accepts that the IEMs have the right to access without restriction to all Project documentation of the Principal/Owner including that provided by the Applicant(s)/Contractor(s). The Applicant(s)/Contractor(s) will also grant the IEMs, upon his request and demonstration of a valid interest, unrestricted and unconditional access to his project documentation. The same is applicable to subcontractors. The IEMs shall be under contractual obligation to treat the information and documents of the Applicant(s)/ Contractor(s)/ Subcontractor(s) confidentiality.

8.7 The Principal/Owner will provide to the IEMs sufficient information about all meetings among the parties related to the Project provided such meeting could have an impact on the contractual relations between the parties. The parties will offer to the IEMs the option to participate in such meetings.

8.8 The IEMs will submit a written report to the Chairman, NDMC within 8 to 10 weeks from the date of reference or intimation to him by the Principal/Owner/Applicant(s)/Contractor(s) and, should the occasion arise, submit proposals for correcting problematic situation. However an opportunity of hearing shall be provided by the IEMs to the buyers /Applicants before submitting their written report.

9. **Facilitation of Investigation**

In case of any allegation of violation of any provisions of this pact or payment of commission, the Principal/Owner or its agencies shall be entitled to examine all the documents including the Books of Accounts of the Applicant(s)/Contractor(s) and the Applicant(s)/Contractor(s) shall provide necessary information and documents in English and shall extend all possible help for the purpose of such examination.

10. **Law and Place of Jurisdiction**

This pact is subject to Indian Law. The place of performance and jurisdiction is the seat of the Principal/Owner.

11. **Other Legal Actions**

The action stipulated in this Integrity Pact are without prejudice to any other legal action that may follow in accordance with the provisions of the extant law in force relating to any civil or criminal proceedings and Jurisdiction in case of dispute between the parties if any shall be new Deficiency.

12. **Validity**

12. 1 The validity of this Integrity Pact shall be from date of its signing and extend upto 12 months beyond the defects liability period of the contracts. In case Applicant(s)/Contractor(s) is unsuccessful, this Integrity Pact shall expire after six months from the date of the signing of the contract by the successful Applicant.

12.2 Should one or several provision of this Pact turn out to be invalid, the remainder of this Pact shall remain valid. In this case, the parties will strive to come to an agreement to their original intention.

13 The parties hereby sign this Integrity Pact at ______________ on __________

Principal/Owner
Applicant(s)/Contractor(s) Name of the Officer,
Chief Executive Officer Designation

New Delhi Municipal Council

Witness Witness

1. ____________________________ 1. ___________________________

2. ____________________________ 2. ___________________________

* Provisions of these clauses would need to be amended / deleted in line with the policy of The Principal/Owner in regard to involvement of Indian agents of foreign suppliers.

Annexure-3

Power of Attorney for Lead Member of Consortium

Whereas the NDMC has invited applications from interested parties for the "**Request for Proposal for Selection of System Integrator for NDMC Smarty City Project ""Design, Development, built, Implementation, Operation and Maintenance of Command and Control Centre & Data Center, ERP Solution and integration with various Smart City/NDMC Applications".**

Whereas, ……………………., ……………………., …………………….. and …………………….. (collectively the "Consortium") being Members of the Consortium are interested in bidding for the Project in accordance with the terms and conditions of the Request for Proposal (RFP document) and other connected documents in respect of the Project, and

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 bid for the Project and its execution.

NOW, THEREFORE, KNOW ALL MEN BY THESE PRESENTS

We, …………………….. having our registered office at ……………………................,

M/s. …………………….. having our registered office at ……………………................,

M/s. ……………………having our registered office at ……………………........, and

M/s. …………………….. having our registered office at …………………., (hereinafter collectively referred to as the "Principals") do hereby irrevocably designate, nominate, constitute, appoint and authorise M/s. …………………….. having its registered office at ……………………., being one of the Members of the Consortium, as the Lead Member and true and lawful attorney

of the Consortium (hereinafter referred to as the "Attorney"). We hereby irrevocably authorise the Attorney (with power to sub-delegate) to conduct all business for and on behalf of the Consortium and any one of us during the bidding process and, in the event the Consortium is awarded the contract, during the execution of the Project and in this regard, to do on our behalf and on behalf of the Consortium, all or any of such acts, deeds or things as are necessary or required or incidental to the pre-qualification of the Consortium and submission of its bid for the Project, including but not limited to signing and submission of all applications, bids and other documents and writings, participate in Applicants and other conferences, respond to queries, submit information/ documents, sign and execute contracts and undertakings consequent to acceptance of the bid of the Consortium and generally to represent the Consortium in all its dealings with the NDMC, and/ or any other Government Agency or any person, in all matters in connection with or relating to or arising out of the Consortium's bid for the Project and/ or upon award thereof till the Contract Agreement is entered into with the NDMC.

AND hereby agree to ratify and confirm and do hereby ratify and confirm all acts, deeds and things done or caused to be done by our said Attorney pursuant to and in exercise of the powers conferred by this Power of Attorney and that all acts, deeds and things done by our said Attorney in exercise of the powers hereby conferred shall and shall always be deemed to have been done by us/ Consortium.

IN WITNESS WHEREOF WE THE PRINCIPALS ABOVE NAMED HAVE EXECUTED THIS POWER OF ATTORNEY ON THIS …………………......... DAY OF ………, 20....…

For ……………………..
(Signature)

……………………..
(Name & Title)

For ……………………..
(Signature)

……………………..
(Name & Title)

For ……………………..
(Signature)

……………………..
(Name & Title)

Witnesses:

1.

2.

………………………………………

(Executants)
(To be executed by all the Members of the Consortium)

Notes:

- *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*.

- *Also, wherever required, the Applicant should submit for verification the extract of the charter documents and documents such as a board or shareholders' resolution/power of attorney in favour of the person executing this Power of Attorney for the delegation of power hereunder on behalf of the Applicant.*

- *For a Power of Attorney executed and issued overseas, the document will also have to be legalised by the Indian Embassy and notarised in the jurisdiction where the Power of Attorney is being issued. However, the Power of Attorney provided by Applicants from countries that have signed the Hague Legislation Convention, 1961 are not required to be legalised by the Indian Embassy if it carries a conforming Appostille certificate.*

Annexure-4

Joint Bidding Agreement

(To be executed on Stamp paper of appropriate value)

THIS JOINT BIDDING AGREEMENT is entered into on this the ………… day of ………, 20....…

AMONGST

1. {………… Limited, a company incorporated under the Companies Act, 1956} and having its registered office at ………… (hereinafter referred to as the "**First Part**" which expression shall, unless repugnant to the context include its successors and permitted assigns)

AND

2. {………… Limited, a company incorporated under the Companies Act, 1956} and having its registered office at ………… (hereinafter referred to as the "**Second Part**" which expression shall, unless repugnant to the context include its successors and permitted assigns)

AND

3. {………… Limited, a company incorporated under the Companies Act, 1956 and having its registered office at ………… (hereinafter referred to as the "**Third Part**" which expression shall, unless repugnant to the context include its successors and permitted assigns)}

The number of Parties will be shown here, as applicable, subject however to a maximum of 4 (four).

WHEREAS

(A) New Delhi Municipal Council (NDMC), represented by its Chairman and having its principal offices at Palika Kendra, Sansad Marg, New Delhi (hereinafter referred to as the "**NDMC**" which expression shall, unless repugnant to the context or meaning thereof, include its administrators, successors and assigns) has invited applications (the **Applications**") by its Request for Proposal No. ………… dated …………(the "**RFP**") **for Selection of System Integrator for NDMC Smarty City Project "Design, Development, built, Implementation, Operation and Maintenance of Command and Control Centre & Data Center, ERP Solution and integration with various Smart City/NDMC Applications".**

(B) The Parties are interested in jointly bidding for the Project as members of a Consortium and in accordance with the terms and conditions of the RFP document and other bid documents in respect of the Project, and

(C) It is a necessary condition under the RFP document that the members of the Consortium shall enter into a Joint Bidding Agreement and furnish a copy thereof with the Application.

NOW IT IS HEREBY AGREED as follows:

1. Definitions and Interpretations

In this Agreement, the capitalised terms shall, unless the context otherwise requires, have the meaning prescribed thereto under the RFP.

2. Consortium

2.1 The Parties do hereby irrevocably constitute a consortium (the "**Consortium**") for the purposes of jointly participating in the Bidding Process for the Project.

2.2 The Parties hereby undertake to participate in the Bidding Process only through this Consortium and not individually and/ or through any other consortium constituted for this Project, either directly or indirectly or through any of their Associates.

3. Covenants

The Parties hereby undertake that in the event the Consortium is declared the selected Applicant and awarded the Project, it shall for entering into a Contract Agreement with the NDMC and for performing all its obligations as the SI in terms of the Contract Agreement for the Project.

4. Role of the Parties

The Parties hereby undertake to perform the roles and responsibilities as described below:

(a) Party of the First Part shall be the Lead member of the Consortium and shall have the power of attorney from all Parties for conducting all business for and on behalf of the Consortium from the Bidding Process, upto the end of contract period.

(b) Party of the Second Part shall be the Member of the Consortium

(c) Party of the Third Part shall be the Member of the Consortium; and

5. Joint and Several Liability

The Parties do hereby undertake to be jointly and severally responsible for all obligations and liabilities relating to the Project and in accordance with the terms of the RFP, RFP and the Contract Agreement, till such time as the Financial Closer for the Project is achieved under and in accordance with the Contract Agreement.

6. **Shareholding in the consortium**

6.1 The Parties agree that the proportion of shareholding among the Parties in the consortium shall be as follows:

First Party:

Second Party:

{Third Party:}

6.2 The Parties undertake that the Lead member shall have more than 50% of the holding in the consortium and cannot assign or delegate its rights, duties or obligation under the Agreement throughout the contract period.

6.3 The Parties undertake that each of the members, whose experience will be evaluated for the purposes of this RFP document, shall, for a period of 2 (two) years from the date of commercial operation of the Project, have 26% or more holding in consortium as at the time of submission of bid and may only be replaced by such other party having same or better technical capabilities as well as eligibility conditions with prior approval of the NDMC.

6.4 The Parties undertake that the Lead Member will remain responsible for successful delivery of the project at all times throughout the contract period.

6.5 The Parties undertake that each of the members of the Consortium shall have an independent, definite and separate scope of work which was allocated as per each member's field of expertise

6.6 The Parties undertake the members of the consortium will commit to the profit and loss sharing ratio of each member

6.7 The Parties undertake the members of the consortium will commit to the scope of work, rights, obligations and liabilities to be held by each member; specifically commit that the Lead Member shall be answerable on behalf of other members for the performance of obligations and duties under this Agreement

6.8 The Parties undertake that the technical and commercial capacity and Net Worth of the Members shall satisfy the conditions of eligibility as prescribed in this RFP

6.9 The Parties undertake that any change to the composition of the consortium can be done only with the prior approval of the NDMC. The Lead Member will be responsible for the scope of work to be delivered by the exiting member, whether he does it himself or through a new member of the consortium. In case of a new member, the Lead Member will take the prior approval of the NDMC, before on boarding the member, who is expected to possess same or better technical qualifications as well as eligibility criteria that is of the existing member to be replaced by such new member

6.10 The Parties undertake that they shall comply with all holding in consortium lock-in requirements set forth in the Contract Agreement.

7. Representation of the Parties

Each Party represents to the other Parties as of the date of this Agreement that:

(a) Such Party is duly organised, validly existing and in good standing under the laws of its incorporation and has all requisite power and authority to enter into this Agreement;

(b) The execution, delivery and performance by such Party of this Agreement has been authorised by all necessary and appropriate corporate or governmental action and a copy of the extract of the charter documents and board resolution/ power of attorney in favour of the person executing this Agreement for the delegation of power and authority to execute this Agreement on behalf of the Consortium Member is annexed to this Agreement, and will not, to the best of its knowledge:

(i) require any consent or approval not already obtained;

(ii) violate any Applicable Law presently in effect and having applicability to it;

(iii) violate the memorandum and articles of association, by-laws or other applicable organisational documents thereof;

(iv) violate any clearance, permit, contract , grant, license or other governmental authorisation, approval, judgement, order or decree or any mortgage agreement, indenture or any other instrument to which such Party is a party or by which such Party or any of its properties or assets are bound or that is otherwise applicable to such Party; or

(v) create or impose any liens, mortgages, pledges, claims, security interests, charges or Encumbrances or obligations to create a lien, charge, pledge, security interest, encumbrances or mortgage in or on the property of such Party, except for encumbrances that would not, individually or in the aggregate, have a material adverse effect on the financial condition or prospects or business of such Party so as to prevent such Party from fulfilling its obligations under this Agreement;

(c) this Agreement is the legal and binding obligation of such Party, enforceable in accordance with its terms against it; and

(d) there is no litigation pending or, to the best of such Party's knowledge, threatened to which it or any of its Affiliates is a party that presently affects or which would have a material adverse effect on the financial condition or prospects or business of such Party in the fulfillment of its obligations under this Agreement.

8. Termination

This Agreement shall be effective from the date hereof and shall continue in full force and effect until the Financial Close of the Project is achieved under and in accordance with the Contract Agreement, in case the Project is awarded to the Consortium. However, in case the Consortium is either not qualified for the Project or does not get selected for award of the Project, the Agreement will stand terminated in case the Applicant is not qualified or upon return of the EMD/Bid Security by the NDMC to the Applicant, as the case may be.

9. Miscellaneous

9.1 This Joint Bidding Agreement shall be governed by laws of {India}.

9.2 The Parties acknowledge and accept that this Agreement shall not be amended by the Parties without the prior written consent of the NDMC.

IN WITNESS WHEREOF THE PARTIES ABOVE NAMED HAVE EXECUTED AND DELIVERED THIS AGREEMENT AS OF THE DATE FIRST ABOVE WRITTEN.

SIGNED, SEALED AND DELIVERED For and on behalf of LEAD MEMBER by:	SIGNED, SEALED AND DELIVERED For and on behalf of SECOND PART by:
(Signature)	(Signature)
(Name)	(Name)
(Designation)	(Designation)
(Address)	(Address)

SIGNED, SEALED AND DELIVERED
For and on behalf of
THIRD PART by:

(Signature)

(Name)

(Designation)

(Address)

In the presence of:

1.   2.

Notes:

1. *The mode of the execution of the Joint Bidding Agreement 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.*
2. *Each Joint Bidding Agreement should attach a copy of the extract of the charter documents and documents such as resolution / power of attorney in favour of the person executing this Agreement for the delegation of power and authority to execute this Agreement on behalf of the Consortium Member.*
3. *For a Joint Bidding Agreement executed and issued overseas, the document shall be legalised by the Indian Embassy and notarized in the jurisdiction where the Power of Attorney has been executed.*

Format of Bank Guarantee

(To be executed on Requisite Non-Judicial Stamp Paper of Rs.100)

WHEREAS, (Name of the Applicant) wishes to submit his Bid for the selection of SI for PPP Project for "Application for "Request for Proposal for Selection of System Integrator for NDMC Smarty City Project "Design, Development, built, Implementation, Operation and Maintenance of Command and Control Centre & Data Center, ERP Solution and integration with various Smart City/NDMC Applications".

KNOW ALL MEN by these presents that we (Name of bank) of (city and country) having our registered office at ____(hereinafter called "the Bank") are irrevocably and unconditionally bound to the New Delhi Municipal Council or its successor, (hereinafter referred to as " NDMC" in the sum of Rs. _________________________(in Words)________________________________ which payment can truly be made to NDMC. The Bank binds themselves, their successors and assigns by these presents.

Sealed with the Common Seal of the Bank this _______ day of, 2017

THE CONDITIONS of this obligation are:

(a) If the applicant withdraws his Bid at any time during the stipulated period of Bid Validity specified in the RFP document and; or

(b) If the Applicant, for the period of the Bid Validity as per RFP document in NDMC's opinion, commits a material breach of any of the terms and/or conditions contained in the RFP Documents and/or subsequent communication from NDMC in this regard; or

(c) If the applicant, refuses to accept the correction of errors in the Bid; or

(d) If the applicant, having been notified of the acceptance of its Bid by the NDMC fails or refuses to comply with the following requirements:

- Pay either the performance security of the first installment of the Contract fee as specified in Clause 5.4.1 of the RFP document to New Delhi Municipal Council (NDMC)
- Sign the Contract Agreement as provided in the RFP Document We agree and undertake, absolutely, irrevocably and unconditionally to pay to the NDMC, as the case may be, the above amount without protest, delay or demur upon receipt of NDMC's first written demand, without the NDMC having to substantiate its demand, provided that in its demand the NDMC will

note that the amount claimed by it is due to it owing to the occurrence of one or more of the conditions set out above, specifying the occurred condition or conditions.

The Guarantee will remain in force up to and including the date of expiry of the period of Bid Validity as stated in the RFP Document or as extended by NDMC at any time as per RFP, notice of which extension to the Bank being hereby waived.

Provided however, that

In the event that this Applicant is selected for award of the project through the issue of the Letter of Intent, the EMD shall remain in force until the date of signing of agreement by such Applicant

OR

In the event this Applicant is not selected for award of the Project, the Earnest Money Deposit shall remain in force up to and including a period of 60 days after the expiration of the bid validity period or signing of the agreement, which is later.

Any demand in respect of this Guarantee should reach the Bank not later than the date of expiry (as defined above) of this Guarantee.

The jurisdiction in relation to this Guarantee shall be the courts of Delhi and the Indian law shall be applicable.

SIGNATURE OF AUTHORISZED
REPRESENTATIVE OF THE BANK___________________________________
NAME AND DESIGNATION ____
SEAL OF THE BANK____
NAME OF THE WITNESS ____
ADDRESS OF THE WITNESS _______________________________________

Formats for Submission of the Financial Bid

Sl	Head	Amount (in Rs.)	Amount (in words)
1.	**Total CAPEX price**		
2.	**Total OPEX price**		
3.	**Total price (1+2)**		

N.B –

1. Bidder must ensure that all amounts to be quoted in INR and inclusive of all taxes/levies/duties/charges.
2. Value coated as total price must contain all the components required for the successful implementation of the project.
3. Nothing extra will be paid by NDMC beyond the value quoted in the above form.
4. Service Tax will be paid by SI and the same will be reimbursed by NDMC on production of proof of payment .

Price component for CAPEX:

The Bidder shall consider all the components and quantity to fulfill the RFP and project requirements in totality.

Sl#	Line Item	Make & Model	Unit of Measurement	Proposed Quantity	Unit base price	Total Price
1	2	3	4	5	6	7=5*6
Sub Total of Service Components						
Sub Total of Infrastructure Components including Hardware, AMC and Software licenses & support (for ICCC & Data Center)						
Total CAPEX Price						

Total CAPEX Price (in words) -

___

1. Note: 1. Bidder must ensure that all the line items are covered as specified in Bill of Material (BOM) and all required fields in the Commercial bid format are duly filled and calculated appropriately.
2. All amounts to be quoted in INR. The price will be inclusive of all taxes/levies/duties/charges.
3. Service Tax will be paid by SI and the same will be reimbursed by NDMC on production of proof of payment .
4. The sequence of items provided in the above table (for Infrastructure Components including Hardware, AMC and Software licenses & support)

must match with the sequence of items provided in the Proposed Bills of Material as per Annexure-21 this volume of the RFP.

OPEX Cost for five years

S. No.	Description of Item	O&M Cost					Total Cost
		1st year	2nd year	3rd year	4th year	5th year	
1.							
2.							
3.							
4.							
5.							
						Total Cost	

Power of Attorney for signing of Application

Know all men by these presents, We………………………………………….. (name of the firm and address of the registered office) do hereby irrevocably constitute, nominate, appoint and authorise Mr/ Ms (name),…………………… son/daughter/wife of ………………………………and presently residing at …………………, who is presently employed with us/ the Lead Member of our Consortium and holding the position of ……………………………. , as our true and lawful attorney (hereinafter referred to as the "Attorney") to do in our name and on our behalf, all such acts, deeds and things as are necessary or required in connection with or incidental to submission of our application for pre-qualification and submission of our bid for the ***** Project proposed or being developed by the ***** (the "Authority") including but not limited to signing and submission of all applications, bids and other documents and writings, participate in Pre-Applications and other conferences and providing information/ responses to the Authority, representing us in all matters before the Authority, signing and execution of all contracts including the Contract Agreement and undertakings consequent to acceptance of our bid, and generally dealing with the Authority in all matters in connection with or relating to or arising out of our bid for the said Project and/ or upon award thereof to us and/or till the entering into of the Contract Agreement with the NDMC.

AND we hereby agree to ratify and confirm and do hereby ratify and confirm all acts, deeds and things done or caused to be done by our said Attorney pursuant to and in exercise of the powers conferred by this Power of Attorney and that all acts, deeds and things done by our said Attorney in exercise of the powers hereby conferred shall and shall always be deemed to have been done by us.

IN WITNESS WHEREOF WE, ……………….., THE ABOVE NAMED PRINCIPAL HAVE EXECUTED THIS POWER OF ATTORNEY ON THIS ……… DAY OF ………, 20......

For…………………………..

(Signature, name, designation and address)

Witnesses:
1.
2.

(Notarised)

Selection of SI for this PPP project

Accepted
……………………………

(Signature)
(Name, Title and Address of the Attorney)

Notes:

- *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*.
- *Wherever required, the Applicant should submit for verification the extract of the charter documents and documents such as a board or shareholders' resolution/ power of attorney in favour of the person executing this Power of Attorney for the delegation of power hereunder on behalf of the Applicant.*
- *For a Power of Attorney executed and issued overseas, the document will also have to be legalised by the Indian Embassy and notarised in the jurisdiction where the Power of Attorney is being issued. However, the Power of Attorney provided by Applicants from countries that have signed the Hague Legislation Convention, 1961 are not required to be legalised by the Indian Embassy if it carries a conforming Appostille certificate.*

Annexure-8

Statement of Legal Capacity

(To be forwarded on the letterhead of the Applicant/ Lead Member of Consortium)

Ref. Date:

To,
****
****

Dear Sir,

We hereby confirm that we/ our members in the Consortium (constitution of which has been described in the application) satisfy the terms and conditions laid out in the RFP document.

We have agreed that …………………… (insert member's name) will act as the Lead Member of our consortium.*

We have agreed that ………………….. (insert individual's name) will act as our representative/will act as the representative of the consortium on its behalf* and has been duly authorized to submit the RFP. Further, the authorised signatory is vested with requisite powers to furnish such letter and authenticate the same.

Thanking you,

Yours faithfully,

(Signature, name and designation of the authorised signatory)
For and on behalf of……………………………..

** Please strike out whichever is not applicable.*

Annexure-9

Declaration of Non-Blacklisting

(To be provided on the Company letter head)

Declaration for Lead Applicant:

Place________________

Date________________

To,
Office of the Executive Engineer
Room No.1503, 15th Floor,
New Delhi Municipal Council
Palika Kendra New Delhi – 110001
Tel No:- 011-23348418
Email: to be added

Subject: Self Declaration of not been blacklisted in response to the Request for Proposal for Selection of System Integrator for NDMC Smarty City Project "Design, Development, built, Implementation, Operation and Maintenance of Command and Control Centre & Data Center, ERP Solution and integration with various Smart City/NDMC Applications".

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 Lead Applicant)

Printed Name
Designation
Seal
Date:
Place:
Business Address:

Annexure-10

No Deviation Certificate

This is to certify that our offer is exactly in line with your tender enquiry/RFP (including amendments) no._________ dated._______. This is to expressly certify that our offer contains no deviation either Technical (including but not limited to Scope of Work, Business Requirements Specification, Functional Requirements Specification, Hardware Specification and Technical Requirements Specification) or Commercial in either direct or indirect form.

(Authorised Signatory)

Signature:

Name:

Designation:

Address:

Seal:

Date:

Annexure-11

Manufacturers'/Producers' Authorization Form

(This form has to be provided by the OEMs of the hardware and software solutions proposed. This letter of authority 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,
Office of the Executive Engineer
Room No.1503, 15th Floor,
New Delhi Municipal Council
Palika Kendra New Delhi – 110001
Tel No:- 011-23348418
Email: to be added

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 Applicant) 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 Applicant and or maintenance or support services for software products against this invitation for bid by ______(Name of the Applicant) as per requirements of this RFP.

Thinking you,
Yours faithfully,
(signature)

For and on behalf of:__________(Name of the OEM)
Authorised Signatory
Name:
Designation:
Place:
Date:

Credential Summary

S.No.	Project Name	Client Name	Project Value (in INR)	Project Components	Documentary evidence provided (Yes/No)	Project Status (Completed or Ongoing or Withheld)
1						
2						
3						
4						
5						
6						
7						
8						

- Client type- Indicate whether the client is Government or PSU or Private
- Project Components- Indicate the major project components like setting up of ICCC.
- 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)

Annexure-12

Formats for Submission of the Pre-Qualification Bid

Pre-qualification bid checklist

Sl No.	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 3		
5.	· Copy of Certification of Incorporation/Registration Certificate · PAN card · VAT registration ·		
6.	Audited financial statements for the last three financial years (FY 2014-15, 2015-16 and 2016-17). 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		

15.11 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	
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:

	2014-15	2015-16	2016-17
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 Rs. 20 Crore as an end of financial year 2015-16 i.e. 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.

Annexure-13

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:

Annexure-14

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:

Annexure-15

Overview of Proposed Solution

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

Annexure-16

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 Programme						
		1	2	3	4	5	6	…
	Project Plan							
1	Activity 1							
1.1	Sub-Activity 1							
1.2	Sub-Activity 2							

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.

Annexure-17

Manpower Plan

I. Till Go-Live (Implementation)

Sl No.	Manpower	Months				Total
		Month 1	Month 2	……………..	Month 12	
1.	Program Manager					Onsite
2.	Citizen Service/Municipal Domain expert					Onsite
3.	Water SCADA or Electrical SCADA expert					Onsite
4.	IBMSexpert					Onsite
5.	Surveillance Expert					Onsite
6.	ITMS Expert					Onsite
7.	Solution Architect					Onsite
8.	Project Manager-Software					Onsite
9.	Project Manager-Infrastructure					Onsite
10.	Database Architect					Onsite
11.	Security Expert					Onsite
12.	Command and Control Centre management Expert					Onsite
13.	Mobile App development Expert					Onsite

II. After Go-Live (Operation & Maintenance for 5 Years)

S.N	Type of Resource	Minimum Quantity	Minimum Deployment during Operation and Maintenance phase
1.	Project Manager	1	100%
2.	Solution Architect	1	Onsite Support to Project team on need basis
3.	Project Manager-Software	1	100%
4.	Project Manager – Infrastructure	1	100%
5.	Database Architect/DBA	1	100%
6.	Security Expert	1	Onsite Support to Project team on need basis
7.	Command Centre Expert	1	100%
8.	IBMS expert	1	Onsite Support to Project team on need basis
9.	Help Desk Manager	1	100%
10.	Help Desk Executives	As per requirement	100%

.

Annexure-18

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

Annexure-19

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. .

7.9 Manufacturers/Producers Authorization Form

(This form has to be provided by the OEMs of the hardware and software solutions proposed. This letter of NDMC 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,
Executive Engineer
New Delhi Municipal Council
Palika Kendra, New Delhi

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:

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 **Request for Proposal for Selection of Master System Integrator for Integrated Command and Control Center for New Delhi Municipal Council (NDMC)** in **NDMC**, New Delhi against the RFP issued by Procuring Entity, 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:

Annexure 20

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>> "**Request for Proposal for Selection of System Integrator (SI) for NDMC Smarty City Project "Design, Development, built, Implementation, Operation and Maintenance of Command and Control Centre & Data Center, ERP Solution and integration with various Smart City/NDMC Applications".**

" (hereinafter called the said 'RFP')to the "[NDMC]", 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 :

Annexure 21

Proposed Bill of Material

The Bidder should provide the proposed Bill of Material (BoM). Bidders are required to mention the unit of measurement, quantity proposed, details of the make/brand and model against each line item, wherever applicable. Bidder may feel free to do the addition of list of line items based on their proposed solution for ICCC. The bidders are proposed to rationalize / justify the quantities mentioned in the proposed BOM in line with the scope of work defined this RFP. This will be evaluated during technical presentation. Once the bidder provides this information in the submitted bid, the bidder cannot change it with any other component / equipment etc. of lower specifications / performance; it can only be upgraded at the time of actual deployment/installation.

This Proposed Bill of Material is required to be submitted along with technical proposal submitted by the bidder. The bid can be considered non-responsive in the absence of such details.

The list of items mentioned hereunder is indicative. The Bidder shall consider the components and quantity to fulfill the RFP and project requirements in totality.

Format for Un-priced Bill Of Material (BOM)

Bill of Material (Tentative items and their quantities have been given however System Integrator (SI) has to assess the quantities based on their design, NDMC requirements and site conditions. The number of items and quantities can also be more, some of these are the minimum required hardware and software items and quantities whereas some are illustrative, but in order to implement this scope of work, the items required may be more and the SI has to assess and provide those items to fully implement and made functional all the services as per scope defined in this RFP document).

Sr. No.	Description of items for supply and installation as per detailed specifications given in RFP document.	Unit of measurement	Qty. proposed	Make /Brand warranty	Model Details	Full compliance with RFP requirements (Yes/No)
1.	Command and Control Room site preparation covering Design, Supply, Installation of Civil, interior decoration (flooring, false ceiling, wall paneling, roof paneling, glass partitions, glass doors, creation of viewing gallery, space for video wall etc.), electrical works, air-conditioning, data cabling, furniture, fire control system, CCTV, work console for operators for Command control centre complete in all respects.	Lump sum	1			
1.1	Civil, interior decoration (flooring, wall paneling, roof paneling, glass partitions, glass doors etc.), creation of space for Video-Wall.	Lump sum				
1.2	Electrical works	Nos.				
1.3	Air-conditioning	Nos.				
1.4	Data cabling	Nos.				
1.5	Workstation Console & Peripherals- Cubicles with Table and Chair for operators (As required) - for 25 operators	Nos.	1			
1.6	Other furniture items	Nos.				
1.7	Fire control system	Nos.				
1.8	Access control	Nos.				
1.9	Camera	Nos.				
1.10	Other miscellaneous items.	Nos.				
2.	Data Center Site preparation covering Design, Supply, Installation of Civil, interior decoration (flooring, wall paneling, roof paneling, glass partitions, glass doors etc.), electrical works, air-conditioning, data cabling, furniture, CCTV, fire control system, work console for operators for Data Centre complete in all respects.	Lump sum	1			

2.1	Civil, interior decoration (flooring, wall paneling, roof paneling, glass partitions, glass doors etc.),					
2.2	Electrical works	Nos.				
2.3	Air-conditioning	Nos.				
2.4	Data cabling	Nos.				
2.5	Networking racks with rack based air-conditioning	Nos.				
2.6	Other furniture items	Nos.				
2.7	Fire control system	Nos.				
2.8	Access control	Nos.				
2.9	Camera	Nos.				
2.10	Other miscellaneous items	Nos.				
3.	Command Control Center (CCC) Solution with integration/Data Normalization & City Operation software in HA.	Lump Sum	1			
4.	Study, Design, development and implementation of ERP Solution as per requirement defined in this RFP and integration with ICCC.	Lump sum	1			
5	Smart City Data Center					
5.1	Blade Chassis & Management	Nos.	3			
5.2	Blade Servers for applications (Min-Qty)	Nos.	12			
5.3	Operating Systems & DB License	Lot	As required			
5.4	Data Center Switch-Type I	Nos.	2			
5.5	Data Center Switch-Type II	Nos.	2			
5.6	Primary & Secondary Storage Solution (Non Video) Applications (Min 200TB) And for CCTV Applications 800 TB i.e. for 500 CCTV @15 fps of 2 MP for 30 days	Lot	1			
5.7	Tape Library	Lot	1			

5.8	Backup Storage	Lot	1			
5.9	Backup Software	Lot	1			
5.10	Internet Router	Nos.	2			
5.11	WAN Services Router	Nos.	2			
5.12	Firewall	Nos.	2			
5.13	Anti-APT for Command & Control Room	Lot	1			
5.14	Network Behaviors Analyses	Lot	1			
5.15	Web-security appliance	Lot	1			
5.16	IPS	Nos.	2			
5.17	Network Management System and WLAN Management System	Lot	As required			
5.18	EMS for DC,SLA management and helpdesk	Lot	As required			
5.19	Networking (Passive Components)	Lot	As required			
5.20	Air conditioning	Lot	As required			
5.21	UPS (30 minutes backup) of required capacity as per equipments installed in data centre	Nos.	1			
5.23	Suitable rack solution for stacking Servers having complete electrical connections and rack based air conditioning.	Nos.	5			
5.24	Video Management System- Software for Recording, Viewing of Videos **(500 Cameras)**	Nos.				
5.25	Onboard/Server Based Advanced Video Analytics Package Software for Left Object Detection	Nos.				
5.26	Onboard/Server Based Advanced Video Analytics Package Software for Crowd Monitoring	Nos.				
5.27	Onboard/Server Based Audio Analytics Software for Gunshot Detection	Nos.				
6	**City Operation Centre Physical infrastructure**					
6.1	Video Wall (along with hardware & software) Solution - 6x3 Display of 70” each.	Nos.	1			

6.2	Operators Client Workstations for Command Control Centre and Communication System -40” to 45” LED Curved Screen –	Nos.	25			
6.3	Multi-Function Laser Printer	Nos.	2			
6.3	1 Screen – Help Desk/Admin Operation	Nos.	2			
6.4	Networking Cost (Passive Components)	Nos.	1			
7	**Collaboration and Virtual Education Solution**					
7.1	VC End Point - Meeting Room Based Video conferencing Solution	Nos.	5			
7.2	Smart Class Solution - Centralized Video Portal with centralized distribution engine as per technical specifications	Nos.	1			
7.3	Collaboration Solution - Multipoint Control Unit as per technical specifications	Nos.	1			
7.4	Collaboration Solution - all Control with scheduling and Firewall Traversal as per technical specifications	Nos.	1			
7.5	Collaboration Solution - Recording Solution as per technical specifications	Nos.	1			
7.6	Collaboration Solution - Centralized Video Portal with centralized distribution engine as per technical specifications	Nos.	1			
8	UPS with 30 minutes backup (ICCC & DC)	Nos.	1			
9	CCTV					
9.1	Type 1: Panoramic Camera	Nos.	75			
9.2	Type 2 :Fixed IR Camera	Nos.	225			
9.3	Type 3 : Fixed Box Camera	Nos.	125			
9.4	Type 4 : Camera- High Definition	Nos.	75			
9.5	IR Illuminators	Nos.				
9.6	Poles, Mounting for Cameras, Light and Equipments	Nos.				
9.7	Provisioning of Electrical Power for CCTV camera	Nos.				

9.8	Industrial Grade Network Switches – Type 2	Nos.				
9.9	Industrial Grade Network Switches – Type 3	Nos.				
9.10	Video Analytics	Nos.				
10	RFID based Solid Waste Management System					
10.1	RFID Tags for each household bins	Nos.	75000			
10.2	RFID Tags Readers to be installed in Garbage Collection vehicles alongwith the data transfer module.	Nos.	45			
10.3	Supply and installation of Weight measuring sensors at each garbage collection vehicles.	Nos.				
10.4	ICT based Solid Waste Mgmt. System	Nos.	1			
10.5	RFID based Bin Management System, Weight & Volume Sensor Management System	Nos.	1			
11	DG Set of required capacity for ICCC & DC	Nos.				
12	Project Management & Project Installation cost	Lot	1			
13	Manpower Cost for Helpdesk and Call Centre operation (24X7) for five years	Nos.	1			
14	Comprehensive O&M cost including Manpower for 5 Years for the date of GO-LIVE	Lot	1			
15	Training and Capacity Building	Lot	1			
	Total Cost including 5 year Comprehensive AMC and Warranty					

Request for Proposal for Selection of System Integrator (SI) for NDMC Smarty City Project "Design, Development, built, Implementation, Operation and Maintenance of Command and Control Centre & Data Center, ERP Solution and integration with various Smart City/NDMC Applications".

Volume II

Detailed Scope of Work & Technical Specifications

NEW DELHI MUNICIPAL COUNCIL

PALIKA KENDRA, SANSAD MARG,

NEW DELHI

Table of Contents

Abbreviations

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.	**ICCC**	Integrates Command and Control Centre
7.	**CCTV**	Close Circuit Television
8.	**DHCP**	Dynamic Host Configuration Protocol
9.	**ERP**	Enterprise Resource Planning
10.	**FMS**	Facility Management Service
11.	**FRS**	Functional Requirement Specification
12.	**GIS**	Geographical Information System
13.	**GOI**	Government of India
14.	**IBMS**	Integrated Building Management System
15.	**ICT**	Information and Communication Technology
16.	**IEEE**	Institute of Electrical and Electronics Engineers
17.	**IT**	Information Technology
18.	**ITMS**	Intelligent Transport Management System
19.	**KPI**	Key Performance indicators
20.	**LDAP**	Lightweight Directory Access Protocol
21.	**MPLS**	Multiprotocol Label Switching
22.	**SI**	System Integrator
23.	**NOC**	Network Operation Centre
24.	**NDMC**	New Delhi Municipal Council
25.	**OEM**	Original Equipment Manufacturer
26.	**OFC**	Optical Fibre Cable
27.	**PABX**	private automatic branch exchange
28.	**RAID**	Redundant Array of Inexpensive Disks
29.	**RTU**	Remote Terminal Unit
30.	**SAN**	Storage Area Network
31.	**SCADA**	Supervisory Control and Data Acquisition
32.	**SITC**	Supply Installation Testing and Commissioning
33.	**SLA**	Service Level Agreement
34.	**SNMP**	Simple Network Management Protocol
35.	**SRS**	Software Require Specification
36.	**SSL**	Secure Sockets Layer
37.	**VLAN**	Virtual Local Area Network

1. Introduction

1.1 About NDMC

NDMC is one of the five urban local body in National Capital Territory of Delhi. It has its origins in the Imperial Delhi Committee, which was constituted on 25 March 1913 to overlook the construction of the new capital of India. The administrative area under the New Delhi Municipal Council comprises of 42.7 sq. km. The NDMC is governed by a Council by a 13 member Council. The Council Members includes the Member of Parliament of New Delhi Parliamentary Constituency, the Member of Legislative Assembly of New Delhi and Delhi Cantonment Assembly Constituency.

NDMC consists of nearly 3% of the area and 2.5 lakh of the resident population of National Capital Territory of Delhi. However, there is about 16-20 lakhs floating population in daytime which possess challenges for managing the civil services in NDMC area.

NDMC is a seat of the head of the Federal Legislature, Executive and the Judiciary. The NDMC region comprises of Lutyen's Delhi, the area which was historically come was regarded as the centre of Central in Union of India. It also consists of important buildings such as Rashtrapati Bhawan, Parliament House, Supreme Court, North and South Blocks and others. In addition to this, NDMC area also comprises of the embassy area. The strategic geo-political location of the NDMC area and its history makes the area extremely important for the country. Efficient functioning of the municipal body is, thus, extremely important for the country.

NDMC's main responsibilities are –

- Providing basic civic amenities
- To manage its own assets and collection of Property Tax
- Building Regulation
- Registration of Birth and Death
- Construction, and maintenance of municipal markets and regulation of trades
- Sanitation & Public Health
- Maintenance of public parks, gardens or recreational centres

NDMC is one of the few local bodies in the country who is financial self-reliant. It is also a distribution company for water and electricity and its municipal solid waste is 100% scientifically disposed of.

1.2 Objective of this RFP

Through this RFP NDMC intends to select a System Integrator (SI) by following competitive bidding process to design, develop, implement and maintain the Integrated Control and Command Centre (ICCC) for a period of 5 (Five) years after Go Live (Go-Live date) on turnkey basis.

This document contains the following details:

a. Scope of work in setting up ICCC by SI
b. Other terms and conditions

This document provides a high-level overview of the technology approach in setting up the ICCC and in-depth details of the functional roles of ICCC system components, and the interactions between roles of various stakeholders, to achieve an end-to-end system design.

The ICCC will be a central hub for city management. The ICCC will be helpful in managing the city assets City Operations including emergency response. The primary hosting of all applications and database will be done at in premise Data Centre. SI should ensure provision of Disaster Recovery (DR) on Cloud in future whenever required by NDMC in future. Integrated Building management system will be implemented in the ICCC building for managing and monitoring building utilities, access, security etc.

1.3 Project Vision

Integrated Control and Command Centre (ICCC) will be established for NDMC area to run city operations. Citizens will be using ICT as backbone and seamless integration will be completed with all the required & existing ICT systems / Smart components of NDMC initiatives.

Integrated Control and Command Center (ICCC) of NDMC will be a place which will gather all the departments and mind of the city using ICT as a backbone.

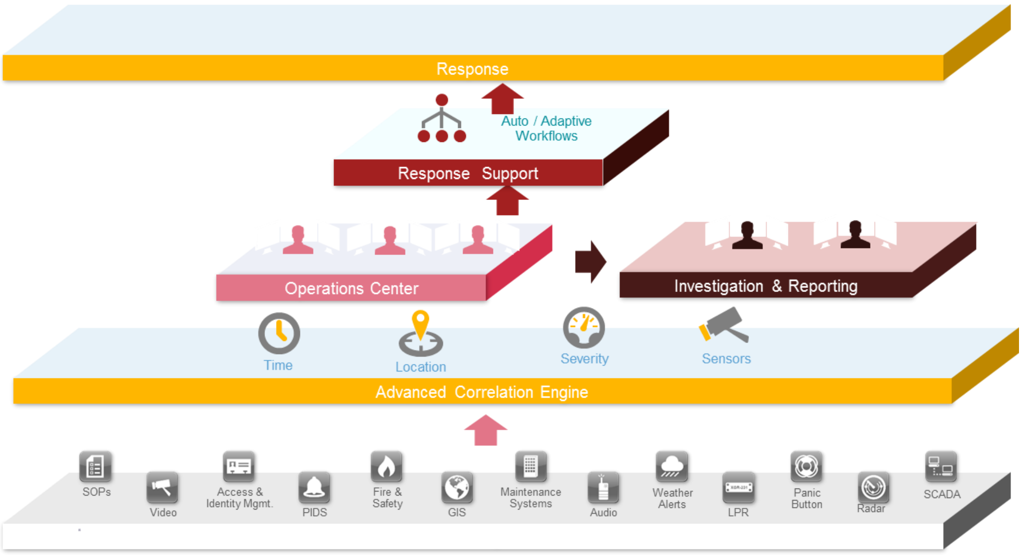
ICCC will be a place where information from various departmental command centers and data related to various applications will be collected and analyzed for better planning of the city. ICCC will have Business Intelligence engine which will process all the information and generate insights. These insights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

ICCC will have its own data center, co-located with command center.

ICCC will have physical capacity for future activities like co-locating services and its infrastructure based on the agreed plan.

ICCC will be scalable to host more applications and services in future for managing city more effectively.

ICCC will eventually become single source of truth for the city and its operations. ICCC will help make NDMC smart and livable for its citizens.



1.4 Project Objectives:

NDMC envision the planned ICCC to fulfil following objectives:

(i) “Single source of information” for all civic functions of NDMC

(ii) Platform with the ability to receive, intelligently correlate & share information with stakeholders who are into city operations and planning to better predict outcomes

(iii) Act as City’s emergency and disaster management platform

(iv) Ability to integrate multiple types of system originating heterogeneous data like text, voice, data, video and smart sensors communication interfaces

(v) Ability to integrate and correlate online and offline interactions

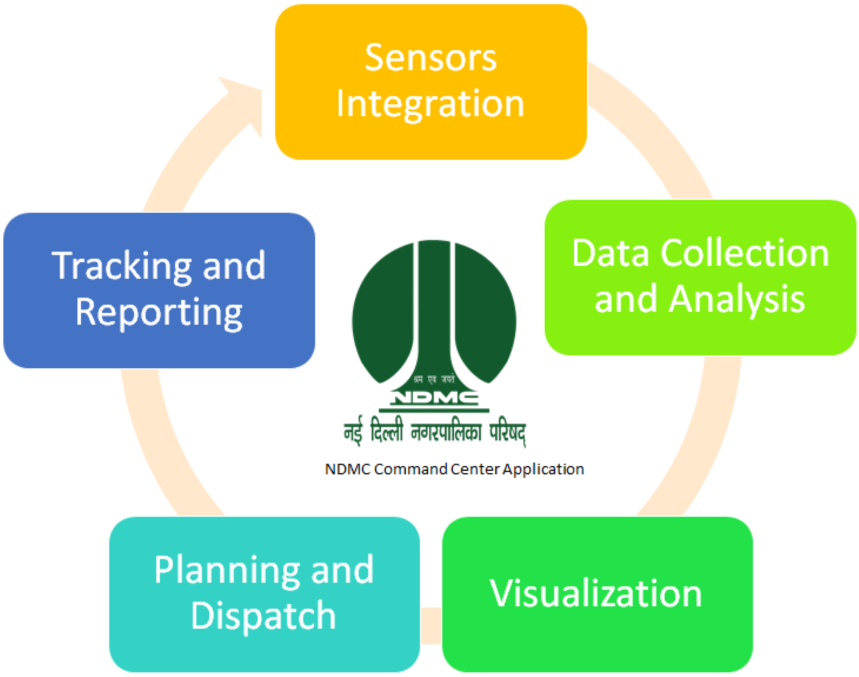
(vi) Capabilities to support GIS based incidents visualization

(vii) Future proof - based on Modular, Open, Configurable architecture with capabilities to integrate innovative new applications

(viii) Intelligent and Intuitive work-flow management

(ix) Advanced historical records management and archiving capabilities

(x) Advanced industrial grade cyber security features


Sensors Integration
Data Collection and Analysis
Visualization
Planning and Dispatch
Tracking and Reporting
NDMC
नई दिल्ली नगरपालिका परिषद
NDMC Command Center Application

1.4.2 The objective of establishing an Integrated Command and Control Center (ICCC) is to implement holistic and integrated solution for multiple IT initiative (existing and future) for NDMC. The IT initiative may of any department for example whether it is safe city (CCTV surveillance) or SCADA network of Municipal Council. The end objective of establishing ICCC is to drive the actions by NDMC on behalf of all the departments for city operations.

1.4.3 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:

(i) Support police to maintain Law and Order
(ii) Disaster Management
(iii) Environmental Control/ Pollution Control
(iv) Efficient user of public resources like electricity and water
(v) Efficient and timely delivery of public services
(vi) Better health and education services

1.5 Phase wise envisaged activities of ICCC

The overall implementation of ICCC is subdivided into three phases. The following activities to be undertaken by the System Integrator (SI).

- Pre-Implementation Phase
- Implementation Phase
- Post Implementation Phase

Pre –Implementation Phase:

- Conducting site survey, obtaining necessary permissions, developing system requirements, standard operating procedures etc.
- Providing physical layout of the ICCC (with 3D simulation) – This layout must contain the following:
  - Control and Command Setup
  - Data Center Setup
  - Other facilities which will be required forspeciallyabled people as per guidelines defined by Govt. of India
- 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.
- Formulation of solution architecture, detailed design of smart city solutions, development of test cases (Unit, System Integration and User Acceptance), SoP documentation

Implementation Phase:

- Physical Setup of ICCC as per the layout agreed with NDMC. This includes activities like false flooring, false ceiling, partitions, network cabling, electric fitting, establishment of office spaces, ICCC facility, data center facility, and other facilities as mentioned above along with required furnishing of the complete ICCC facility.
- 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 SI
- Software Application customization (if any), development of bespoke solution (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 GIS Platform, Integration of solutions with Command and Control Centre
- Facilitating user acceptance testing and conducting the pre-launch security audit of applications
- User training and roll-out of solution
- Integration of the various services &solution with ICCC platform
- 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

Post Implementation Scope for the Operation and Maintenance Phase:

- Deploying manpower 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 centralized Helpdesk and central control centre to receive citizen calls till the end of contractual period
- Recurring refresher trainings for the users and Change Management activities
- Conducting disaster recovery site testing through regular mock drills
- Provide facility, information and required access to NDMC 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.
- Overall maintenance of the ICCC facility and continuity of operations as per SLAs.
- Submit Quarterly reports as defined in the RFP.

Exclusions

- Built-up space, without furbishment for the control and communication center and data centre, will be provided by NDMC.
- Provisioning of network bandwidth and connectivity at various locations to connect with ICCC.
- Provisioning of power and water connection at ICCC location; however, the maintenance and continuity of operations of ICCC & Data Centre and maintenance of SLA’s thereon shall be the responsibility of the SI.

1.6 Regarding NDMC and need of ICCC

1.6.1 With respect to citizen services of urban development department, following are the major challenges that are being faced by NDMC city:

(i) Severe pressure on city resources
(ii) Unequal distribution of city resources
(iii) Lack of social inclusion
(iv) Livability challenges for citizens
(v) Environmental sustainability
(vi) In efficiency in city operations

Floating population in NDMC is putting lot of pressure on cities infrastructure resulting scarcity of resources. City resources are becoming difficult to manage day by day to increasing population and further putting pressure on the city administration in terms of optimum utilization of resources. Liveability of city is also a challenge since the residents do not get required city resources. Safety and security of city residents has become a major issue. Unplanned growth is also resulting in environmental sustainability of the city. An inefficient city is also not preferred as investment destination which in turn results in less employment opportunity for residents. These are putting severe pressure on city administrators in terms of improvising the living conditions of the citizens in the cities.

These issues can be mitigated through the adoption of scalable solutions that take advantage of information and communications technology (ICT) to increase efficiencies, reduce costs, and enhance quality of life. However, the key obstacle in implementing such scalable ICT solutions is the complexity of how cities are operated, financed, regulated, and planned. For example, every application is being developed independently, resulting in:

(i) Isolation of infrastructure and IT resources
(ii) No sharing of intelligence and information such as video feeds, data from sensors, etc.
(iii) Duplication in investment and effort
(iv) Difficulty in scaling infrastructure management

This fragmented approach is neither scalable nor economical and does not benefit from cross-functional sharing of data and services. For example, a city's congestion management solution can't use data from street-lighting sensors. Faced with this complexity, city leaders and stakeholders struggle on how to agree on the methodologies for implementing Smart City solutions.

Various perspectives of the implementation of Smart City solutions, and hurdles or challenges in each of them, are listed below:

(i) Cities have an opportunity to use the network as the platform to offer urban services and to be sustainable. Using the network as the fourth utility - along with electricity, water, and natural gas, cities can integrate multiple systems to deliver on-demand services over a highly secure Internet-enabled cloud infrastructure. Such services and related networks can help cities address urban challenges as well as improve their livability index.

(ii) State-of-the-art systems, such as intelligent transportation, parking, safety, and energy management, are helping cities to implement Smart City services. City leaders are partnering with private organizations to expand infrastructure and to create scalable systems and processes for economic growth.

(iii) With the aim of providing all citizen services on a single unified network, it is recommended that the city council both lead and facilitate cross-department collaboration, breaking silos of operations. The methodology brings together different city management services, and helps enable information exchange between resources and applications across different domains. This leads to consolidated investments in shared technology infrastructure and a common data layer where multiple services like smart parking, smart traffic, and smart lighting can be delivered. All of these services can then be delivered from a common citywide foundational network.

(iv) This approach not only gives cities a way to maximize returns from their investments but also allows for cross-domain collaboration. For example, it is helpful for public safety departments to know lighting conditions in the city. Similarly, the traffic department would do well to understand environmental data trends, such as of quality of air or temperature, over time in order to make better planning decisions. In the event of a public safety situation, different department representatives sitting together in a common center can coordinate their response much better as well. Likewise, sensors can help city officials monitor key environmental metrics to better be aware of seasonality heat/cold bursts and plan emergency response plans.

Considering the above, NDMC has decided to develop state-of-art Integrated Control and Command Centre in NDMC which will help to deliver below services:

a) ICCC Solution Exposes device control and data using a standardized API for third-party application developer ecosystem in a vendor-agnostic way.
b) Consolidates all city infrastructure assets onto a single operations platform.
c) Collects, stores, and provides access to data generated from “Connected” city infrastructure (through the digital platform) assets using common data models.
d) The extensible platform allows Customer to start small scale and then add solutions as needed.
e) Integration with ICCC with Unique Smart Addressing Solution for Urban Properties/ Establishments (USASUP)
f) Offers rapid, reliable flexible deployment
g) Offers greater trust and security with security standards.
h) Reporting (Data presentation)- Data can be reported for city modules, functionalities, and major performance indicators.
i) Integration with biometric attendance.

Example reports include:

- Parking occupancy, violations, and revenue
- Lighting-energy consumption and intensity
- Urban mobility (sizes of crowds, dwell time, traffic density, and speed)

j) Trends in the air quality index (AQI) and environmental pollutants such as carbon dioxide, carbon monoxide, and nitric oxide and nitrogen dioxide
k) Monitoring of water quality, STP.
l) 24x7 water supply, Electricity SCADA, Public Bike sharing, Smart Class Room, Solid Waste Management.

1.7 Current ICT based systems of NDMC

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 NDMC envisages to integrate these IT systems with command and control center of smart city:

a) Smart LED Street Lights/Smart Poles

a. Converting traditional street lights to LED based intelligent lights
b. Smart poles with capability to accommodate multi operator telecom Base Stations for 2G/3G/LTE to reduce mobile call drops
c. Surveillance cameras inbuilt into smart poles/separately installed CCTV
d. Wi-Fi hotspots
e. Interactive Digital Signage for traffic & business
f. Environment sensors
g. CCMS of different LED Manufacturer to be integrated

b) Sensor Based & Camera Based Smart Parking

NDMC has already invited RFP for sensor based parking. Different type of sensors will be installed on individual parking slot to uniquely identified the occupancy of these parking slots. Data of each sensor will come to the Central Command and control centre. NDMC/Public can monitor the real time data of occupancy of parking slots.

Feed for CCTV installed in these parking lot will also come to the ICCC on requirement basis on real time.

c) Water- SCADA & Water Meter

NDMC has planned to install AMI meters at all consumers locations and bulk electromagnetic flow meter at all inlet points. Real time data of quantity and quality of water will be made available to the consumers. SCADA System will also be implemented to get real time information of water network on GIS and can be controlled through ICCC.

d) Electricity – SCADA & Electricity Meter

SCADA System is already implemented upto 33KV ESS. Now, it is being implemented upto 11KV ESS. AMI meters at all consumers are proposed to be installed. Up gradation of the Electricity distribution System is under process. Tenders already invited. This complete system will be integrated to ICCC.

e) Property Tax (GIS)

i. Property Tax Identification Number (PTIN)
ii. Mobile Number & Aadhar number/email IDs (if available) of the residents/occupants/tenants/ managers/ caretakers
iii. Total land area of the property: which will have measurement of the plot area /individual dwelling unit area / commercial unit area / institutional unit area/ civic facility unit
iv. Electricity Connection, consumer numbers and total Number of connection
v. Water Connection consumer numbers and total Number of connection
vi. Estate License/lease number (if any)
vii. Other source of electricity e.g. Solar/DG Set.
viii. Other source of water
ix. Gas connection.
x. Petrol pumps, LPG Station, Hospitals, Hotels, cinemas, Schools, CNG Stations etc.
xi. Year of construction/redevelopment of the property /
xii. Any known litigation /dispute
xiii. License number / shop establishment/ VAT registration number
xiv. Rain -water harvesting facility
xv. In-house MSW recycling /disposal facility.

f) Smart Classroom

(i) New Delhi Municipal Council has set-up 444 Smart Classrooms in place of traditional Chalk and Board Classrooms' in all NDMC/Navyug schools from classes VI to XII. The initiative is a part of the 'Smart City Project' and will provide NDMC schools a high level of academic environment.

(ii) Besides actual syllabus teaching, children can take advantage of upgraded technology in learning about socio-political events, leading personalities, culture, heritage, sports, environment and other areas related to child development.

(iii) Smart Classrooms have been set up in all Hindi and English Medium sections from class VI to XII in 29 NDMC/ Navyug Schools. Availability of the educational digital contents both in Hindi & English medium in all subjects and their regular up-gradation is an important feature of the project. The educational digital contents of the smart classrooms have been designed to make the syllabus more comprehensive and easy to understand. With the help of the smart classroom, the complex chapters of any subject will be easy to understand for the students.

(iv) The standard Smart Classroom consists of White board, Interactive Ultra short throw interactive projector, green board, CPU, UPS, Keyboard, Mouse and Sound system with woofers. CCTV cameras have also been set up in all smart classrooms to make it more useful and sustainable.

(v) To make the project efficient and effective, continuous and intensive training of the teachers been as an integral part of the project. Apart from the intensive training of one week, there will be regular training of teachers on quarterly basis to make it more convenient for the teachers.

(vi) It is a privilege for the NDMC's students, to get opportunity to avail the latest educational digital contents facility comparable with such facilities in the best schools in Delhi. This endeavor will no doubt have a greater impact on improving the academic environment of the NDMC schools.

g) CCTV: CCTV cameras have been installed in NDMC Class rooms, Hospital, dispensaries, ESS and other office buildings.

h) App NDMC311 (For Citizen and NDMC internal App)

For ensuring transparency and easy accessibility of civic services NDMC has expended the digital platform to mobile platform. The aim is to take civic services to people's doorsteps and move towards deliberative democracy and citizen empowerment. The mobile digital platform helps in reducing the number of trips the citizens have to make to a municipal services office. It is a convenient tool on account of the fact that over 2 million citizens in Delhi alone use smart phones in India. This platform is also ideal for G-to-C and C-to-G interface. NDMC provides integrated public services to citizens and tourists through a user-friendly mobile cloud based NDMC 311 CITIZEN App since March 2016. There are 14 integrated services for providing information and for registering complaints while giving location, image. This comes also with an SMS facility so that the citizen gets acknowledgment of the receipt of complaints and online information about the progress of its resolution. Complaints regarding water, electricity, sanitation, sewerage, water-logging, damaged roads, street-lights maintenance etc. can be lodged, monitored and closed by citizen to their satisfaction. The complaint is routed to a field monitoring Smart City 311 Officers App operated by the officials of the municipality for prompt resolution. The app also features real time traffic and parking situation in NDMC area, water quality monitoring reports, notifying the nearby points and places of interest to the citizens and tourists such as hospitals, monuments, markets, metro stations, PTUs. Helpline Numbers relating to citizens' safety, the availability of medicines in NDMC hospitals and clinics, FAQs with information about NDMC Departments, online payment facilities, online approval for building online. The app has MIS reports indicating performance metrics with regard to complaint resolution, field inspections, attendance, work assignments. Feedback system and social media integration is inbuilt for user value assessment and public cooperation. Available on Android & IOS Platforms, the NDMC311 Citizen App has been downloaded by 10,551 users since its launch in March 2016; 8689 complaints were lodged and 8511 resolved. On Smart City 311 officers App, 35,658 online Inspections conducted by 550 officials.. NDMC recently added online littering and encroachments monitoring & prosecutions functionalities to the app.

It has following sub-modules:

i) **Field work monitoring module**: SmartCity-311 is a Mobile App for officers, which they use to report day-to-day field inspections for various categories/departments. This module enables them to capture a photo of the location, get GPS Information of the location, which automatically tags its respective circles and zones. Using this module, senior officers and the management team of the municipalities, can track down the progress in the field reported. The messaging / commenting system of this application enables them to make task specific communication with officers concerned about that particular issues/complaints.

ii) **GPS Attendance Module**: Using this modules, Sr. Official can track down information regarding the attendance of field staff based on GPS coordinates and the exact location and time of the staff can be known. This can be used to ascertain whether a staff has visited the area of inspection/ event place.

iii) **GPS Road Checking Module**: This is a mobile solution for field technicians and road inspectors to electronically replace paper-based information, regarding materials testing, road construction, inspection activities as well as Geotechnical investigations. This feature enables field data collection on the most handheld devices, ie. Smart phones and tablets - iPhone and Android.

iv) Project Tracking Module: **This module enables the field engineering staff to pursue and manage physical and financial progress of government projects (for e.g. Drainage or Water supply.) It's simple user interface allows to capture critical information in just a few steps.**

v) Enforcement e- Challan Module: **This module enables the field staff to file Enforcement Challans directly from their mobile device, these can be directly sent offender via SMS/ Whatsapp/ Email/ Photo. At other End Magistrate will be able to see all Challans on Mobile devices or Tablets.**

i) Variable Messaging Signs (VMS)

Large size VMS are under installation. Several VMS for traffic information/parking availability/other information's are proposed to be installed. Digital interactive information panels are also proposed to be installed. Content to be displayed on these VMS is planned to be pushed from central location and monitored.

NDMC is in process to install Digital information panels & Digital Interactive information Panels at various locations in NDMC. Through these Digital panels various online services will be delivered to Citizen.

j) **Building Plans Approval**

The Architecture of adopted solution must support implementation of end-to-end business processes as per the requirement of NDMC. Main Benefits that NDMC expects from the proposed system are:

- Applicants who seek permission or approval from NDMC for a building plan approval will be able to do so in a transparent and convenient way.
- The system will speed up the procedure of receiving and approving building plans.
- The information of the pending application at each stage will be available through the system
- It will guide the applicant about the regulations and generate scrutiny reports
- An automated system will associate documental data with Building drawings for automatic scrutiny of building proposal by reading AutoCAD® drawings. It will automate the lengthy and cumbersome manual process of checking the development regulations, thus reducing paper work, valuable time and effort of Architect Department of NDMC. It will also help in attaining the e-Governance by supplying all electronic versions of the documents and in standardizing the building drawing plan process.

k) Accounts Module (e-fin module)

l) e-Hospital

Key features of the e-Hospital application are as follows:

1. e Hospital is available to government hospitals through Software as a Services (SaaS) model.
2. Hospitals are relieved from Application & Server Management as eHospital is available on cloud.
3. Simplified on-boarding process and master data management for Hospitals.
4. Single Interface for Patients through Online Registration System (ORS) for various services.
5. Uniformity of e-Hospital Application across the all Government Hospitals.
6. e-Hospital application built using open source technology and standards recommended by Ministry of Health & Family Welfare (MoHFW).
7. e-Hospital has 16 modules, which are loosely coupled and implementable in phases.

8. NIC has empanelled roll out agencies for implementation of e-hospital/ORS/e-Blood Bank in various hospitals which will cover ICT Gap analysis, master data configuration, training, hand holding, Go-Live & Support

m) GPS devices has been installed on NDMC vehicles like Garbage trucks, C&D waste lifting trucks, water tankers and other vehicles for real time tracking of vehicles, point of interest, distance travelled, fuel consumed etc.

n) **Office Automation System (e-Office)**

I. E-File system

a. File Monitoring System (Physical as well as Electronic File).
b. Letter Monitoring System (Dispatch & Diary work).
c. Proper channel routing.
d. Tracking of physical files.

II. Employee Information system (EIS)

a. Service Record
b. Leave Account Management
c. Income Tax statement
d. Salary Slip & Form – 16, HBA Details, Loans
e. Travel & Training Management system
f. Employee Identity, Skill set, contact details, posting and location.
g. Other relevant details may be incorporated.

III. Court case management system (CCMS)

Court Case Monitoring System (CCMS) is a web based application developed in .NET Platform for monitoring of all the ongoing court cases for various departments. It generates a list of pending cases till particular date so that officers can easily refer to the list and pursue the case accordingly. This application is also accessible through the Intranet Portal only and is being used by all the departments. There are different sets of roles for users and depending upon the role of user the different option of menu will be enabled for the logged in user.

IV. Knowledge Management System (KMS)

a. To track and store Electronic documents and/or images of paper documents i.e. online repository.
b. Access to critical database for authorized users.

V. Collaboration and Messaging Services (CAMS)

a. Scheduling appointments meetings, events & conventions etc.

o) Online Booking of Yellow Fever Vaccinations.

p) Citizens can book their appointment online through this application Public Wi-Fi : NDMC has a plan to implement Citywide Wi-Fi

q) Estate License/ License fee module

r) Citizen Interactive Kiosks for Urban Service Delivery

s) Environmental Monitoring (sensor based)

t) Smart Waste Management

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.
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.

u) Operational Automation Systems for Electricity and water Bill (Commercial Department)

To serve its customers better, NDMC plans to have end to end integrated IT system in place to comply with regulatory reporting requirements and operations like Availability Based Tariff (ABT), Energy exchange, Open Access, SAIDI, CAIDI, SAIFI, CAIFI, MAIFI, CEMI, CEMSMI, Crew duration by Job etc and to meet the DERC requirements. IT Solutions for NDMC are proposed to eliminate inefficiencies from operations, so that NDMC can reduce costs and maximize the output and reliability of assets going forward. IT department, NDMC has awarded the work for implementation of Operational Automation Systems for Power, Commercial, Electricity and Other Departments of NDMC. The major modules of the project are given as under:-

- Asset Management System
- Meter Data Management
- Load Analysis System
- Energy Accounting System
- Forecast system
- Profile and settlement system (ABT)
- Billing and customer Care system
- Electric Network Management system
- Mobile Work Force Management System

Automation of NDMC Utilities :

Customer Care & Billing (CC & B):

CC&B handles every aspect of the NDMC citizen's utility lifecycle – from service connection, meter reading, rating, billing, payments processing, collections to field work. It incorporates customer relationship features such as comprehensive contact center capability, order entry, conservation program management, contract management and affinity programs. It also supports the management of new products and services that a utility may wish to market and sell to all or a defined segment of their customer base

Customer Care and Billing handles every aspect of utility Services like:

- Electricity
- Water
- Property Tax
- License

MDM: MDM (Meter Data Management) modules provide different functionality to manage meter read data for Electricity & water Consumers. Master Data Management consolidates the master data into one place to cleanse it.

WAM:

- Work and asset management information —e.g., work orders, maintenance schedules, regulatory requirements, resource availability, etc. — regardless of location or format. Oracle Utilities Work and Asset Management supports a continuous cycle of improvement and can be used use to optimize the entire asset lifecycle from planning through disposal—including all intervening acquisition, construction, maintenance, repair, and inspection activities — and can manage purchasing and inventory
- Work and Asset Management is a leading asset , work, and supply chain management application that addresses many mission-critical functions for Electricity & Information Technologies Department, GA Department, Medical Services Department.

v) Event Management-(Venue Booking, Bharat Ghar Booking and other events)

w) Birth & Death Module

x) Online Health licenses

(i) Citizens will be able to apply online for a new license
(ii) Citizens will be able to apply for the renewals online
(iii) Payment gateway will be integrated to facilitate online payments
(iv) Certificates will be generated online upon successful completion of the process
(V) Unique identification codes will be generated for the license holders
(vi) Verification of the license holders will be done through QR codes
(vii) Applicants will be able to track status online
(viii) Email and SMS integration will be done to help applicants stay informed

(ix) Less documents will be required by the citizens for license purposes

(x) Online integration will be done with other internal departments for reporting / inspection purposes

(xi) Deficiency reports will also be generated online at various levels for the citizens and the users

y) Asset Management

z) Work Asset Management

aa) Central workshop Management

bb) HRMS including pay roll and pension, Biometric Attendance

cc) REMOTE INFORMATION KIOSKS: POINTs OF DELIVERY (PODs)

i) Allowing citizens to identify locate and connect with experts for specific services.

ii) Helping experts to conduct a complete service transaction, including document sharing and printing.

iii) Enabling citizens to have personalized experiences, maintaining complete confidentiality throughout the session.

iv) Allowing for the creation of a centralized, virtual pool of experts, thereby increasing efficiency and enabling the full utilization of the available knowledge base.

v) Providing a secure and confidential setting via the remote expert kiosk (POD)

dd) Sewage Treatment Plant (STP)

a) Total STP functional location wise.

b) Water processed.

c) Water used.

d) Treated water grid on GIS map.

e) Treated water quality parameters.

f) Tagging of STP with the green area to be feed.

ee) Geographic Information System (GIS)

In the year of 2010, NDMC has created a base map of GIS with 137 several utility layers and mapped with base map of GIS platform but due to non availability of licenses Department cannot use this for edit, update, publish, query, printing etc, resulting which it cannot be properly utilized by the Departments of NDMC. For utilization of this data licenses is required. Description of present available layers as under:

Level	**Category**
Community_park.sdf	Public Utilities
Concrete_bollard_Type_1.sdf	Roads & Transport
Concrete_bollard_Type_2.sdf	Roads & Transport
Concrete_bollard_Type_3.sdf	Roads & Transport

Concrete_bollard_Type_4.sdf	Roads & Transport
Concrete_road_Signage.sdf	Roads & Transport
Double_Dustbin.sdf	Public Utilities
Electrical_Substation.sdf	Electric
Fire_Hydrant.sdf	Fire
Fire_Tank.sdf	Fire
Footpath_Land.sdf	Roads & Transport
Garage.sdf	Public Utilities
Gas_line_indicator.sdf	Utilities
Gas_line_indicator_type_2.sdf	Utilities
Gas_line_indicator_type_3.sdf	Utilities
Generator_room.sdf	Electric
Kerb_land.sdf	Roads & Transport
Letter_box.sdf	Utilities
Low_light_type_1.sdf	Electric
Low_light_type_2.sdf	Electric
Low_reflector_type_1.sdf	Signages
Low_reflector_type_2.sdf	Signages
Low_reflector_type_3.sdf	Signages
Main_Master_Manhole.sdf	Water & Sewarage
Medium_height_park_light.sdf	Electric
Metal_road_signage_type_4.sdf	Signages
Metal_signage_type_1.sdf	Signages
Metal_signage_type_2.sdf	Signages
Metal_signage_type_3.sdf	Signages
Mosque.sdf	Worship
Plot_water_main_connection_ferule_Point_id.sdf	Water & Sewarage
Boundary_wall.sdf	Others
Open_green_area.sdf	Trees & Parks
Open_step.sdf	Others

Overhead_electric_pole_440v.sdf	Electric
Overhead_Telephone_pole.sdf	Communications
Park_fencing_type_1.sdf	Trees & Parks
Park_fencing_type_2.sdf	Trees & Parks
Park_fencing_type_3.sdf	Trees & Parks
Petro_pump.sdf	Public Utilities
Primary_gate_entry.sdf	Others
Primary_road_sigange.sdf	Signages
Primary_road_sigange_Type_2.sdf	Signages
Primary_road_sigange_Type_3.sdf	Signages
Primary_road_sigange_Type_4.sdf	Signages
Primary_road_sigange_Type_5.sdf	Signages
Public_horticulture_water_outlet.sdf	Trees & Parks
Public_park_bench.sdf	Trees & Parks
Public_park_Dustbin.sdf	Trees & Parks
Public_park_Rain_harvesting_point.sdf	Trees & Parks
Rain_water_Manhole.sdf	Water & Sewarage
Rain_water_Outlet_type_1.sdf	Water & Sewarage
Rectangular_manhole_type_1.sdf	Water & Sewarage
Secondary_gate_Entry.sdf	Others
Round_manhole_600mm_Dia.sdf	Water & Sewarage
Round_manhole_900mm_Dia.sdf	Water & Sewarage
Round_street_light.sdf	Electric
Secondary_Telephone_pillar_box.sdf	Communications
Single_dustbin.sdf	Utilities
Single_dustbin_type_2.sdf	Utilities
Single_dustbin_type_3.sdf	Utilities
Speed_breaker_signage.sdf	Sinages
Street_sculpture_and_art.sdf	Roads & Transport
Survillance_System_type_1.sdf	Communications

Tall_mast_light.sdf	Electric
Tall_street_light.sdf	Electric
Tall_street_light_type_2.sdf	Electric
Traffic_Light_type_1.sdf	Electric
Traffic_Light_type_2.sdf	Electric
Traffic_Signal_Control_box_type_1.sdf	Roads & Transport
Vent_pipe_outlet.sdf	Water & Sewerage
Walking_path_type_1.sdf	Roads & Transport
Water_Harvesting_Point_Bore.sdf	Water & Sewerage
Water_main_Sluice_valve.sdf	Water & Sewerage
Water_tank.sdf	Water & Sewerage
Water_Tank_underground.sdf	Water & Sewerage

NDMC have ArcGIS licenses

Technology details given as under:

Application Server
· Xeon E5-2637v2 4 core, 3500 MHz 12 GB RAM Windows Server 2012 OS 64 bit. 1 TB HDD
· Bandwidth connectivity to Application server to be minimum of 2 Gbps
Database Server
· DBMS: Xeon E5-2637v2 8 core (2 chip) 3500 MHz 98 GB RAM Windows OS
· We recommend Active – Active High Availability configuration.
Desktop System
· CPU Speed: 2.2 GHz minimum; Hyper-threading (HHT) or Multi-core recommended
· Platform: x86 or x64 with SSE2 extensions
· Memory/RAM: 2 GB minimum
· Display properties: 24-bit color depth

·	Screen resolution: 1024x768 recommended minimum at normal size (96 dpi)
·	Swap space: Determined by the operating system; 500 MB minimum

Features:

Application Scope
Search
Queries (max 10)
Base Map gallery
Themes
Legends
Share
Around me
Info summary
Draw
Measure
Print (as per NDMC template)
Bookmarks
Online Help
Story Map (Tourism / heritage or mix-mode)
Map viewer
Home page

ff) UNIQUE SMART ADDRESSING SOLUTION FOR URBAN PROPERTIES /ESTABLISHMENTS (USASUP) IN NDMC AREA ON DESIGN, BUILD, OPERATE, MAINTAIN & TRANSFER (DBOMT) BASIS.

The Digital on site Real Time Survey should collect the following **mandatory information**:

i. Full Address including House Number, Floor Level , Building /Apartment Name Landmark near the building /establishment , Street Name/Road /lane , Sub-Locality,

Locality, nearby locality/.sub-locality, City, State, Pin Code.

ii. Meta-data to include multiple images of the property.
iii. Dwelling type (Commercial/Residential/Mixed/institutional/ recreational) civic facility unit with color coding
iv. Ownership status e.g.-Self-occupied /Rented /partly rented/ vacant
v. Number of person living in the dwelling unit/property.
vi. Civic facilities such as parks, Public Toilet Units, Garbage stations/ BQS/ Foot-Over bridges /information kiosks
vii. Type of use / kind of business / institutional activity in the property Digital Surveyed.
viii. Construction type: concrete /brick pucca structure/ steel /metal fabricated/Porta-cabin/ temporarily shed structure.
ix. Geo- coordinates- Latitude-Longitude capture for each property unit
x. NDMC circle wise Door-numbers/properties details.
xi. Calculations of distance between properties /landmark.

The Physical Door to Door Number (DDN) Digital Survey also to collect and map/link the following information with the properties Digital Surveyed:

i. Property Tax Identification Number (PTIN)
ii. Mobile Number & Aadhar number/email IDs (if available) of the residents/occupants/tenants/ managers/ caretakers
iii. Total land area of the property: which will have measurement of the plot area /individual dwelling unit area / commercial unit area / institutional unit area/ civic facility unit
iv. Electricity Connection, consumer numbers and total Number of connection
v. Water Connection consumer numbers and total Number of connection
vi. Estate License/lease number (if any)
vii. Other source of electricity e.g. Solar/DG Set.
viii. Other source of water
ix. Gas connection.
x. Petrol pumps, LPG Station, Hospitals, Hotels, cinemas, Schools, CNG Stations etc.
xi. Year of construction/redevelopment of the property /
xii. Any known litigation /dispute
xiii. License number / shop establishment/ VAT registration number
xiv. Rain -water harvesting facility
xv. In-house MSW recycling /disposal facility.

gg) Hospital Information System (HIS):

Hospital Management Information System in all healthcare institutions. It is proposed to improve the efficiency and effectiveness of the health system through cloud-based integration of existing public medical facilities. This will enable access and reduce response time to avail healthcare facilities, especially to economic weaker section of the society, through a centralized portal. NDMC has initiated to move to the NIC cloud based Hospital Management Information System (HMIS), which is the first in the country in a government setup. The software comprise of various modules making the health care delivery more efficient, like Patient Registration, Clinics, Emergency Registration, Billing & Accounts, Laboratory, Radiology/ Imaging, Picture Archiving and Communication System, IPD (Admission, Discharge & Transfer), OT Management, Pharmacy Management, Electronic Medical Records (EMR), Birth & Death Registration, Stores and Inventory, Personnel Management. This in-turn will lead to better patient care and improved outcome as well. In the first phase, few modules of the HMIS have been initiated working in Charak Palika Hospital, Palika Maternity Hospital, and Palika Health Complex since November 2015. Operationalize requisite modules in all NDMC healthcare institutions will also be made functional. All healthcare institutions would be connected through a broad band communication network.

hh) Video conferencing facility :

Video conferencing facility at NDMC Hospitals - It is proposed to set-up video-conferencing facility at Charak Palika Hospital and Palika Maternity Hospital to facilitate utilization of real-time online services of medical experts. Video conferencing facility to other NDMC offices and schools will also be started in future.

ii) Skill Training Centres:

Three Skill Training Centres will be set-up in NDMC schools for imparting future skills like 3-D printing, computer graphics and animation to the students in collaboration with National Skill Development Council (NSDC) under Pradhan Mantri Kaushal Vikas Yojna.

jj) Public bike sharing : NDMC have plan to implement Public bike sharing system for which RFP already invited. Approximately 500 bike will be provided by the Concessionaire at about 50 locations. Location of bikes can be tracked with the GPS installed in these bikes. The SI has to integrate all the reports generated and also to integrate

1.8 Technology in use by IT Department, NDMC in Data Centre.

Applications	.NET/JAVA
Data Base	ORACLE 10g
OS	RHEL 6.5
Customer care and billing ,MDM/WAM	ORACLE APP

IT Department mostly using ORACLE 10g Database. Application wise detailed description given as under:

I. Property Tax (GIS) -Application JAVA DataBase- ORACLE 10g

II. Building Plans Approval Application .NET DataBase- SQL SERVER 2005

III. Accounts Module (e-fin module) Application JAVA DataBase- ORACLE 10g

IV. Legal Module Application .NET DataBase- ORACLE 10g

V. e-Hospital Application PHP DataBase- Post grace

VI. e-office (including e-dak) Application PHP DataBase- Post grace

VII. Estate License/ License fee module Application ORACLE APP DataBase- ORACLE 10g

VIII. Billing of Electricity & Water (Commercial Department) Application ORACLE APP DataBase- ORACLE 10g

IX. Event Management-(Venue Booking, Bharat Ghar Booking and other events) Application .NET DataBase- SQL SERVER 2005

X. Birth & Death Module Application .NET DataBase- SQL SERVER 2005

XI. Health License Application PHP DataBase- Post grace

XII. Asset Management Application ORACLE APP DataBase- ORACLE 10g

XIII. Material Management& Procurement Management Application ORACLE APP DataBase- ORACLE 10g

2. Scope of the Project

2.1 Scope of Services

SI (along with its consortium partner) will be responsible to implement and maintain the Integrated Control and Command Centre (ICCC) for NDMC Smart City Programme. The scope includes software/solution development and implementation, Information Technology (IT) and required Non IT infrastructure procurement, deployment, implementation and maintenance of the ICCC system. The maintenance phase will be for a period of 5 (five) years after Go-Live. Post completion of the 5years period, the contract can be extended, at discretion of NDMC, for additional five years on yearly basis or part thereof.

SI needs to design, implement and operate the ICCC project on turnkey basis. SI 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 SI has not considered any component/service which is necessary for the project requirement, the same needs to be brought by the SI at no additional cost to NDMC.

2.2 Overview of Scope

The snapshot of scope is as below:

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

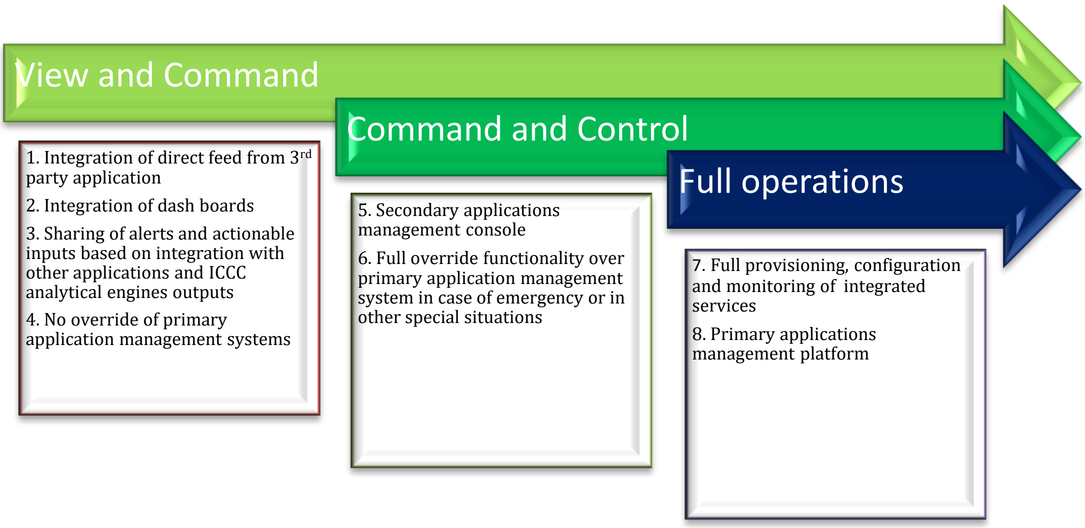
    a. Assessment of the business requirements and IT Solution requirements for the ICCC

    b. Design and build the solution for ICCC as per the Design Considerations

    c. Plan for development, configuration and customization of software products

    d. Conduct Integration test cases to achieve seamless integration with envisaged smart city systems and applications

2. **SI** will design, customize, supply, implement and maintain the ICCC software platform with integration with the following types of smart city components. These components can be classified on the basis of their respective functions:



View and Command
1. Integration of direct feed from 3rd party application
2. Integration of dash boards
3. Sharing of alerts and actionable inputs based on integration with other applications and ICCC analytical engines outputs
4. No override of primary application management systems
Command and Control
5. Secondary applications management console
6. Full override functionality over primary application management system in case of emergency or in other special situations
Full operations
7. Full provisioning, configuration and monitoring of integrated services
8. Primary applications management platform

A. SI will design, supply, install and maintain Command and Control Centre comprising of:
   a. Video Wall & controller system

   b. Integrated Command and Control Centre Application.

   c. Operator Workstation and accessories

   d. Civil Work like false floor, ceiling, ducting etc.

B. SI will be required to conduct the survey of the existing systems and accordingly define the implementation roadmap for ICCC.
   a. Assessment of the business requirements and IT Solution requirements for the ICCC

   b. Design and build the solution for 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

C. SI will design, supply, install and commission the network and backbone connectivity for ICCC.

D. SI will supply, install and maintain Infrastructure including Hardware and Application Software at ICCC.

E. SI will provide and maintain the Hardware and Software IT infrastructure services at Data Recovery Center hosted on cloud for recovering the data in case of crash of server at the ICCC.

F. SI will be required to provide Help Desk and Call Centre (with operators 24X7) in ICCC for following activities:

   a. To receive call from citizens, forwarding the same to the respective NDMC officials, updating the status to the citizens on 24X7X365.

   b. Technical and operational support of the system

   c. Maintenance of the IT and Non-IT Infrastructure

   d. Technical & Operational Manpower for smooth running of the system

   e. This help desk will also act as a functional call center to send instructions to various field agencies to do the needful.

G. SI will provide the design and area specific requirement for the Physical building for the ICCC. SI must appoint Civil Architect and Interior designer for doing a designing and defining the requirements for ICCC.

H. 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.

I. SI should present design of the ICCC using 3D modeling, which can be refined and present the final view of the actual ICCC.

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

        1. Outdoor camera
        2. Virtual Education

2.3 Detailed Scope of Work

2.3.1 Feasibility Study for finalization of detailed technical architecture and project plan

After signing of contract, the SI needs to deploy the team proposed for the project and ensure that a Project Inception Report is submitted to NDMC which should cover following minimum aspects:

a. Project Charter, Project concept understanding

b. Project Team members name with their roles & responsibilities

c. Approach & methodology to be adopted to implement the Project
d. Co-Location plan for identified services in agreement with relevant stakeholders like NDMC, and current service provider.

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

f. Establish and measure resource assignments and responsibilities

g. Highlight the milestones and associated risks

h. Responsibility matrix for all stakeholders

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

j. Measure project deadlines and performance objectives.

k. Detailed Project Plan, specifying dependencies between various project activities / sub-activities and their timelines.

l. 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. Proposed revision to planned schedule provided such revision is necessitated by reasons beyond the control of SI
iv. Support needed
v. Highlights/lowlights
vi. Issues/Concerns
vii. Risks/Show stoppers along with mitigation

m. Identify the activities that require the participation of client personnel (including NDMC), and communicate their time requirements and schedule early enough to ensure their full participation at the required time.

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

2.3.1.1 Requirement Gathering Stage

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

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

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

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

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

e. SI must get the sign off from user groups formed by NDMC.

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

g. NDMC 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.

h. SI will prepare interoperability traceability matrix with third party systems (existing legacy systems with ICCC) in consultation with NDMC 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.

2.3.1.2 Design Stage

The SI shall design and build the solution for ICCC as per the Design Considerations detailed in RFP document. The solution proposed by SI should comply with the design considerations requirements as mentioned therein.

2.3.1.3 Development Phase

The SI shall carefully consider the scope of work and provide a solution that best meets the proposed ICCC requirements. Considering the scope set in this RFP, the SI shall carefully understand the various prevailing Smart City individual solutions which are currently under implementation and envisaged in near future under the Smart City Programme of NDMC 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 SI proposes software products the following need to be adhered:

   i. SI shall be responsible for supplying the application and licenses of related software products and installing the same so as to meet ICCC requirements.

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

   iii. The SI 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 SI shall report any exceptions to license terms and conditions at the right time to NDMC. However, the responsibility of license compliance solely lies with the SI. Any financial penalty imposed on NDMC during the contract period due to license non-compliance shall be borne by SI.

   iv. SI shall also supply any other tools & accessories required to make the integrated solution complete as per requirements. For the integrated solution, the SI 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 NDMC
    - Quality assurance procedures
    - Change management histories
    - Version control data
    - SOPs, procedures, policies, processes, etc. developed for NDMC
    - 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 NDMC.

b. Bespoke (Custom Developments)

i. The successful SI shall identify, design and develop the customization for components/functionalities that are required to address the requirements mentioned in this RFP.

ii. The SI shall supply the following documents along with the developed components:

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

2.3.1.4 Integration & Testing Phase

The Command and Control Centre Software at ICCC should be integrated with data feeds of the following Smart City systems envisaged under the Smart City Programme of city.

a. Smart LED Street Lights

b. Sensor Based & Camera Based Smart Parking

c. Water- SCADA & Water Meter

d. Electricity – SCADA & Electricity Meter

e. Property Tax (GIS)

f. Smart Classroom

g. CCTV

h. App NDMC311

i. Variable Messaging Signs (VMS)

j. Building Plans Approval

k. Accounts Module (e-fin module)

l. Legal Module

m. e-Hospital

n. GPS

o. e-office (including e-dak)

p. Public Wi-Fi

q. Estate License/ License fee module

r. Citizen Interactive Kiosks for Urban Service Delivery

s. Environmental Monitoring (sensor based)

t. Smart Waste Management

u. Billing of Electricity & Water (Commercial Department)

v. Event Management-(Venue Booking, Bharat Ghar Booking and other events)

w. Birth & Death Module

x. Health License

y. Asset Management

z. Material Management& Procurement Management

aa. Central workshop Management

bb. HRMS including pay roll and pension, Biometric Attendance

cc. STP

dd. Public Bike Sharing

ee. 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 by NDMC.

Broadly there are four kinds of data feed possible from all of the above systems. The software solution provided by SI 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, GPS Co-ordinates of vehicles, Alert messages, ITMS, Smart Pole ICCC
Voice Call	Calls from Call center, IVRS System.

The SI 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.

2.4 Integration Capabilities

1) The ICCC will aggregate various data feeds from sensors and systems and further process information out of these data feeds to provide interface /dashboards for generating alert and notifications in real time.
2) The ICCC would also equip city administration to respond quickly and effectively to emergency or disaster situation in city through Standard Operating Procedures (SOPs) and step-by-step instructions. The ICCC shall support and strengthen coordination in response to incidents/emergencies/crisis situations.
3) Single Dashboard for City Infrastructure Management & Smart City Services for Smart Lighting, Utility/Surveillance System, GIS Services and Other Services of Authority work visualized real time on 2D/3D map of City. This dashboard can be accessed via web application as well as mobile app. The various information that may be accessed from the system but not limited to are as below:
    - Visual alerts generated by any endpoint that is part of the city infrastructure e.g. Surveillance cameras, City lights or any other sensors that manages various city management use cases.
    - Access information of water management resources
    - Information about waste management resources
    - Various citizen services e.g. Land records, Municipality tax, billing etc.
    - City environmental data
    - Take action based on events generated by any city infrastructure device
4) The system shall provide reporting & audit trail functionalities to track all the information and monitor operator interactions with the system and to impart necessary training to the users
5) Below are Brief of Scope for Integration; (The scope is illustrative and not exhaustive)

S. No.	List of Services	Brief Scope for Integration (Scope is only illustrative and non-exhaustive)
1)	Smart LED Street Lights/Smart Poles	a) The ICCC should aggregate various data feeds from light sensors and systems further process information out of these data feeds to provide interface /dashboards for generating alert and notifications in real time. b) Provide single dashboard/reports of various brand of lighting solution. c) ICCC should support lighting control like diming, switch on/off, group/individual control etc. d) Various reports can be generated like non-working lights in a given time frame. e) Integration with GIS map with analytic layer. Developing heat map to identify areas which needs systematic improvement. f) Existing SCADA system for non Smart Street Light till they are upgraded.
2)	Sensor Based & Camera Based Smart Parking	a) Consolidates all city parking information onto a single operations platform. b) 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 be required get video feeds from the parking areas on real-time basis on requirement basis. These video feeds will help monitor assets of NDMC. All the information received will be required to be mapped on the GIS map. All the information received from the Smart Parking command centre will go into the Analytical layer which will help city in better planning and running of operations. ICCC should be able to trigger the commands/alerts (if required)to the respective command centre. c) Should provide parking availability, revenue collection information on dashboard, received from various sources on real time basis. d) The platform should be able to integrate any type of parking sensor irrespective of the technology used. For example, some parking sensors might use RF technology like LoRa or ZigBee to communicate the data and events, some might use GPRS or some might use Wi-Fi. Some parking sensors might use infra-red based detection, some might use magnetic field based detection or combination of the both where as some might use a video camera to detect parking occupancy. Irrespective of the technology, the platform should be able to integrate with these devices and their software managers and provide the data from such devices in a normalized and standard based data models. Viewing of CCTV feed of parking lots. e) Integration with GIS map with analytic layer. f) Data from non-Smart Parking to be integrated.
3)	Water- SCADA & Water Meter	a) The Water SCADA should be integrated into ICCC via web services (REST or SOAP) b) The data exchange format should be JSON/XML c) ICCC uses an Adapter(WSO2) for consuming the web services from SCADA application d) ICCC Integration Engine stores auth and other historic data for generating reports e) ICCC initially makes call to get the authentication tokens for calling web services

S. No.	List of Services	Brief Scope for Integration (Scope is only illustrative and non-exhaustive)
		f) MIS Details of following are integrated viz., - Total Commercial Users– DJB–inlet points water received - Total Domestic Users - Total Flat Rate Users - Total Water Users - Total Demand Raised for a month– Variation in water received - Total Payments Collected Today - Total Payments Collected this month - Total Pending Payments - Season wise trends of water usage– supply - Projected Demand - Area wise water demand/usage - Peak Water Usage Days in a week/month - NRW reports - Water received from DJB at all inlet points, variation in quantity at each inlet point. Specific customers on a real time basis to monitor actual uses of water g) KPIs on Demand vs Supply, Expected Collection vs Actuals Collected h) Integration with GIS map with analytic layer. i) Tagging of consumers, house hold, alternate sources of water
4)	Electricity – SCADA & Electricity Meter	- The Electricity SCADA should be integrated into ICCC via web services (REST or SOAP) - The data exchange format should be JSON/XML - ICCC uses an Adapter(WSO2) for consuming the web services from Electricity SCADA application - ICCC Integration Engine stores auth and other historic data for generating reports - ICCC initially makes call to get the authentication tokens for calling web services - MIS Details of revenue Collection, Power Management, Usage, Peak Usage, Demand vs Distribution location wise should be integrated into the dashboard - MIS details of following are integrated into Dashboard viz., - Total Commercial Users - Total Domestic Users - Total Flat Rate Users - Total Electricity Users - Total Demand Raised for a month - Total Payments Collected Today - Total Payments Collected this month - Total Pending Payments - Season wise trends of electricity usage - Projected Demand - Area wise electricity demand/usage - Peak Electricity Usage Days in a week/month j) KPIs on Demand vs Supply, Expected Collection vs Actuals Collected k) Integration with IPDS software. l) Integration with GIS map with analytic layer.

S. No.	List of Services	Brief Scope for Integration (Scope is only illustrative and non-exhaustive)
5)	Property Tax (GIS)	a) The Property Tax module should be integrated into ICCC via web services (REST or SOAP) b) The data exchange format should be JSON/XML c) ICCC uses an Adapter(WSO2) for consuming the web services from Property Tax application d) ICCC Integration Engine stores auth and other historic data for generating reports e) ICCC initially makes call to get the authentication tokens for calling web services f) ICCC makes calls to get the required data from Urban Local Bodies (ULB) viz., City Corporation, City Municipal Council, Town Municipal etc., g) ICCC expects the following services viz., Property Details per Location, h) ICCC displays the analytical information of property tax collections across the NDMC bodies in a GIS map I. All the below services can be integrated into ICCC II. Create New Property-ID III. Get Property details- Size, address, year of construction IV. Get Property Bill V. Make Payment VI. Get Receipt i) Following reports can be displayed on ICCC, if required I. Demand / Collection Register II. Assessment Register III. Ward-wise / Zone-wise Recovery reports IV. Top Defaulters Report with respect to time and value V. Occupancy wise / Flat wise report' VI. Tax-wise Recovery Details VII. Tax-wise Demand Details VIII. Advance Payment Reports IX. Objection / Hearing Details j) Integration with GIS map with analytic layer. k) Online Mutation
6)	Smart Classroom	a) The Smart Classroom should be integrated into ICCC via web services (REST or SOAP) b) The data exchange format should be JSON/XML c) ICCC uses an Adapter(WSO2) for consuming the web services from Smart Classroom application d) ICCC Integration Engine stores auth and other historic data for generating reports e) ICCC initially makes call to get the authentication tokens for calling web services f) MIS Details of reports on Classroom viz., location, facilities, components and their status should be integrated into the dashboard, active/inactive, usages duration and pattern. Usage pattern to be co-related with the school time table and with user ID's and generate report. g) Connect class with ICCC for the purpose of data uploading/downloading. h) Overall implementation vs. current status details of Smart Classrooms

S. No.	List of Services	Brief Scope for Integration (Scope is only illustrative and non-exhaustive)
		should be integrated into Dashboard i) CCTV analytics–server details about j) MIS reports of education k) Integration with GIS map with analytic layer.
7)	CCTV	a) ICCC will receive feeds of CCTV existing cameras and new cameras on real time basis. ICCC will integrates with existing cameras and new cameras. Should support multiple video sources from multiple locations. Platform should have no limitation in displaying the number of CCTV video sources. b) Integrate and assess inputs from different sources such as CCTV, Video Analytics, and sensors further to assist with actionable intelligence. Push the video feed to police control room. c) Should use dynamic channel coverage specifically for video stream function for efficient bandwidth usage for multiple Remote Control center d) Display module should have capability to control multi-screened display wall in sync with operator console e) Should support Fixed type and PTZ camera. Control PTZ function from the screen to control the camera but with changing tile configuration each camera should be viewed with much lower resolution. f) The system should dynamically reduce the bit rate and bandwidth for each stream based on the viewing resolution at the remote location. g) Integration with GIS map with analytic layer. h) Should also be able to trigger the commands/alerts (if required)
8)	NDMC Mobile App both Intra NDMC & Public App	a) Provides unified northbound API to abstract diverse sensors and its attributes by single northbound API to allow interfacing and integration with existing systems. b) 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. c) Provides Query-based language to access sensor parameter from sensor cloud d) Provides mechanism to translate and map business logic to sensor functionality e) Integration with GIS map with analytic layer and generate analytics with respect to complain time, area, time of resolution. f) Generate intelligence w.r.t field inspection, ongoing projects etc.
9)	Variable Messaging Signs (VMS)	The VMS system should be integrated into ICCC via web services (REST or SOAP) The data exchange format should be JSON/XML ICCC uses an Adapter(WSO2) for consuming the web services from VMS application ICCC Integration Engine stores auth and other historic data for generating reports ICCC initially makes call to get the authentication tokens for calling web services From Dashboard a message can be sent via API POST call to VMS System Any data of VMS system can be got via the service Integration with Existing–3 Nos; new–5 Nos; markets, digital interactive panels-75 Nos.) Centralized management of VMS

S. No.	List of Services	Brief Scope for Integration (Scope is only illustrative and non-exhaustive)
		Content management of VMS Security of the content to be displayed on VMS Integration with GIS map with analytic layer.
10)	Building Plans Approval	a) The building plans approval system should be integrated into ICCC via web services (REST or SOAP) b) The data exchange format should be JSON/XML c) ICCC uses an Adapter(WSO2) for consuming the web services from Building Plans approval application d) ICCC Integration Engine stores auth and other historic data for generating reports like applications received, disposed, pending area wise receipts etc. e) ICCC initially makes call to get the authentication tokens for calling web services f) MIS Details of buildings, registered and unregistered, demand should be integrated into the dashboard. g) Integration with GIS map with analytic layer.
11)	Accounts Module (e-fin. module)	a) The Accounts module should be integrated into ICCC via web services (REST or SOAP) b) The data exchange format should be JSON/XML c) ICCC uses an Adapter(WSO2) for consuming the web services from Accounting application d) ICCC Integration Engine stores auth and other historic data for generating reports e) ICCC initially makes call to get the authentication tokens for calling web services f) Details of Financial Transactions, KPIs should be integrated into the dashboard g) This module get MIS data from other systems viz Payroll, Property Tax, Estate, other sundry earnings for which receipt is generated. Trade License etc for integration onto dashboard h) Also integrates details on reconciliation, budgeting vs usage and other key MIS information
12)	Legal Module	a) The Legal module should be integrated into ICCC via web services (REST or SOAP) b) The data exchange format should be JSON/XML c) ICCC uses an Adapter(WSO2) for consuming the web services from legal module application d) ICCC Integration Engine stores auth and other historic data for generating reports e) ICCC initially makes call to get the authentication tokens for calling web services f) ICCC should integrate with Legal Module to get MIS information details numbers on legal cases g) ICCC dashboard should integrate MIS details of daily board register, cases whose PWR is due to be furnished h) MIS details of Cases whose judgment implementation is due i) MIS details of Cases whose CA's are due to be filed, Next Date Of Hearing (NDOH) j) Status of Lawyer's fees. k) Integration with GIS map with analytic layer.

S. No.	List of Services	Brief Scope for Integration (Scope is only illustrative and non-exhaustive)
13)	e-Hospital	a) The e-Hospital system should be integrated into ICCC via web services (REST or SOAP) b) The data exchange format should be JSON/XML c) ICCC uses an Adapter(WSO2) for consuming the web services from e-Hospital application d) ICCC Integration Engine stores auth and other historic data for generating reports e) ICCC initially makes call to get the authentication tokens for calling web services f) and get following MIS details from e-Hospital system viz., Facilities, Specialties, Expertise Wards in/out patient, Case Reports Numbers, Financials g) Following MIS reports should be integrated into Dashboard viz., m) Total New Patient Registration – Overall n) Total New Patient Registration – Hospital wise o) Total Revisited Patients Today – Overall p) Total Revisited Patients Today - Hospital wise q) Total Vaccination Registration Summary (by type)– Today r) Total Vaccination Registrations Till Date s) Total Vaccinations based Revenue Collected Today t) Total Vaccinations based Revenue Collected Till Date h) Any Alerts and Notifications in case of any epidemics should be shown in ICCC i) ICCC should also integrate Case Reports and Other information into City Dashboard j) Medicines distributed inventory,integration of all module of e-hospital (Pharmacy module, lab module, OPD/IPD/online registration, students and employees heath data integration.) k) OPD of each hospitals, dispensaries l) Login details of doctor’s day/month/year and patient attended. m) Integration with GIS map with analytic layer. n) Yellow fever integration.
14)	GPS	a) ICCC should integrate with Vehicle tracking of garbage vehicles, C&D Waste, mechanical road sweepers, water tankers and other municipal vehicles. b) Actionable alerts on vehicle breakdown, route deviation, missing point of interest etc. c) Summary of distance traveled by each vehicle, point of interest, route deviation. d) Integration with GIS map with analytic layer.
15)	e-office (including e-dak)	a) The e-office management should be integrated into ICCC via web services (REST or SOAP) b) The data exchange format should be JSON/XML c) ICCC uses an Adapter(WSO2) for consuming the web services from Material management application d) ICCC Integration Engine stores auth and other historic data for generating reports e) ICCC initially makes call to get the authentication tokens for calling web services f) All MIS data like file tracking, Dak tracking, personnel management etc from e-office modules should be integrated into ICCC

S. No.	List of Services	Brief Scope for Integration (Scope is only illustrative and non-exhaustive)
		g) Following MIS reports integrated into dashboard viz., (Aadhar based bio-metric attendance integration) - Total Registered Employees - Total Active Employees - Total Employees Present today - Total Devices - Devices Status
16)	Public Wi-Fi	a) ICCC should integrate with Wi-Fi solution and project real time user information like available bandwidth and usages ofbandwidth, total data consumed on city dashboard b) Integration with GIS map with analytic layer.
17)	Estate License/ License fee module	a) The Estate License management should be integrated into ICCC via web services (REST or SOAP) b) The data exchange format should be JSON/XML c) ICCC uses an Adapter(WSO2) for consuming the web services from Estate License application d) ICCC Integration Engine stores auth and other historic data for generating reports e) ICCC initially makes call to get the authentication tokens for calling web services f) MIS data to be integrated into Dashboard viz., Vacant properties for auction - Licenses issued today/week/quarter/year wise - New application received /disposal/timelines - Pending Licenses for issuance - Area wise trend on new license, pending dues/pending renewals/pending transfers, issuance, pending - Revenue Generated today - Projected Revenue this month - Allotment Transfers done in a week/month/year - Revenue split of stalls, shops office space, commercial premises-hotels, restaurants - Comparison of per unit license rate of similar properties - Licenses expiring in coming week/month/quarter. - Payment status due/paid resumed licenses pending renewal applications. - Alerts on vacant premises/shops, outstanding dues - Integration with GIS map with analytic layer.
18)	Citizen Interactive Kiosks for Urban Service Delivery	a) Interface with Citizen Interactive Kiosks for multi-services Urban Service. b) Provide APIs for integration of citizen services c) Manage and Control Kiosk content with a Content Management System login user details, services accessed, breakdown alerts. d) Integration with GIS map with analytic layer.

S. No.	List of Services	Brief Scope for Integration (Scope is only illustrative and non-exhaustive)
19)	Environmental Monitoring (sensor based)	a) Monitor key inputs from city environmental sensors like Temperature, Humidity, CO, CO_2, NO_2, SO_2, PM_{10}, $PM_{2.5}$, b) Create awareness within the city based on dynamic inputs received from sensors and display output to various interfaces including city application, multi-services c) Integration with GIS map with analytic layer.
20)	Smart Waste Management	a) Monitoring of the smart waste management system web application real-time level information for containers as well as the automatic warning system which notifies when containers require attention. b) GIS based Real-time monitoring of solid waste collection vehicles. c) Geo tagged bins whether cleaned or not through GPS on vehicles, in case sensors are on C&D Waste. d) Log calls/jobs on the helpdesk database utilizing helpdesk software (inquiries may be received by telephone, facsimile, email or in person). e) Track progress of waste management service requests against pre-determined KPIs. f) Maintain asset information held in the helpdesk database. g) Update site specific waste management files and other documentation for helpdesk compliance. h) Integration with control room complaints and GIS map with analytic layer.
21)	Billing of Electricity & Water (Commercial Department)	a) Communicate locations of personnel, equipment, outage information from Electricity system. b) Integrate with MIS reporting system c) Utilize the IoT system to monitor system statistics. d) Perform IoT operations as required by line personnel. e) Reports & Analytics on Electricity & Water Bill Collection, Drill down reports on Area wise Collection. Targeted Collection vs Current Collection, Water/Electricity Supply vs Demand Analysis f) KPIs on water and electricity supplied vs demand and consumed and the bill collection
22)	Event Management-(Venue Booking, Bharat Ghar Booking and other events)	a) Maintain asset information in the database using GIS and ERP system. b) Provide interface to mobile app for venue booking c) Provide MIS reports & analytics on - Venue location demand - Assets at venue - Venue assets/facilities usage - Venue capacity - Venue occupancy - Bookings per day/month - Venue Peak booking days in a week/month, - Venue peak booking times - Bookings Revenue per day/month per venue - Booking Trends seasonal/festivals/monthly - Intelligent analytics based of previous year uses, important days
23)	Birth & Death Module	a) Integrate the portal for displaying birth and death data via APIs b) Integrate with master data and other modules for information validity c) MIS Reports on Birth/Death information per location/age/gender etc.

S. No.	List of Services	Brief Scope for Integration (Scope is only illustrative and non-exhaustive)
		viz., - Online Birth Certificates printed today - Online Death Certificates printed today - Total Birth Certificates printed - Total Death Certificates printed - Birth Registrations – Today, period- between dates. - Birth Registrations – Total - Death Registrations – Today, period- between dates. - Death Registrations – Total - Re-print requests per day/month - Verification requests per day/month - Pending Certificates issuance - Location/Hospital wise birth/death registrations/Issue status - Age group wise death registrations - Gender wise birth/death registrations d) Analytics on Population vs Birth/Death e) KPI's on birth and death certificate issuance by location per location f) Integration with GIS map with analytic layer.
24)	Health License	a) The Health License management should be integrated into ICCC via web services (REST or SOAP) b) The data exchange format should be JSON/XML c) ICCC uses an Adapter(WSO2) for consuming the web services from Health License application d) ICCC Integration Engine stores auth and other historic data for generating reports e) ICCC initially makes call to get the authentication tokens for calling web services f) MIS data on Health licenses added day/week/quarter/year wise from various locations should be integrated to ICCC g) Integration with GIS map with analytic layer. h) Licenses applied /issued/suspended/revoked/expired/ renewal cancelled period wise(date/week/month/year)
25)	Asset Management	a) The Asset management module should be integrated into ICCC via web services (REST or SOAP) b) The data exchange format should be JSON/XML c) ICCC uses an Adapter(WSO2) for consuming the web services from Asset Management application d) ICCC Integration Engine stores auth and other historic data for generating reports e) ICCC initially makes call to get the authentication tokens for calling web services f) MIS Details on procured assets, material details, and financial impacts on the assets, assets under maintenance, asset categorization, asset usage should be integrated into the dashboard g) Integration with GIS map with analytic layer.
26)	Material Management & Procurement Management	a) The Material management should be integrated into ICCC via web services (REST or SOAP) b) The data exchange format should be JSON/XML c) ICCC uses an Adapter(WSO2) for consuming the web services from Material management application

S. No.	List of Services	Brief Scope for Integration (Scope is only illustrative and non-exhaustive)
		d) ICCC Integration Engine stores auth and other historic data for generating reports e) ICCC initially makes call to get the authentication tokens for calling web services f) ICCC should integrate MIS details on Material supplied, material requirements, material usage by location/by asset and other details viz., Financials g) The Procurement management should be integrated into ICCC via web services (REST or SOAP) h) The data exchange format should be JSON/XML i) ICCC uses an Adapter(WSO2) for consuming the web services from Procurement management application j) ICCC Integration Engine stores auth and other historic data for generating reports k) ICCC initially makes call to get the authentication tokens for calling web services l) ICCC should integrate with MIS reports/data tenders published yearly/quarterly, Tender Type wise published, Category wise of tenders along with split up of Works, Services, Goods
27)	Central workshop Management	a) The Central Workshop management should be integrated into ICCC via web services (REST or SOAP) b) The data exchange format should be JSON/XMl c) ICCC uses an Adapter(WSO2) for consuming the web services from Material management application d) ICCC Integration Engine stores auth and other historic data for generating reports e) ICCC initially makes call to get the authentication tokens for calling web services f) ICCC Integrates key MIS reports on workshop by location, asset details by workshop g) Integration with GIS map with analytic layer.
28)	HRMS including pay roll and pension, Biometric Attendance	a) The HRMS should be integrated into ICCC via web services (REST or SOAP) b) The data exchange format should be JSON/XML c) ICCC uses an Adapter(WSO2) for consuming the web services from HRML application d) ICCC Integration Engine stores auth and other historic data for generating reports e) ICCC initially makes call to get the authentication tokens for calling web services f) ICCC should integrate the MIS details of Payroll, Employee Wise Pay Summary, Department/Section wise, PF/CPF
29)	Sewage Treatment Plant (STP)	a) Total STP functional location wise. b) Water generated. c) Water used. d) Treated water grid on GIS map. e) Treated water quality parameters. f) Tagging of STP with the green area to be feed.

S. No.	List of Services	Brief Scope for Integration (Scope is only illustrative and non-exhaustive)
30)	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. These video feeds will also help monitor assets of NDMC. 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 NDMC.

Note: (i) Water Scada will be stationed at the proposed ICCC location.

(ii) Sufficient storage space shall be kept in Data Center for power scada.

2.4.1.1 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 NDMC Smart City. 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.

2.4.1.2 Go-Live Preparedness and Go-Live

a. SI shall prepare and agree with NDMC, the detailed plan for Go-Live which should be in-line with NDMC ’s implementation plan as mentioned in RFP.

b. The SI shall define and agree with NDMC, the criteria for Go-Live.

c. The SI shall ensure that all the system integration is done with existing systems.

d. SI shall submit signed-off UAT report (issue closure report) ensuring all issues raised during UAT are being resolved prior to Go-Live.

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

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

2.4.2 Design, Supply, Installation and Commissioning of IT infrastructure at ICCC

The SI shall be responsible for procurement, supply and installation of entire ICT hardware and software infrastructure at the Command and Control Centre for successful operations of the systems. The ICT infrastructure includes servers, storages, back up, networking, load balancers, 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. SI 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 NDMC.

d. SI 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 SI shall not use the same for any other purpose.

g. The ownership of ICT infrastructure shall get transferred to NDMC after "Acceptance and Go Live" of such items by NDMC.]

h. SI to ensure warranties/AMCs are procured for all the hardware components for entire duration of the project i.e. 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.

1. Following are the benchmark requirements which the SI 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 at ICCC, and connectivity of individual centers with ICCC.

c. Application Integration Services within ICCC building premises

- Indoor CCTV Cameras would be required to be installed to monitor the physical access of the system from remote location
- 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 Project.

f. Physical infrastructure components such as UPS, Units, Power, and cabling for power and data connectivity, etc.

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".

i. All IT equipment models offered should be latest released with bundled version update.

j. Seamless Integration with other Smart City Systems and applications

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 NDMC.

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.

o. SI has to provide the remote licenses for all HOD's and other senior officer to see the ICCC from remote location.

p. SI shall also provide chatting tool/software for communication.

2. The SI shall provide system integration services to customize and integrate the applications procured. The ICCC application proposed by the SI 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 SI bidder will be approved by NDMC 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
- Database Server
- Backup Server
- Domain Controller
- Failover Servers for application Servers
- Virtualization software (wherever applicable)
- Any other Server required to the cater to the scope of work mentioned in this

ii. Application & System Software

- Enterprise Integrated Command and Control Centre Software
- Enterprise Management Software (EMS)
- 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 & Secondary and Storage Management Solution
- Blade Chassis
- Core and Access Switches
- WAN Services Routers
- KVM Switches
- Security Solution Live Firewall, IPS, Anti APT
- Racks
- IP Phones

- 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 SI.

4. The SI 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 NDMC . The detailed plan shall be also comprising of the scalability, expandability and security that such data centre will implement under this project.

5. The SI 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. UPS

   xv. Furniture and fixtures

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

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

2.4.3 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.

2.4.4 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 NDMC smart city projects.

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.)

2.4.5 Helpdesk and Call Centre

a. SI will be required to provide Help Desk cum Contact center in 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.

Work flow for call centre

- Receive call at call centre. Input complainant data into the system.
- Enter the nature of compliant & other details.
- Fire priority of complaints.
- Auto assign the complainant to concerned officer through Geo tagging.
- Complainant get complaint number and assignment status.
- After assigning of complaint the complainant can check the status, if the complaint is forwarded/pending with officer/resolved.
- Complainant can also get notification of each step.

2.4.6 Disaster Management

SI 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 NDMC. 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.

2.4.7 Integration of GIS Properties Platform

NMDC has prepared a GIS application for providing NDMC area information. The SI should be able to integrate these GIS layers on user interface of command and control software application.

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

2.4.8 ICCC Data Centre

The SI shall be responsible for establishing state of art in-premises data center for ICCC including design, procurement, supply and installation of entire ICT hardware and software infrastructure at the Data Centrefor successful operations of the. The Data Center will be planned considering the below factors:

a. Data Center should be minimum Tier 3+ as per the Uptime Institute/ EIA-TIA 942standards.

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. SI 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 NDMC.

e. SI shall optimize procurement of ICT infrastructure i.e. the equipment shall not be procured earlier than its requirement.

f. Virtualization technologies to be used to reduce the physical space required for hosting

g. ICT infra deployed for ICCC should be dedicated for the project and SI shall not use the same for any other purpose.

h. The ownership of Data Centre shall get transferred to NDMC after "Acceptance and Go Live" of such items by NDMC/ NDMC appointed TPAs.

i. SI to ensure warranties/AMCs are procured for all the hardware components for entire duration of the project including O&M Phase (1+5years). 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.

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

k. In the Data Center SI should provide dedicated blade chassis space for the ICCC Infrastructure.

l. Data Center should be as per Telecommunications Infrastructure Standard for Data Center and should be Certified 27001.

m. Access to the Data Center Space where the ICCC Infrastructure is hosted should be demarcated and physical access to the place would be given only to the authorized personnel.

n. Indoor CCTV Cameras would be required to be installed to monitor the physical access of the system from remote location

o. 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.

p. Networking & Security Infrastructure and other associated IT Components.

q. Following are the Key Infrastructure Elements of the Data Centre

  - Servers (inclusive of OS)
    - Application Servers
    - Database Server
    - Enterprise Backup Server
    - Domain Controller
    - Failover Servers for application Servers
    - Any other Server required to the cater to the scope of work mentioned
  - 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
    - Customized Software to cater to requirements of Project Requirements
  - 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

2.4.9 Data Backup

Periodic Data Backup Plan Update

The service provider shall be responsible for –

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

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

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

The SI should then obtain ISO 27001 certification for all the ICCC centre within 2 quarters of Final Acceptance Test. Payment from 3rd Quarter onwards shall be withheld till this certification is obtained by the SI.

2.4.11 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. NDMC 's employees
   b. NDMC Smart City Limited's employees
   c. Stakeholder departments

2. The SI'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 SI has to provide cost for additional and optional training sessions in its commercial proposal in case more training's are required. SI has to conduct such additional training sessions on NDMC 's request.

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

6. SI will get the Training and capacity building strategy including training material finalized with NDMC before starting the training programs.

7. SI 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 NDMC 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 ICCCmodules

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

8. SI 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 NDMC.SI has to ensure the following points:

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

    b. The contents developed shall be the property of NDMC with all rights.

9. There are estimated 100 users who need to be trained. SI may accordingly plan the training budget.

10. SI 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 SI 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 NDMC.

11. 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 NDMC for each training session.

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

13. 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.

2.4.12 Smart City Surveillance

2.4.12.1 Functional requirement of City Surveillance

The City Surveillance System shall manage video feeds for all CCTV systems required under this project through Video Management System (VMS) application hosted at Command and Control Centre or sub-command and control centre. Proposed VMS should support 10000 Cameras in design from day1.

This organization requires an integrated security solution that includes a command and control style operator console; a open source (like Linux) based video management software system, standard and high definition IP-based cameras, and system should meet the following requirements.

The Video Surveillance System should intend to effectively monitor all the critical operational areas of the locations. The broad objectives of the Video Management System are as follows:

a) Access points monitoring with Motion Detection Alarms

b) Coverage for detection of any intrusion of defined areas

c) Enhancement of operational control by covering critical areas

d) Recording of camera outputs for analyzing critical events. Concessionaire shall provide recording solution at 15FPS of 2MP for day as well as night. Proposed application should support for back-up.

e) Any such other requirement

The Video Surveillance System should provide effective Security & surveillance of an area as well as creating a tamper proof record for post event analysis. The Surveillance System shall provide an on-line display of video images on monitors at local security control room, Command and Control Center, police stations and at any other place as defined for large locations as per requirement.

System should design to monitoring CCTV cameras from multiple locations, minimum monitoring locations will be approx. 5 locations. System should also have capability to group the cameras as per NDMC requirement for each location. If at any stage the CCTV online data is required to be connected to Police Station, the concessionaire will connect it to the Police Station in NDMC area.

Storage of CCTV data to be planned for 30 days.

2.4.12.2 Technical Specifications of City Surveillance

2.4.12.2.1 Video Management System

General Requirements

a) The surveillance system shall provide a scalable and reliable platform to enable customized, network-based surveillance applications.

b) The surveillance system shall be open standard supporting multiple vendor IP cameras and encoder manufacturers within the same system. The system shall support integration of ONVIF compliant cameras.

c) The system shall support digital pan-tilt-zoom on live video. PTZ cameras should allow operators to use PTZ controls to zoom to a specific region in the viewing pane. Operators should select part of the full image and perform the PTZ controls within that region.

d) The surveillance system viewing system should be in thick client for local viewing and thin client through http browser for remote viewing. Both thin and thick client shall provide the capability of viewing single or multiple live and archive cameras, control PTZ camera.

e) VMS Review Player should support stand-alone Windows utility that plays video archive clips without a browser. The Review Player should also support MP4 files into a tamper-proof MPX (tamper proof MP4 file formats) formats. MPX file should include a password that is entered when the file is created. Application should ask the password to open and view the video file.

f) VMS application should be a mobile application for Android & Apple devices such as the iPad and iPhone. App features should include recorded video playback, thumbnail video preview, and user profiles that allow multiple users to share a single device.

g) The proposed surveillance system can be supported by the existing network infrastructure

h) The System shall support the scalability of additional camera installation beyond the originally planned capacity. One single Video Management system shall be expandable up to 10,000 cameras.

i) The proposed video management system shall support deploying the software on Virtual servers, so that the hardware requirement can be reduced for this project.

j) The system shall have capability to stream video at remote sites by optimizing the bandwidth on WAN.

k) The System should support automatic discovery and configuration, when any camera connect to network, the switch should recognizes the camera as a video endpoint, and then uses Smart Port macros to set the right network parameters for the video stream on the network.

l) The system should allow users to access video streams from remote locations that have limited outbound bandwidth. The video should be delivered to multiple users without placing additional load on the remote locations.

m) The System should support Maps integration in future with below features;

   i. Adding Image Layers to the location map.

   ii. Define the location map for each location.

   iii. Add cameras to the map images.

   iv. Add image layers to the map.

   v. Add a Maps Server

   vi. System should support raster format images of jpeg/jpg and png file and Vector (shape files)

n) Video Surveillance Storage System – The video surveillance storage system should support multiple options to store video. Servers, Direct Attached, shall augment server internal storage. The video surveillance storage system shall store video in loops, one-time archives, or event clips triggered by alarm systems. It shall support for RAID 6 storage.

o) The system shall provide for integration with other software applications through an open and published Application Programming Interface (API). Such applications shall include, but not be limited to, access control, video analytics, and other alarm and sensor inputs.

p) The system should ensure that once recorded, the video cannot be altered; ensuring the audit trail is intact for evidential purposes.

q) All camera recordings shall have camera ID and location or area of recording and shall be programmable by the system administrator with user ID and password.

r) System shall support camera template to define the resolution, frame rate, recording duration, and then apply to a group of cameras. The modification of the template will be reflected to all the cameras under the template.

s) The system shall supports Bulk Action to allow to search and perform administration activities on multiple camera.

t) The system shall support Bulk import of cameras from file such as excel/.csv, or other standard file format. The files shall include camera name, ip address, server, template, location, camera username and password

u) The System should support LDAP (Lightweight Directory Access Protocol) server

v) It is preferred to have Video Surveillance Software and Cameras from single OEM for better integration and interoperability perspective. In case more than one OEM is proposed, in such case there should be compatibility and interoperability and integration between the Surveillance Software and Cameras.

Preference will be given to solution from single OEM in QCBS criteria.

However, Concessionaire are free to provide the various brands solution & the same will be evaluated in QCBS criteria.

VMS System

VMS System should have below application/ Console;

VMS Server Management Console

a) VMS Server Management Console to be used by system administrators to perform infrequent administration tasks on a single physical or virtual machine. For example, use the Management Console to complete the initial server Setup Wizard, monitor system logs and resources, troubleshoot hardware and system software issues, and gather information about the installed hardware and software components.

b) The VMS Server Management Console user interface should be available for each instance of system software installed on either a physical server or as a virtual machine.

c) VMS Server Management systems should support network time protocol (NTP) on server, which automatically sets the server time and date.

d) VMS Server Management Console should support configurable in a high availability (HA) arrangement that should allows a primary server to be paired with additional Failover, Redundant, or Long Term Storage Media Server. These HA servers should support the primary server with hot standby, redundant stream storage and playback, and long term recording storage to help ensure that functionality and recordings are not lost if the primary server goes offline.

VMS Operations Management Console

a) The VMS Operations Management Console should have browser-based configuration and administration tool used to manage the devices, video streams, archives, and policies for Video Management System deployment.

b) The VMS Operations Management Console should have following features ;

i. Manage physical devices - Add, configure and monitor the cameras, servers, and encoders that provide live and recorded video.

ii. Manage server services - Configure, enable or disable server services, such as the recording servers that manage video playback and recording.

iii. Monitor video - View live and recorded video, save video clips, search thumbnail summaries of recorded video, use the camera, Pan, Tilt and Zoom (PTZ) controls, or configure pre-defined video Views and Video Walls.

iv. Define recording and event policies - Create recording schedules, define event-triggered actions, configure motion detection, and other features.

v. Monitor system and device health - View a summary of system health for all devices, or device status, alerts and events.

vi. Backup and restore - Backup the system configuration, and optionally include historical data (such as alerts).

vii. The VMS Operations Management Console should support (if required) configurable as a redundant pair for high availability (HA) and system should ensure uninterrupted system access for users and administrators.

VMS Monitoring Console

a) VMS monitoring Console application should allow VMS System users to monitor live and recorded video.

b) VMS monitoring Console should below viewing tool features;

i. Desktop monitoring application

- ✓ Allows simultaneous viewing of up to 25 cameras per Workspace, and up to 48 cameras per workstation.
- ✓ Create Video Matrix windows for display in separate monitors.
- ✓ View Video Walls.
- ✓ Create unattended workstations.
- ✓ View and manage alerts.
- ✓ View cameras, video, and alerts based on a graphical map should support (if required)

ii. Web-based configuration and monitoring tool

- ✓ Allows simultaneous viewing of multiple video panes:
- ✓ View up to 25 cameras with the 64-bit version of Internet Explorer.
- ✓ Add the users, Views and Video Walls available in the desktop application.
- ✓ Configure the camera, streams and recording schedules.

iii. Desktop video clip player

- ✓ Simple player used to view video clip files.

iv. Web-based server console

- ✓ Should provide basic viewing features for a single stream (Stream A) from a single camera.

c) VMS monitoring Console should have below features;

i. Client Application - A full-featured monitoring application should provide access to the cameras and video from a single screen should include the following workspaces and features:

- ✓ Video workspace
- ✓ Wall workspace
- ✓ Alert workspace
- ✓ Maps workspace support (if required)
- ✓ Forensic Analysis Tools should support (if required)

ii. Video Player - monitoring application that includes the following monitoring workspaces:

- ✓ Video workspace
- ✓ Wall workspace

iii. Video Wall Application – This should launches a monitoring application for unattended workstations. Unattended mode allows video monitoring windows to display Video Walls without access to the monitoring console configuration interface. The unattended screens should remain open even is the keyboard and mouse are disconnected, and can (optionally) re-appear when the workstation is rebooted.

iv. Forensic Analysis Tools - VMS monitoring Console should support (if required) below features ;

- ✓ Thumbnail Search—Use Thumbnail Search to quickly locate specific scenes or events in recorded video without fast-forwarding or rewinding. Thumbnail Search should display a range of video as thumbnail images, should allow to identify a portion of the recording to review.
- ✓ Clip Management—Use Clip Management to view, download and delete MP4 clips. that are stored on the server.
- ✓ Motion Analysis—Use Motion Analysis to view a summary of motion events for recorded video.

v. Camera Recording Management

- System should have option to Merge Recorded primary & secondary streams. A camera's recordings from Stream A and Stream B should be played through a single timeline. For example, application should record continuous video throughout the night at a lower quality, but also record higher-quality video whenever an event occurs. The video should displayed in a single timeline.
- System should support recording management to view the recordings available on a camera's local storage device (such as an SD card), and copy them to the server.

2.4.13 Enterprise Resource Planning (ERP)

2.4.13.1. Salient Features of the Proposed e-Governance Application

Various features envisaged for the proposed ERP system at NDMC are given below:

(a) Architecture

- Centralized Server Architecture (n-tier architecture with web enabled user interface)
- The presentation logic should be decoupled from the business components logic
- Data access layer should be on RDBMS platform. Backend RDBMS should be of latest proven version of leading RDBMS.
- Single Database (No Heterogeneous Database to be allowed as part of the proposed solution.

(b) User Interface

- The solution proposed should be Unicode compliant. Authority envisages requirements for both English and Hindi for Data Entry, Display, Input and Output
- Single Sign-on (for all the users) for accessing all the modules
- Any data entry needs to be carried out only once and further it should be made available as often as necessary to all the systems by providing pre-fill feature
- All modules should be homogeneous with respect to Keyboard use, screen layout and menu operations with Graphic User Interface (GUI) support
- GUI Form Administration should support
  - o Changing fields or tab labels

- Hiding fields or tabs.
- Changing the position or size of field or labels
- Adding restrictions like mandatory or not
- Setting default value in a field
- Changing list of value (LOV) contents
- Capability to setup logic to trap conditions to pop messages in response to conditions like logical data entry errors, certain conditions etc. For an example UT is NCT of Delhi and Country is India
- Ability to provide various configurable parameters down to the end user level so that the user screens can have different functionality for a given user.
- Disparate information can be consolidated from a number of systems as required to produce reports and carry out ad hoc analysis and reporting

(c) Access & Data Security

- Role based authentication for accessing various functionalities of different modules with encrypted passwords. Access Rights can be given to Individual Users or Groups

- Flexibility to define separate Role and Designation to the users. Upon transfers of officers / employees, applications / letters / complaints pending with the employee shall remain to the role and new employee will be able to take action on these applications / letters / complaints.

- User rights to various forms should be Create New Record, View existing Record or Edit existing record.

- System should be able to capture exceptions to detect frauds / mistakes

- An audit trail of changes to data in the system should be maintained to identify the users responsible for the modification. There should be a facility to create reports on audit logs

- Information Security i.e. Integrity, Confidentiality & Availability of data to be maintained

(d) Scalability

- System should be built using Service oriented, Open Architecture

- It should be possible to add more fields to the data input screens for capturing additional business specific information without appending source code for that application/module. (for COTS modules / Bespoke development environment)

- Capability to modify existing forms to suit the requirements without requiring additional development tools

- The Application Software should have the capability to scale up to requirements for next decade like: Face recognition, e-building, Adhar based services, utility ducts, sensor based management system, public transportation system etc.

(e) Integrated Application Software

- Authority intends to implement a holistic and an integrated e-Governance system. Different modules need to be seamlessly integrated with each other so that the data duplication can beavoided. This would help Authority to build a strong base for effective and efficient decision support system.

- The solution should have following functionalities: SMS Gateway Integration, Mobile device compatibility, Dashboards for Senior Management and Regular MIS Reports.

- UID integration would be one of the main focus area during implementation. It is expected that the application uses the required Gateways for UID Authentication & integration with SRDH (State Resident Data Hub).

- Authority would also develop a comprehensive GIS. It is envisaged that GIS and the proposed e- Governance systems should work in an integrated fashion to allow Authority to extract maximum benefits from the system. Bidders would have to work closely with GIS vendor to integrate GIS & e-Governance Core Application. Various indicative integration points are mentioned in the subsequent sections.

- It would be a sole responsibility of the Module owner to provide Discounting functionality to be included as part of final billing as and when required

(f) <u>Work flow Management System as an Application:</u>

Workflow Management System would serve as an integrated functionality across all the departmental modules to receive and process the request / applications received via any of the service delivery channels. Each request/application should be processed via workflow engine mechanism. I.e. each of the application should be routed to the respective department official's activity dashboard. WMS should also have a facility of delegation of powers.

Following functionalities should also be part of the integrated applications proposed by a successful bidder:

1) **Role based Access Management System** – Proposed User management module should have following categories of Users:
   a. Super User – IT Cell, IT Manager, Municipal Commissioner
   b. Master Admin – IT cell
   c. Admin – IT Manager, HoD of a department
   d. Regular / Anonymous Users – Employees from various departments of Authority, Citizens requesting/applying for any service/information.

   Available information and user options will vary on all pages throughout the system depending on privileges assigned to the users.

2) **Admin Section** – This section should be privilege restricted and should have the facility to:
   a. Create, modify delete Users and Groups
   b. Assign and remove privileges(modules, sub-modules, workflow & other) to individuals and groups
   c. Administer restricted sections / modules / Webpages

3) Content Management

- System Integrator would be responsible for maintaining and uploading of content on the web portal for implementation phase and also under operation and maintenance period of 5 years.
- Necessary approval from the associated department needs to be taken by the System Integrator for uploading and maintaining of CMS (Content Management System).

General

- The system requires continuous availability (24 * 7)

- The system shall be designed in such a way so as to ensure that the loss of data is minimized due to network 'drop outs'. Automatic refreshing of data at specified time intervals. The information shall be refreshed from the database and shall not require user intervention

- System should have an online help capability, which should be customizable. Should have a facility for online learning and collaboration

- All reports should be query based and should have options like departments zones, wards, employees, from date, to date, etc.

- Authority Users will access the system using Ethernet LAN / Lease Line / RF / Internet

2.4.13.2 Department to be covered under ERP

2.4.13.2.1 Property Tax Department

Functionality	Integration required with
A] Capture of various details of the Property	
• Ward/ Zone/ Block/Route – Administration or Geographical divisions	GIS
• Property Holder's Name – One or multiple owners	
• Property Holder's Email ID / Mobile No.	
• Property Holder's Address (Present Address, Permanent Address)	
• Property Location details (FP No., TP No., Survey No., etc.)	GIS
• Property address	GIS
• Linkage with Building Permission Module to carry forward building details	
B] Capture of various details required for Property Assessment	
• Type and Sub Type of Property	GIS
• Usage of Property	GIS

• Construction Class / Vicinity Factor / Amenity Factor	GIS
• Age of Building	GIS
• Property tax as per rent assessment.	GIS
• Any other factor required for Assessment	GIS
• Re-Assessment of the affected properties to be carried out again in case of road widening.	GIS
C] Self-Assessment Module	
• Allow citizens to enter their property details through Web Portal	Web Portal, GIS
• Option to the citizens to submit their Assessment to the department for confirmation	GIS, WMS
D] System based calculation of Ratable Value	
• Room-wise / Flat-wise/ Whole Property Assessment	
E] Tax Generation	
• Tax Generation as per Rate Chart	
• Tax Exemptions	
• Bifurcation of rates for General Tax, Fire Fighting, Water Tax, Conservancy Tax, Educational Cess, etc.	GIS
F] Other relevant Details for Property	
• Property history	
• Advance property tax payment	
• Property Rental details	
• Date of Assessment	
G] Other Departmental Process	
• Generation of Special Notice	
• Objection	
• Hearing	
• Property Billing o Individual flat-wise billing/ Property wise billing o Calculation of Property Tax as per prevailing Stamp Duty for different areas.	Accounts
o Interest Calculation o Consideration of Advance paid earlier	
• Demand Notice Generation	
• Issue of Warrant Notice	
• Seizure of Property	
• Auction of Property	
• Rebate Calculations	Accounts
• Automatic mailing of Bills / Notices to the E-Mail ID	
• Advance / Excess Collection / Refunds	Accounts
• Cheque Dishonor and Outstation Cheque charges	
• Facility for online tracking of bounced cheque	

• E-Mail / SMS to be sent to the owner upon transactions	SMS Gateway / Web Server
H] Citizen Services	
• Change in Property Ownership	Accounts
• Splitting of Property Tax Assessment	
• Duplicate Bill	
• Assessment Certificate	
• Copy of Property Tax Assessment Extract	
• No Dues Certificate	
• Payment of Property Tax	
• Linkage with Grievance module for Property Tax related grievances	Grievance Redressal
I] MIS	
• Demand / Collection Register	GIS
• Assessment Register	GIS
• Closing Register	
• Ward-wise / Zone-wise Recovery reports	GIS
• Top Defaulters Report	GIS
• Occupancy wise / Flat wise report	
• Escalation alert to be generated for new property assessments to zonal assessors, NDMC officials.	Building Permission Module
• Tax-wise Recovery Details	
• Tax-wise Demand Details	
• Advance Payment Reports	
• Objection / Hearing Details	
• Inspector wise report (Assessment of property as per Building permission/ Citizen request / Inspection)	
• Assessment as per citizen / Assessment as per inspector	
• MIS reports for self-assessment, concessions.	
• Alerts from License Module upon New License / change in business	License Module

Displays the analytical information of property tax collections across the NDMC bodies in a GIS map VII. All the below services can be integrated into ICCC VIII. Create New Property-ID IX. Get Property details- Size, address, year of construction X. Get Property Bill XI. Make Payment XII. Get Receipt Following reports can be displayed X. Demand / Collection Register XI. Assessment Register XII. Ward-wise / Zone-wise Recovery reports XIII. Top Defaulters Report with respect to time and value XIV. Occupancy wise / Flat wise report' XV. Tax-wise Recovery Details XVI. Tax-wise Demand Details XVII. Advance Payment Reports XVIII. Objection / Hearing Details	
J] Other Requirements	
• Data Porting / Data Entry Suite	
• Query of Property Dues	ICCC, Web
• Scope to link up to Land Records / Registration system	
K] Integration with GIS map with analytic layer.	

2.4.13.2.2 Estate Management

S.No.	Functionality		Integration required with
A	Estate Management		
		Creation of Record in the Estate Register • Hand-over from other agencies	Project Systems, Building Permission Module
		Issuance of Municipal Property on rent / lease	
		Generation of Bills	
		Acceptance of Payment	
		Renewal of Rent / Lease agreement	
B	Workflow for Following		
		Renewal of license	
		Transfer of license on legal heir basis/Partnership basis	
		Clubbing of license	
		Outstanding liabilities	

C	MIS		
		Authority Land Register	GIS
		Land Acquisition related reports	GIS
		Revenue Reports for Estate on Rent / Lease	GIS, Accounts
		Outstanding Register for Estate on Rent / Lease	GIS, Accounts
		Top Defaulters List	
		Vacant properties for auction - Licenses issued today/week/quarter/year wise - New application received /disposal/timelines - Pending Licenses for issuance - Area wise trend on new license, pending dues/pending renewals/pending transfers, issuance, pending - Revenue Generated today - Projected Revenue this month - Allotment Transfers done in a week/month/year - Revenue split of stalls, shops office space, commercial premises-hotels, restaurants - Comparison of per unit license rate of similar properties - Licenses expiring in coming week/month/quarter. - Payment status due/paid resumed licenses pending renewal applications. - Alerts on vacant premises/shops, outstanding dues	
D	Other Requirements		
		Data Porting / Data Entry Suite	Accounts
E	Integration with GIS map with analytic layer.		

2.4.13.2.3 Asset Management

Functionality	Integration required with
A] Classification of Assets	
▪ Immovable Assets o Land o Building o Roads, Footpaths o Bridges, Culverts, Flyovers, Subways & causeways o Drains including underground drains o Water Works Distribution o Public Lighting System o Lakes and Ponds o Capital Work-in Progress	GIS, Project Systems

□ Movable Assets o Plant and Machinery – including machinery of Water Works & Drainage, Road dept. machinery o Vehicles o Furniture & Fixtures o Office Equipments o Other Equipments o Live Stock	Central Workshop System
□ Investments	Accounts
□ Capture Various details for the Assets o Ownership o Cost Details (construction / Purchase / Transfer) o Depreciation Principles o Other details to arrive at Current Value	Accounts
□ Preparation of Opening Balance for Asset Valuation	Accounts
B] Asset Transactions	
□ Purchase of New Assets	Municipal Secretary, Projects, Accounts, WMS
□ Acquisition of Land	
□ Asset Sale	
□ Investment on Assets (like construction of new floors, road re-surfacing, etc.)	
□ Insurance Details	
□ Insurance Claim Related Information capture	Accounts
C] MIS	
□ Asset Register	GIS
□ Revenue Report	Accounts
□ Outstanding Register	GIS, Accounts
□ Search facility for various information (like search for name of road)	GIS
MIS Details on procured assets, material details, and financial impacts on the assets, assets under maintenance, asset categorization, asset usage should be integrated into the dashboard	
D] Other Requirements	
□ Data Porting / Data Entry Suite	Accounts
The Asset management module should be integrated into ICCC	
E] Integration with GIS map with analytic layer.	

2.4.13.2.4 Solid Waste Management Department

Functionality	Integration required with
A] Area details	
▯ Area information (Zone / Ward / Colony / Society) ▯ Population details ▯ Volume of the Solid waste (Recycled & Non Recycled) ▯ Resources required (Manpower, Vehicle, Equipment) ▯ Collection procedure (i.e. Primary : Residential & Commercial collection, Gate to Dump / Transfer Station; Secondary : Community Bin to dump site / transfer station)	GIS, Property Tax Module, Fleet Management, GPS Software Solution
B] Garbage Collection Scheduling	
▯ Assign SWM Vehicles to pick-up the Garbage. Route / Category wise assignment.	GIS, Fleet Management, GPS Software Solution
▯ Zone wise / Ward wise / Location-wise / Bin wise assignment of Sanitation Staff	GIS, HRMS
▯ Scheduling of garbage collection and cleaning activities with the objective of maximizing citizen friendliness on one hand and optimum use of resources on the other.	
▯ Assigning routes to SWM vehicles / Dumper placers / Compactor vehicles etc.	GIS, Central Workshop
C] Primary Garbage Collection & Disposal through weigh bridge	
▯ Record the volume of garbage collected and disposed on a daily basis from each household through RFID based system.. Source segregation like Quantum of waste collected with further segregation for vermiculture, Bio dispose can be kept on Monthly /Yearly basis. The same can be used for RV benefit.	Central Workshop
▯ Linkage with Garbage Bins in case of Citizen Grievance	CCRS, GPS
▯ Keeping certain Checks as per environmental regulations, like minimum frequency of lifting garbage, transportation mode, etc.	GPS Software Solution
▯ Record of garbage bin/container (Community bin) lifted as per schedule.	GPS Software Solution, GIS
▯ Record of cleaning of roads / boundaries done as per schedule	GIS

Record of waste gone to process plant as per schedule	GIS, GPS Software Solution
D] Treatment of Waste & Disposal of Inert Waste at Landfill site	
Reports on Input of Waste by plants, final products made by the plants	
Reports on inert waste sent to the land fill site by the plants	
Revenue generation to Authority from process plants (may be in the form of royalty)	GPS Software Solution
E] MIS	
Monitor the deployment of pickup trucks and personnel based on the schedule originally drawn.	GIS, GPS Software Solution
Generation of registers like: Contracts Register for SWM, Site Register (landfills), Contractors Register, etc.	
SWM Contract Wise Status Reports, Site Wise Progress Summary, Contractor wise Performance Analysis, etc.	
Comparison of expenditure on SWM activities over different geographical areas, years, agencies, etc.	GIS, GPS Software Solution, Accounts
Daily / Monthly reports of comparison for how much garbage has to be lifted as per target & how much garbage is actually lifted. If less lifted then reasons for the same for e.g. Breakdown / Labour problem.	GIS, GPS Software Solution
Daily / Monthly status reports of waste bin process plants	
MIS report for expenditure incurred on primary sweeping, door-to-door / gate-to-dump / transfer station	HRMS, Accounts
MIS report for expenditure incurred on transportation	Central Workshop, Accounts
MIS report for expenditure incurred on disposal	Accounts, GPS Solution Software
Record of waste vehicles operating with schedule details at various regional/zonal offices & Ramp	GIS, GPS Software Solution
Daily / Monthly status report of cleaning of Public urinals, toilets.	GIS, GPS Software Solution

Daily / Monthly status report of action taken by Health Inspectors & Class III / IV employees assigned to each Ward offices / Zonal offices.	
Mandatory reports (annual reports to GPCB, CPCB, MOEF, annual report to planning dept. of Authority)	
• Monitoring of the smart waste management system web application real-time level information for containers as well as the automatic warning system which notifies when containers require attention. • GIS based Real-time monitoring of solid waste collection vehicles. • Geo tagged bins whether cleaned or not through GPS on vehicles, in case sensors are on C&D Waste. • Log calls/jobs on the helpdesk database utilizing helpdesk software (inquiries may be received by telephone, facsimile, email or in person). • Track progress of waste management service requests against pre-determined KPIs. • Maintain asset information held in the helpdesk database. Update site specific waste management files and other documentation for helpdesk compliance.	
F] Other requirements	
Capturing RFID Details of all waste collection vehicles /dumper/compactor, etc. along with details of waste collected by each of them.	GPS Software Solution, Accounts
G] Integration with control room complaints and GIS map with analytic layer.	

In addition to the ERP of the Solid waste Management, the SI has to provide the RFID tags to the Bins of the 75,000 household in the NDMC area and the RFID reader to all the Vehicles collecting garbage from the NDMC area. The information of all the RFID tag will be read by the readers installed in these vehicles while collecting garbage in the area. The same information will be transferred through GPRS/wifi/ wired network to the command and control centre. Based on the real time data received of individual household various reports will be generated by the System which will help NDMC to take further decision of improving efficiency of the system. Weighing sensors will also be installed on all the garbage collection vehicles for tracking of real time weight of the garbage lifted and disposed off.

2.4.13.2.5 Project Systems (Engineering) Module

S.No.	Functionality		Integration required with
A	Project Initiation		
		Defining New Project	
		Selection of Department, Officers for scrutiny	HRM
		Selection of Budget Code	Accounts
B	Project Estimation		
		Identification of different items, defining units	
		Selection of SOR / Market Rates / DSR /ESR / WSR Rates	Document Management System
		Preparation of Measurement Sheet	Accounts
		Addition of Analysed items not included in Standard DSR (for special items)	
		Preparation of Abstract sheet	
		Preparation of Rate Analysis Sheet	
		Preparation of Recapitulation Sheet	
		Defining various Milestones / Time limit	
		Workflow for A/A & E/S.	
C	Administrative Sanction		
		Workflow for Administrative sanction as per Delegation of Powers(DEP)	Workflow System
		Workflow system to support To & Fro movement of proposal	
		NIT preparation work flow for NIT preparation to approval.	Access rights to be given as per DEP
D	Technical Sanction		
		Workflow for Technical sanction as per chart of competent authorities	Workflow System
		Workflow system to support To & Fro movement of proposal/file	
E	Tendering		
		Generation of information for press Advertisements	
		Check-list for Tender Notice	
		Special conditions for contract if any	
		Publish Tender Notice on Web Portal	Web Portal
		Publish Tender Document on Web Portal	
		Reports to assist Tender Document preparation	
		Check-list for Tender Terms & Conditions	
		Purchase of Tender Documents/RFP	Accounts, Web
		Submission of bids	e-procurement
		Technical bid evaluation	

		Cross-check of vendors with the approved Vendor list of Authority and their previous records	
		Commercial bid evaluation	
		Justification preparation	
		Award of work	
		Issue of PG letter	
		Issue of Award Letter	
		Cross-check of rates with similar projects in past	
		Award of contract	
		Milestone entry	
F	Project Monitoring		
		Physical & Financial Status updation	
		Monitoring & Project Head wise,	
		Division wise, circle wise, Chief Engineering wise.	
G	Project Execution		
		Project Scheduling	
		Measurement Book Entry and it's movement diary	Accounts
		Monitoring of progress	
		Quality Control (PMC / TPIA report)	
		Notices to agencies / vendors (for delay, for poor quality, any other reason)	
		Levy of Penalty	Accounts
		Agencies Black-listed / restricted for certain period	
H	Billing & Completion Certificate		
		Running Account Bills	Accounts
		Billing for Extra items/ Substitute item/ Additional quantity.	
		Completion / utilization certificate	
I	MIS Reports		
		Project wise comparison of Budgeted Expenditure Vs. Actual Expenditure	Accounts
		Milestone Monitoring Report	GIS
		Measurement Sheet / Abstract Sheet / Rate Analysis Sheet / Recapitulation Sheet	
		Technical Bid Comparison	
		Financial Bid Comparison	
		Billing Information	Accounts
		Project Summary Sheet	
		Reasons for delay in achieving milestones. The responsible parties to be identified like any Authority Department or Contractor.	
		Reports / Alerts through other systems for New Projects • Building Permission Module • Grievance Redressal Module	GIS

		• Alerts for Road Re-surfacing / Repairing	
		Cross-departmental information as alerts while defining new projects • E.g. : Water Department should get alerts for Pipeline laying, if the Road (location, measurement) is being prepared / re-surfaced / Grouting / Paving	GIS, Integration of all modules with this.
J	Other Requirement		
		Registration of contractors/Suppliers	
		Up-gradation of contractors data / Blacklisting of contractors	
		Contractors Register	
		Confidential Register of Contractors/Suppliers	
		Road register (Traffic (PCU) / Road history register/ Building assets register / Defect liability)	
		Works Manual / Account Manual	
		Manual followed by dept. for implementation of projects (IRC / CPHEO / WHO / ISO / etc.)	
		Assets register (history / annual maintenance / Continuous monitoring /details of PCU)	
		Monitoring of Sewerage treatment plants. History & all the relevant data (Monthly report of influent & effluent characteristics of sewage, electricity consumption, BOD, COD, GPCB reports, Third Party Reports, etc)	SWM
		Revenue generation from STP	
		Expense for O&M of Sewerage System • Collection Cost • Sewage Treatment cost • O&M of Pumping Station	
		Monitoring of Drainage Pumping Stations. History & all the relevant data	
		Monitoring of Water treatment plants. History & all the relevant data (Monthly report of raw & treated characteristics of water, electricity consumption, Central Laboratory / Health Dept., Third Party Reports, etc)	
		Monitoring of Water Pumping Stations. History & all the relevant data (Monthly report of functioning, electricity consumption, etc)	
		Expense for O&M of Water Distribution System • Raw water cost • Production cost • Distribution Cost	
		Monitoring of Hot mix plant (material stock, consumption, TPIA reports, etc)	

2.4.13.2.6 Audit Module

Functionality	Integration required with
A] Departmental Process	
Pre-Audit of Tenders, Estimates	Accounts
Audit Para Entry	Accounts
Post Audit of the Departments	
Inspection of Contractor & Supplier Bills	Accounts
Inspection of Other Bills like Telephone Bills	
Inspection of Advance Adjustment proposals	
B] Reports	
Department-wise Budget Provision v/s Expenditure Report	
Status report on Audit Para	
Various statutory reports to be submitted to Standing Committee	Accounts
Exception Reports (w.r.t. deletion of records, adjustment entries, etc.)s	Accounts, Other Modules

2.4.13.2.7 Web Portal

Functionality	Integration required with
A] Home Page	
Message from Chairman	
Vision, Mission, Objectives	
Link to various sub-sections o City Information o Online Services o About Authority o Projects o Citizen Grievances	
B] City Information	
History of NDMC	
Tourist Locations	
City Map with citizen related GIS information	GIS
C] About Authority	
Administrative Information	
Information on Elected Representatives, Various Committees	

D] RTI Names of PIO. Departments/Wards: Intro, Objectives, responsibilities, powers & duties of officers, employees with gross salary, activities, time limit, directory with telephone no. Committee: Members, purpose, type, freq. of meeting, docs available for public. Projects/ Activities: Budget head, work activities, allocated amount, current statistics. Details of concessions, subsidies given, computerization done in various depts. Integration required for updation of data for RTI with projects, accounts, HRMS, Fleet, material, asset.	Projects, Accounts, HRMS, Material Mgmt., Fleet Mgmt., Hospital Mgmt., Asset Mgmt.
Opinion Poll	
Photo Gallery	
Tenders	Accounts, Projects
FAQ’s	
Emergency Information	
Employee Login using LDAP	HRMS, Associated Department
Feedback	HRMS
Contact Us	
E] Online Services	
Application acceptance for various services / certificates o Birth / Death Certificates o Duplicate Bills o Building Permission related services o Water Connection o No Dues Certificates	Accounts, Corresponding Module, CCRS
Downloading of Forms	
Online Tendering o Sale of Tender Forms o Acceptance of Tenders	
Complaints o Acceptance o Status Tracking	
Status on Applications / Complaints	
Payment Details, Bill Details	
Online Payments	

□ Self-Assessment of Property Tax	Property Tax Module
f. Web portal must be dynamic and interactive	
g. Provision for individual department to update the information at their end.	
h. Registration of the citizens for availing online services.	

Note: The SI has to do the study of above mentioned departments for development of ERP software and incorporate all the functionalities and requirement of that department. The ERP to be develop shall be complete in all request. It is a turnkey project and during study and implementation stage no change request will be consider. The applicant shall study the requirements of such works before submitting their bids. Change request will only be applicable after Go-Live.

2.4.15 Acceptance Testing

1. SI 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 SI may propose further detailed Acceptance plan which the NDMC will review. Once NDMC provides its approval, the Acceptance plan can be finalized. In case required, parameters might be revised by NDMC 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	SI	1. SI to perform System testing 2. SI to prepare test plan and test cases and maintain it. NDMC may request the SI 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 SI. NDMC doesn't intend to own these tools
Integration Testing	SI	1. SI to perform Integration testing 2. SI to prepare and share with NDMC the Integration test plans and test cases 3. SI 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 SI. NDMC doesn't intend to own these tools
Interoperability Testing	SI	1. SI will prepare interoperability traceability matrix with third party systems (existing legacy systems with ICCC) in consultation with NDMC 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. SI to perform Interoperability testing 3. SI to prepare and share with NDMC the Interoperable test plans and test cases with scenarios 4. SI 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	- SI - NDMC / Third Party Auditor (to monitor the performance testing)	1. SI 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 NDMC . 5. Performance testing to be carried out in the exact same architecture that would be set up for production. 6. SI need to use performance and load testing tool for testing. NDMC doesn't intend to own these tools. - NDMC if required, could involve

		third party auditors to monitor/validate the performance testing. Cost for such audits to be paid by NDMC .
Security Testing (including Penetration and Vulnerability testing)	- SI - NDMC / 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 SI 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. SI 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.
User Acceptance Testing of ICCC System	- NDMC appointed third party auditor	1. NDMC appointed third party auditor to perform User Acceptance Testing 2. SI 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. SI should fix bugs and issues raised during UAT and get approval on the fixes from NDMC / third party auditor before production deployment 5. Changes in the application as an outcome of UAT shall not be considered as Change Request. SI has to rectify the observations.

Note:

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

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

c. The SI 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.
d. The cost of rectification of non-compliances shall be borne by the SI.
e. STQC/Other agencies appointed by NDMC shall perform the role of TPA. SI 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. SI 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 SI.

2.4.16 Operations and Maintenance for a period of 5years

SI will operate and maintain all the components of the ICCC for a period of seven (5) years after Go-Live date. During O&M phase, SI shall ensure that service levels are monitored on continuous basis; service levels are met and are reported to NDMC. 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. All the manpower engaged for O&M support of the project should be citizens of India.

SI will ensure that at no time shall any data of ICCC be ported outside the geographical limits of the country.

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

2.4.16.1 Helpdesk and Facilities Management Services

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

The SI shall setup a central helpdesk dedicated (i.e. on premise) for the Project, which shall be supported by smart city command centres, implemented and proposed to be setup under Smart City Programme. 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.

SI shall deploy Manpower during implementation and O&M phases. The deployed resource shall report to NDMC’s Project In-charge for Smart City Project and work closely with Program Management Office of the project. The minimum resources required to be deployed in the Project has been mentioned in Clause 5.3.6.1, however SI may deploy additional resources based on the need of the Project and to meet the defined SLAs in this RFP:

S. No.	Type of Resource	Minimum Quantity	Minimum Deployment during Operation and Maintenance phase
1.	Project Manager	1	100%
2.	Solution Architect	1	Onsite Support to Project team on need basis
3.	Project Manager-Software	1	100%
4.	Project Manager – Infrastructure	1	100%
5.	Database Architect/DBA	1	100%
6.	Security Expert	1	Onsite Support to Project team on need basis
7.	Command Centre Expert	1	100%
8.	IBMS expert	1	Onsite Support to Project team on need basis
9.	Help Desk Manager	1	100%
10.	Help Desk Executives	2	100%

2.4.16.2 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 SI shall keep the application software in good working order; perform changes and upgrades to applications as requested by the NDMC 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 SI in the application support phase are as follows:

a. Compliance to SLA

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

b. Annual Technology Support

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

c. Application Software Maintenance

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

ii. SI shall address all the errors/bugs/gaps in the functionality in the solution implemented by the SI (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 SI ensuring customization done in the solution as per the NDMC's requirements are applied. Technical upgrade of the installation to the new version, as and when required, shall be done by the SI. Any version upgrade of the software / tool / appliance by SI to be done after taking prior approval of NDMC 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 SI 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 NDMC approval. A detailed process in this regard will be finalized by SI in consultation with NDMC.

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

vi. SI, at least on a monthly basis, will inform NDMC 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 SI shall inform about the same immediately along with his recommendations. The report shall contain SI's recommendations on update/upgrade, benefits, impact analysis etc. The SI shall need to execute updates/upgrades though formal change management process and update all documentations and Knowledge databases etc. For updates and upgrades, SI 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. SI 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 NDMC 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 SI needs to follow all such processes (based on industry ITSM framework). For any change, SI 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 SI shall define the Software Change Management and Version control process. For any changes to the solution, SI has to prepare detailed documentation including proposed changes, impact to the system in terms of functional outcomes/additional features added to the system etc. SI shall ensure that software and hardware version control is done for entire duration of SI's contract.

f. Maintain configuration information

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

g. Training

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

h. Maintain System documentation

SI 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

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

i. Source code is documented

ii. Functional specifications are documented

iii. Application documentation is updated to reflect on-going maintenance and 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. SI 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 NDMC by the end of next quarter.

j. For application support SI shall keep dedicated software support team to be based at SI 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 SI 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 SI

k. Any software changes required due to problems/bugs in the developed software/application will not be considered under change control. The SI 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 SI at no extra cost.

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

2.4.16.3 *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. SI 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.

2.4.16.4 *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. NDMC 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
- SI has to mention latest IT Infrastructure (Hardware and Software) during bid submission
- SI has to deliver latest (At the time of commissioning of ICCC) IT Infrastructure (Hardware and Software)
- The SI 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.

2.4.16.5 *Warranty support*

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

b. SI 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. SI 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. SI 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. SI 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 SI shall replace or augment or procure higher-level new equipment or additional licenses/hardware at no additional cost to the NDMC 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 SI shall maintain the systems and repair/replace at the installed site, at no charge to NDMC, all defective components that are brought to the SI's notice.

f. The SI 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 NDMC.

g. The SI 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 SI 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 NDMC team as well.

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

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

    i. SI 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 SI shall introduce a comprehensive Assets Management process & appropriate tool to manage the entire lifecycle of every component of ICCC System.

2.4.16.6 Maintenance of ICT Infrastructure of Command and Control Centre (ICCC)

a. Management of ICT Infrastructure of ICCC

SI need to deploy requisite mix of L1, L2 and L3 resources (on 24X7 basis) for management of entire ICCCC System including ICT infrastructure deployed at Command Center. All resources deployed in the project should be employees of SI 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 NDMC . It is expected that the majority of resources have worked with SI for at least preceding 1 year and have proven track record and reliability. Considering the criticality of the project, NDMC may ask for security verification (Police verification) of every resource deployed on the project and SI need to comply the same before deployment of the resource at the project. At all times, the SI need to maintain the details of resources deployed for the project to NDMC and keep the same updated. A detailed process in this regard will be finalized between NDMC and SI. The SI shall maintain an attendance register for the resources deployed Attendance details of the resources deployed also need to be shared with NDMC on monthly basis. NDMC 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, SI will change the resource on request of NDMC. SI 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. Updating of all Documentation.

During operations phase the SI 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. SI 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 SI may also be reviewed by NDMC.

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

iii. On an ongoing basis, SI 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. SI shall be responsible for identification, diagnosis and resolution of problem areas pertaining to the IT Infrastructure and maintaining the defined SLA levels.

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

vi. SI 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. SI 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 NDMC on need basis.

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

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

c. System Administration

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

ii. SI shall also ensure proper configuration of server parameters and performance tuning on regular basis. SI 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 SI may be reviewed by NDMC .

iii. SI 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. SI 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. SI shall also be responsible for proactive monitoring of the applications hosted

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

vii. NDMC 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. SI 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. SI 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 SI may be reviewed by NDMC .

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

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

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

iv. SI will follow guidelines issued by NDMC 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. SI shall be responsible for implementation of backup & archival policies as finalized with NDMC . The SI is responsible for getting acquainted with the storage policies of NDMC before installation and configuration. It should be noted that the activities performed by the SI may be reviewed by NDMC .

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

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

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

g. Network monitoring

i. SI 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 SI may be reviewed by NDMC .

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

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

iv. SI shall also provide network related support and will coordinate with connectivity service providers of NDMC /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 ICCC system as agreed with NDMC

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

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-malware, phishing and malware for managed resources.

vii. Reporting security incidents and co-ordinate resolution

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

ix. Maintaining secure domain policies

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

xi. 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

xii. Resolution of calls for security notifications, system alerts, vulnerabilities in hardware/software and alerting NDMC as appropriate

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

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

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

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

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

xviii. Performing periodic review of security policy and suggest improvements

xix. 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

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

xxi. Modifying security policy, routing table and protocols

xxii. Performing zone management (DMZ)

xxiii. Sensitizing users to security issues through regular updates or alerts - periodic updates/Help NDMC issuance of mailers in this regard

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

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

xxvi. Testing and implementation of patches and upgrades

xxvii. Network/device hardening procedure as per security guidelines from NDMC

xxviii. Implementing and maintaining security rules

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

i. Other Activities

i. SI 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 NDMC , any changes in the configuration manual need to be approved by NDMC . Configuration manual to be updated periodically.

ii. SI 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. SI 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 SI shall provide from time to time the Updates/Upgrades/new releases/new versions of the software and operating systems as required. The SI should provide free upgrades, updates & patches of the software and tools to NDMC as and when released by OEM.

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

vii. Software License Management: The SI shall provide for software license management and control. SI 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 SI to scale up the Operations & Maintenance (O&M) team as and when required to ensure smooth project execution throughout the project duration.

2.4.16.7 Compliance to SLA

a. SI 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 SI for ensuring the SLA requirements.

b. SI 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 NDMC officials as per the project requirements.

Project Implementation Timelines

2.4.17 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 SI shall provide the following documentation at the stage of exit management:

i) As-build drawing with marking of field devices, controllers and sensors

ii) As-implemented configurations

iii) As-implemented architecture and topology diagrams

iv) Completed UAT and FAT results

v) Standard operating procedures for administration of the installed devices.

vi) Each Site-specific user manual and standard operating procedures for end users

vii) Hardware-devices warranty details

viii) License details

2.4.17.1 Cooperation and Provision of Information

During the exit management period:

a. The SI will allow the NDMC 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 NDMC to assess the existing services being delivered

b. Promptly on reasonable request by the NDMC, the SI 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 SI or sub-contractors appointed by the SI). The NDMC shall be entitled to copy of all such information. Such information shall include details pertaining to the services rendered and other performance data. The SI shall permit the NDMC 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 SI and to assist appropriate knowledge transfer.

2.4.17.2 Confidential Information, Security and Data

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

   v. all other information (including but not limited to documents, records and agreements) relating to the services reasonably necessary to enable NDMC or its nominated agencies, or its Replacement SI to carry out due diligence in order to transition the provision of the Services to NDMC or its nominated agencies, or its Replacement System integrator (as the case may be).

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

2.4.17.3 Employees

a. Promptly on reasonable request at any time during the exit management period, the SI shall, subject to applicable laws, restraints and regulations (including in particular those relating to privacy) provide to the NDMC or its nominated agency a list of all employees (with job titles) of the SI 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 SI to the NDMC or its nominated agency, or a Replacement SI ("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 SI, department, or its Replacement SI may make an offer of employment or contract for services to such employee of the SI and the SI shall not enforce or impose any contractual provision that would prevent any such employee from being hired by the NDMC or any Replacement SI.

2.4.17.4 Transfer of Certain Agreements

On request by the NDMC or its nominated agency the SI shall effect such assignments, transfers, licenses and sub-licenses NDMC, or its Replacement SI in relation to any equipment lease, maintenance or service provision agreement between SI and third party lessors, vendors, and which are related to the services and reasonably necessary for the carrying out of replacement services by the NDMC or its nominated agency or its Replacement SI.

2.4.17.5 General Obligations of the SI

a. The SI shall provide all such information as may reasonably be necessary to effect as seamless a handover as practicable in the circumstances to the NDMC or its nominated agency or its Replacement SI and which the SI 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 SI, associated entity, or sub-contractor is deemed to be in the possession or control of the SI.

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

2.4.17.6 Exit Management Plan

a. The SI shall provide the NDMC 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 SI 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 SI's sub-contractors, staff, suppliers, customers and any related third party as are necessary to avoid any material detrimental impact on the NDMC ’s operations as a result of undertaking the transfer;

   iii. (if applicable) proposed arrangements for the segregation of the SI's networks from the networks employed by NDMC and identification of specific security tasks necessary at termination;

iv. Plans for provision of contingent support to NDMC , and Replacement SI for a reasonable period after transfer.

b. The SI 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 SI to and approved by the NDMC or its nominated agencies.

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

3. *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 SI will ensure that the entire ICCC solution is developed in compliance with the applicable standards.

2. During project duration, the SI 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

3. Apart from the above the SI 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/Deity (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 SI 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 SI 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. NDMC, at its discretion, may also engage independent auditors to audit any/some/all standards/processes. The SI shall support all such audits as per calendar agreed in advance. The result of the audit shall be shared with the SI who has to provide an effective action plan for mitigations of observations/non-compliances, if any.

4 Project Management

4.1 Project Management

SI will have to setup a office for execution of this Project. SI will depute the project implementation team at this office. The operational aspects need to be handled by the SI including maintaining weekly statuses, minutes of the meetings, weekly/monthly/project plans, etc.

Project Management Team 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 Project team for the project implementation phase and operations and maintenance phase.

4.2 Steering Committee

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

The SI 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 SI.

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, NDMC may call for a Steering Committee meeting with prior notice to the SI.

4.3 Project Monitoring and Reporting

The SI shall circulate written progress reports at agreed intervals to NDMC 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. NDMC reserves the right to ask the bidder for the project review reports other than the standard weekly review reports.

4.4 Risk and Issue management

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

The SI shall monitor, report, and update the project risk profile. The risks should be discussed with NDMC 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.

4.5 Planning and Scheduling

The SI 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 SI has to get the plan approved from NDMC 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 NDMC in this RFP. SI cannot change any of the milestone completion dates. SI can only propose the internal task deadlines while keeping the overall end dates the same. SI 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;

5. Change Management & Control

5.1 Change Orders / Alterations / Variations

a. The SI agrees that the requirements given in the Bidding Documents are minimum requirements. 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 SI 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 NDMC.

b. Further upward revisions and or additions required to make SI'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 NDMC.

c. Any upward revision and/or additions consequent to errors, omissions, ambiguities, discrepancies in the Bidding Documents which the SI had not brought out to the NDMC's notice in his bid shall not constitute a change order and such upward revisions and/or addition shall be carried out by SI without any time and cost effect to NDMC.

5.2 Change Order

a. The Change Order will be initiated only in case (i) the NDMC directs in writing the SI 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) SI 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 NDMC and for which cost and time benefits shall be passed on to the NDMC, (iii) the NDMC directs in writing the SI to incorporate changes or additions to the technical specifications already covered in the Contract.

b. Any changes required by the NDMC 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 NDMC in writing.

e. Within ten (10) working days of receiving the comments from the NDMC or the drawings, specification, purchase requisitions and other documents submitted by the SI for approval, the SI 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 NDMC.

6. Functional & Technical Requirements

6.1 Command and Control Centre Application

The Integrated Control and Command Centre (ICCC) will comprise of various software application modules which will be integrated with the Smart City System Applications which are connected to field level equipment's which will provide data and information to the Integrated Control and Command Centre (ICCC). The ICCC will process these inputs and provide the integrated view to the various decision makers like emergency response team for actionable intelligence.

Business Rules and SOP Definitions – The system should enable users to define the business rules around incidents handling and Emergency response as per agreed SOPs for the Smart City

Incident Management — should manage the life cycle of incidents and related entities via pre-defined workflows. The workflow could cut across multiple systems via the interfacing modules. Workflow for operational alerts and escalations should be triggered automatically without human intervention.

The ICCC should have capacity of more than 1000 concurrent users.

The ICCC shall be capable of deployments which can scale to many thousands of users without change to architecture (except addition of servers/workstations/ licenses).

The ICCC shall be capable of receiving SMS/MMS from citizens in addition to voice call

The ICCC shall be accessed via remote devices to undertake specific ROLES (such as command, administrative, dispatch function)

The ICCC shall be multi-lingual.

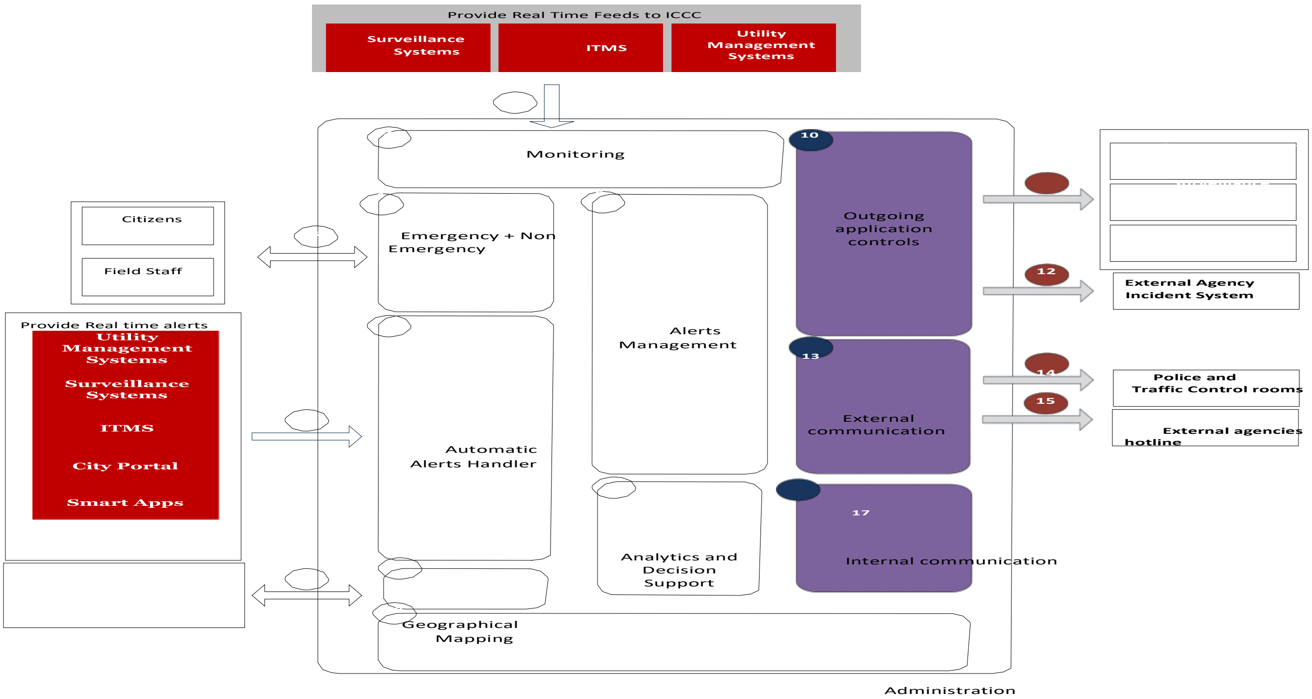
The ICCC shall have a very tight integration between GIS, Common Operating Picture and event/resource/response management functions – ideally at the software level.

The ICCC GIS shall support multiple map formats.

The Solution shall support the receipt of emergency calls from persons with speech or hearing difficulties through the Guidelines defined under Accessible India Program.

The Software solution for ICCC application should be provided with cross platform integration tools at the data level and application level, so that integration can be achieved anytime during the project life cycle. Also data acquisition would happen from various devices and the volume would be too high, so a proper mechanism must be deployed to capture this data

The below diagram shows the interaction of various entities with the various functions of the ICCC:


Provide Real Time Feeds to ICCC
Surveillance Systems
ITMS
Utility Management Systems
Monitoring
10
Outgoing application controls
Citizens
Field Staff
Emergency + Non Emergency
Alerts Management
12
External Agency Incident System
Provide Real time alerts
Utility Management Systems
Surveillance Systems
ITMS
City Portal
Smart Apps
13
External communication
14
Police and Traffic Control rooms
15
External agencies hotline
Automatic Alerts Handler
17
Analytics and Decision Support
Internal communication
Geographical Mapping
Administration

The proposed functionality of each block, as depicted in the diagram above, is described below (S. No‘s mentioned in the table below are mapped to the block numbers mentioned in the diagram):

S. No. (Mapped to ref numbers in the diagram)	Type	Description
1.	Interface	The surveillance, intelligent transport and utility management systems will provide real time, at pre-defined frequency and on-demand feeds into the ICCC
2.	ICCC Function	Feeds received from systems mentioned in 1 above shall enable ICCCA to perform real time monitoring of the city operations. The monitoring shall be facilitated by feeds being transmitted on to the individual desktops and the large video wall inside the City Operations Room for collaborative monitoring.
3.	Interface	The contact centre interface will provide citizens and field staff of various agencies with the single point where they will be able to record their grievances / feedback / incidents. This interface will enable citizens to interact with ICCC through audio call, SMS, mobile interface and web interface. This will be a two way interface enabling citizens to pass information to ICCC and receive updates from ICCC on the actions taken by ICCC.

4.	ICCC Function	The contact centre function will enable ICCC to record and update both day to day incidents such as electricity break down and emergency situations such as accidents. The contact centre will receive the information from citizen and record in the database which will trigger the workflow for resolution of the incident.
5.	Interface	The Interface will enable automatic capture of the following Data : Sensor Data from the various sensor platform including IoT based Gateways deployed as a part of the Smart City Systems The systems deployed throughout the city will be monitoring the various incidents taking place as per the rules defined in the respective systems. The incidents captured automatically by these monitoring systems shall be reported into the ICCC via this automated interface This will enable ICCC to aggregate and create a centralized repository of all Data & incidents reported throughout the city either manually (as in 3 &4 above) or through this automated interface. The envisaged systems that will be generating these alerts are – ● Utility Management Systems (SCADA) ● Surveillance Systems ● Intelligent Transport Management System ● City Portal (Web Interface for stakeholders to record incidents) ● Smart Mobile Apps (Mobile Interface for stakeholders to record incidents)
6.	ICCC Function	This function within the ICCC will enable it to receive the sensor data , normalise the data and generate alerts or receive the alerts directly from other system, add relevant data to the alerts incident and pass on to next entity as per pre-defined workflow
7.	Interface	Surveillance, ITMS and Utility Management Systems would use the geographical functions and geo-spatial data stored in the central GIS application for implementing their functionality that requires GIS layer. The required data and functionality exchange would be done through this system.
8.	ICCC Function	This block refers to the centralized GIS layer that would be created at ICCC for access by other systems.
9.	ICCC Function	The incidents reported manually through contact centre as well as automatically received through alerts handler shall be handled by functional this block. Further, it will enable the ICCC to carry out complex event processing for data received from Sensor system directly, correlate the data through rule engine for alerts creation and will enable execution of workflow for managing the incident life cycle as per pre-defined business rules and SOPs. This will ensure consistency of response to incidents.
10.	ICCC Function	The ICCC will control the surveillance, ITMS and Utility Management systems via this interface enabling them to be controlled through a common interface.
11.	Interface	This interface will enable ICCC to pass data to be used by various systems e.g. view triggers into various systems such as viewing a specific camera view into ICCC, sending SMS through a SMS gateway etc.

12.	Interface	This interface will enable ICCC to pass data to intimate the respective agency about incident reported in ICCC e.g. creating incident in incident management system of electricity department about power failure
13.	ICCC Function	This function will enable ICCC to interact with external stakeholders. This block shall use tools such as Video Conferencing, Agency hot-lines etc.
14.	Interface	This interface shall enable transfer of video feeds to traffic and police control rooms
15.	Interface	This interface shall enable audio and video hotlines to agencies and offices in case of emergency situations
16.	ICCC Function	The internal communication within ICCC shall be managed through video conferencing and IP telephony systems
17.	ICCC Function	This block will enable ICCC to perform analytics on the data gathered during lifecycle of various incidents thereby enabling it to make informed changes to it SoPs, business rules and workflows.
18.	ICCC Function	This block will enable ICCC to define the security access rights, Standard Operating Procedures, Business Rules, and Workflows, Device Provisioning and Management (Sensor System) etc to enable the ICCC to function in the desired manner.

The technical components of the ICCC solution are mentioned below along with the mapping to functionality that they cater as per the functional block diagram.

S. No.	Solution Component	Functional Blocks Catered
1.	ICCC application	1, 2, 5, 6, 9, 10, 11, 12, 17, 18
2.	GIS application with high resolution satellite image (base map) of NDMC	7, 8
3.	Video wall display system	2
4.	Video Conferencing System	13, 14, 16
5.	IP Telephony	13, 15, 16
6.	Contact centre system, appliances and work stations	3, 4
7.	Operator appliances and work stations	2
8.	SMS Gateway	13, 16

In addition to the above mentioned ICCC shall be equipped with following facilities:

- Operating facilities for following personnel:
  - ICCC operators
  - Contact Centre/helpdesk
  - Technical Support
  - NoC
  - Security

- Meeting / conference rooms

SI has to do civil work for setting up the ICCC and install required furniture and fittings. SI has to provision for necessary power backup for the ICCC.

6.2 Integrated Command and Control Centre

The SI has to provide, deploy and configured an integrated operations and dashboard application that integrated various Smart City use cases on this platform.

Proposed Solution architecture should have combination of data normalization and City operation center software with below capabilities, data normalization software should support on-prim and cloud technology, however bidder can choose one platform for this project;

S.NO.	Functionality Description		Compliance (Yes/No)
1.	Data Normalization capabilities	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- m) Smart Outdoor Lighting n) Smart Parking o) Smart Traffic Management p) Smart Energy Metering q) Smart Water Metering r) Public Safety and Safe City Operations s) Connected Public Transport (Metro/DTC) t) Public Wi-Fi and Urban Service Delivery over Public Wi-Fi u) Kiosks for Citizen Information v) Citizen Interactive Kiosks for Urban Service Delivery w) Environmental Monitoring x) Smart Waste Management y) And other integrations as per defined scope	
2.		The platform should be able to integrate with any type of sensor platform being used for the urban services irrespective of the technology used. platform should be on open standards or compatible.	
3.		The platform should also allow the manufacturers of the sensors to develop integrations themselves using SDKs without affecting the northbound applications and existing integration	
4.		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	

S.NO.	Functionality Description		Compliance (Yes/No)
		OEMs etc.) and provide secure access to that data using data API(s) to application developers.	
5.		The platform should support distributed deployment of functions (workflows & policies) across city's network and compute infrastructure with centralized management and control.	
6.	GIS Map Support	System should support Esri, map box, Open street etc.	
7.	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	
8.	Device engine	a) Aggregation and abstraction of sensors: provides aggregation of sensors from diverse sensor cloud b) Normalization of sensor data: organizes sensor data and assigns attributes based on relations; raw data removed and passed to data engine	
9.	Data and Analytics engine	a) Data archive and logging: stores data feeds from the device engine and external data sources. b) Analytics: provides time-shifted or offline analytics on the archived data. c) Reporting: delivers reports based on events triggered by device engine data and external notifications.	
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.	
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,	

S.NO.	Functionality Description		Compliance (Yes/No)
		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 systems) 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.	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.	
26.		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.	
27.		The platform should be able to integrate any type of parking sensor irrespective of the technology used. For example, some parking sensors might use RF technology like LoRa or ZigBee to communicate the data and events, some might use GPRS or some might use Wi-Fi. Some parking sensors might use infra-red based detection, some might use magnetic field based detection or combination of the both where as some might use a video camera to detect parking occupancy. Irrespective of the technology, the platform should be able to integrate with these devices and their software managers and provide the data from such devices in a normalized and standard based data models.	
28.		The same logic and requirement applies to various other urban	

S.NO.	Functionality Description		Compliance (Yes/No)
		services devices like LED control nodes, water meters, energy meters, environmental sensors, waste bin sensors, device embedded in connected vehicles etc.	
29.		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.…)	
30.		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	
31.		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.	
32.	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.	
33.	Policies and Events	Exhibit 1. - 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.	
34.		Exhibit 2. - System should provision to defines a set of conditions that can be used to trigger an event-based policy	
35.	Notifications, Alerts and Alarms	Exhibit 3. - System should generate Notification, Alert and Alarm messages that should be visible within the Dashboard and the Enforcement Officer Mobile App if required.	
36.		Exhibit 4. - 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.	
37.		Exhibit 5. - 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.	
38.	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.	
39.		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	

S.NO.	Functionality Description		Compliance (Yes/No)
		assigned locations only.	
40.		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.	
41.		The platform should allow different roles to be created and assign those roles to different access control policies.	
42.		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.	
43.		System should support LDAP to be used as an additional data store for user management and authentication.	
44.	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.	
45.	Reports	The platform should have capability to provide access to real time data and historical data from various connected devices for reporting and analytics.	
46.		System should allow dashboard to generate reports and have provision to add reports in favorites list	
47.	Data Security	The access to data should be highly secure and efficient.	
48.		Access to the platform API(s) should be secured using API keys.	
49.		Software should support security standards: OAuth 2.0, HTTPS over SSL, and key management help protect the data across all domains.	
50.	Global Market Presence & Support System	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.	
51.		The Smart City supplier should be industry leader and belong to leader quadrant of the "Navigant Research Leader board Report For Smart City Supplier".	
52.		The proposed OEM solution software platform should be deployed in at least 1 city in India and 5 cities globally. Bidder to furnish OEM self- certification with the name of the cities.	
53.		Software 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.	

S.NO.	Functionality Description		Compliance (Yes/No)
54.		Command Centre OEM should have registered office in India at least from last 10 Years and should software development center in India. Should have Quality Management System ISO 9001 and Environmental Management System ISO 14001 Quality Certifications.	
55.	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.	
56.		Standard Operating Procedures should be established, approved sets of actions considered to be the best practices for responding to a situation or carrying out an operation.	
57.		The users should be able to edit the SOP, including adding, editing, or deleting the activities.	
58.		The users should be able to also add comments to or stop the SOP (prior to completion).	
59.		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.	
60.		The ICCC platform should have the capability to bring in multiple stake holders automatically into a common collaboration platform like persistent chat rooms and virtual meeting rooms in response to a SOP defined to handle a particular event.	
61.		The ICCC 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	
62.		The stake holders can be on various types of devices like computer, smart phones, tablets or normal phones	
63.		The operator should also have ability create these collaboration spaces like virtual meeting rooms or chat groups manually.	
64.		The SOP Tool should have capability to define the following activity types:	
65.		Manual Activity - An activity that is done manually by the owner and provide details in the description field.	
66.		Automation Activity - An activity that initiates and tracks a particular work order and select a predefined work order from the list.	
67.		If-Then-Else Activity - A conditional activity that allows branching based on specific criteria. Either enter or select values for Then and Else.	
68.		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.	
69.		SOP Activity - An activity that launches another standard operating procedure.	

S.NO.	Functionality Description		Compliance (Yes/No)
70.	Enterprise resource planning (ERP) integration	System should allow integration of business process in ERP workflows like property tax collection etc.	
71.		System should allow ERP data visualization at city dashboard	
72.		The platform should have the capability to retrieve data directly from ERP systems. The APIs should be RESTful and return the data in JSON format.	
73.		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.	
74.		System should be able to read data from flat CSV files.	
75.	Digital billboards integration	System should share city data to Digital billboards application in API format, Digital billboards management software will do business correlation and push content for outdoor display.	
76.	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.	
77.		The solution should be flexible to integrate with other city and government software applications.	
78.		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	
79.		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	
80.		Analytics Engine should support multiple Data Sources. Min below standard data sources should be supported from day 1 – CSV, TSV, MS Excel , NOSQL, RDBMS	5
81.		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	
82.	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	
83.	Export Formats	System should allow export the analysis into min following formats: a) XML/JSON b) Excel c) PDF d) CSV	
84.	Video Display and integration capabilities	Integrates with existing cameras and new cameras. Should support multiple video sources from multiple locations. Platform should have no limitation in displaying the number of CCTV video sources	
85.		Integrate and assess inputs from different sources such as CCTV, Video Analytics, and sensors further to assist with actionable intelligence.	
86.		Display module should have capability to control multi-screened display wall in sync with operator console	

S.NO.	Functionality Description		Compliance (Yes/No)
87.		Visual integration of maps with video and data displays up to 16 channels simultaneously	
88.		Should support Fixed type and PTZ camera. Control PTZ function from the screen to control the camera	
89.		Supervisors remotely can access the system and monitor the alerts received, action taken status, response etc.	
90.		Should be able to access the CCTV sources both from CCTV Camera and from Video Management software.	
91.		Should be able to display Alarms from different sources such as Video alarm from cameras, video alarms from VMS, if required	
92.		Should support integration of Video analytics from edge and server based video analytics	
93.		Provide configurable intelligent operator console based on the jurisdiction, critical area or sensors to monitor as per situation demands for focused surveillance.	
94.		Should be able to integrate with 3rd party applications alerts, like Video Loss Alarm, Loitering, Vehicle counting etc.	
95.		Alarm Management system should be in place to customize each type of alarm display	
96.		Generate Customized reports based on the area, sensor type or periodic or any other customer reports as per choice of the administrators	
97.		Should support multiple Local operation center along with Viewer stations that requires monitoring function	
98.	Social Media Intelligence	Provide analytics based on the social media feed collected from the open source intelligence and collate with the surveillance inputs to alert the responders for immediate action on the ground.	
99.		There should be a mechanism to retrieve and cache open social data from Facebook, Twitter, G+ and LinkedIn. The system should have the capability to use the cached social data for analysis	
100.	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.	

6.3 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 (min. 10 users) of NDMC.

SI will implement dedicated EMS solution to meet the SLA monitoring and other requirements as mentioned in the RFP. The implemented EMS solution to help NDMC in data driven decision making. In case the SI uses any OEM product(s), the implementation should be as per best practices of the OEM. NDMC 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 SI 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. EMS Solution with all the modules from single vendor would be preferred.

6.3.1 SLA & Contract management System

The SLA & Contract Management solution should enable the NDMC 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 SI 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.

6.3.2 Reporting

- Ability to generate reports on penalty and credit due, to check on non-compliance of SLAs for the ICCC project
- Monetary penalties to be levied for non-compliance of SLA, thus the system must provide Service Level Performance Report over time, contract, service and more.
- 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 ICCC project
- The solution must support security for drill-down capabilities in dashboard reports ensuring visibility for only relevant personnel of the ICCC project
- Support real-time reports (like at-a-glance status) as well as historical analysis reports (like Trend, TopN, Capacity planning reports etc.)
  - Resource utilisation exceeding or below customer-defined limits
  - Resource utilisation exceeding or below predefined threshold limits

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 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.

6.3.3 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.

6.3.4 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.
- The proposed solution should have provision for Automatic Remediation. IT plays a vital role in automatically reducing the noise, so as soon as the problem is detected, the root cause should be determined by the management console and a ticket should be created to focus on remediation. Using the automatic remediation of common IT tasks,

the fix should be handled automatically. For non-common IT tasks the same should be escalated to appropriate level.

- Using automatic remediation, the operators should be able to apply a fix with or without manual intervention based on a predefined fix available for the cause event. Using the automatic remediation of common IT tasks, the fix should be handled automatically after the problem is detected and a service desk ticket has been created and recorded.

6.3.5 Centralized 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.

6.3.6 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 behavior, 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.

6.4 Software Defined Security (SDS) for Applications /Services

S. No.	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.

7. Technical Specifications

7.1.1 Video Wall Solution

7.1.1.1 Video-wall Screen

S.NO.	Specification Item	Detailed Specification Description	Compliance (Yes/No)
1	**Configuration**	CUBES OF 70" DIAGONAL IN A 6 (C) X 2 (R) CONFIGURATION COMPLETE WITH COVERED BASE STAND	
2	**Cube & Controller**	Cube & controller should be from the same manufacturer	
3	**Reputed Company**	The OEM should be an established multinational in the field of video walls and should have installations around the world	
4	**Chip Type**	1-chip Digital micro mirror device	
5	**Resolution**	1920x 1080 native DMD chip resolution	
6	**Light Source Type**	Laser light source	
7	**Brightness**	Minimum 2200 lumens	
8	**Brightness Uniformity**	≥ 90 %	
9	**Dynamic Contrast**	1400000:1 or more	
10	**Control**	IP based control to be provided	
11	**Remote**	IR remote control should also be provided for quick access	
12	**Screen to Screen Gap**	≤ 1.0 mm	
13	**Screen Support**	Screen should have an anti-reflective glass backing to prevent bulging	
14	**Control BD Input terminals**	Input: 1 x Digital DVI	
15		Input: 1 x HDMI	
16		Input: 1 x HD-BaseT	
17		Input: 1 x Display Port	
18		Output: 1 x Digital DVI	
19	**Auto color adjust function**	Should provide auto color adjustment function	
20		Should be sensor based	
21	**Maintenance Access**	Front	
22	**Cube Size**	Each cube should have a screen size of 1550 mm wide and 872 mm high (+-2%). Depth of cube shall be 560 mm or less.	
23	**Cube control & Monitoring**	Videowall should be equipped with a cube control & monitoring system	
24		Provide videowall status including Source , light source ,temperature, fan and power information	

25		Should provide a virtual remote on the screen to control the videowall	
26		Input sources can be scheduled in " daily", "periodically" or "sequentially" mode per user convenience	
27		System should have a quick monitor area to access critical functions of the videowall	
28		User should be able to add or delete critical functions from quick monitor area	
29		Automatically launch alerts, warnings, error popup windows in case there is an error in the system	
30		User should be able to define the error messages as informational, serious or warning messages	
31		Automatically notify the error to the administrator or user through a pop up window and email	
32		Status log file should be downloadable in CSV format as per user convenience	

7.1.1.2 Video-wall Controller & Software

S. No	Parameter	Indicative Specifications	Compliance (Yes/No)
1	Controller	Controller to control Video wall in a matrix as per requirement along with software's	
2	Chassis	19” Rack mount	
3	Processor options	Single Quad Core Intel® Core™ i7 Quad Core 3.4 GHz processor) or better	
4	OS	Supports 64-bit Operating System Windows 7	
5	RAM Capacity	16 GB or more	
6	HDD	500 GB or more	
7	Networking	Dual-port Gigabit Ethernet	
8	RAID	RAID 1, 5, 10 supports	
9	Power Supply	(1+1) Redundant hot swappable	
10	Cooling	Any Advanced Proven cooling mechanism	
11	Input / Output support	DVI/HDMI/USB/ LAN/ VGA/SATA port	
12	Accessories	DVD +RW, Keyboard and mouse	
13	Voltage	100-240V @ 50Hz	
14	Redundancy support	Power Supply, HDD, LAN port & Controller	
15	Scalability	Display multiple source windows in any size, anywhere on	

		the wall	
16	Control functions	Brightness / contrast / saturation/ Hue/ Filtering/ Crop / rotate	
17	Universal Inputs	Minimum 2	
18	Formats	DVI /RGB/Component	
19	Input Format	NTSC/ PAL/SECAM	
20	Operating Temperature	10°C to 35°C , 80 % humidity	
21	Cable & Connections	Vendor should provide all the necessary cables and connectors	

Video Wall Management Software

Sl. No	Parameter	Minimum Specifications	Compliance (Yes/No)
1	Display & Scaling	Display multiple sources anywhere on display up to any size	
2	Input Management	All input sources can be displayed on the video wall in freely resizable and movable windows	
3	Scenarios management	Save and Load desktop layouts from Local or remote machines	
4	Layout Management	Support all Layout from Video, RGB, DVI, Internet Explorer, Desktop and Remote Desktop Application	
5	Multi View Option	Multiple view of portions or regions of Desktop, Multiple Application Can view from single desktop	
6	Other features	SMTP support	
7		Remote Control over LAN	
8		Alarm management	
9		Remote management	
10		Multiple concurrent client	
11		KVM support	
12	Cube Management	Cube Health Monitoring	
13		Pop-Up Alert Service	
14		Graphical User Interface	
15	Cube ,Controller & Wall Management Software	Cube , Controller and Wall management Software should be from the same manufacturer	

7.1.1.3 Operators Client Workstations

S. No	Parameter	Minimum Specifications	Compliance (Yes/No)
1	Operating System (OS)	Windows 7 Pro, Ultimate or Enterprise, 64-bit	
2	CPU	Intel Core i7, 3.07 Ghz or Higher	
3	Memory	32 GB DDR3	
4	Graphics Card	Nvidia GeForce GT430 PCIe Nvidia GeForce GTX460 PCIe or faster.	
5	Network connection	Gigabit Ethernet (GigE) network connection required	
6	Monitor	Min 22 Inch or Higher	

7.2 Smart City Data Center

7.2.1 Blade Chassis & Management

S.no.	Parameter	Description	Compliance (Yes/No)
1	Blade Chassis	Blade chassis shall be 19" Electronic Industries Alliance Standard Width rack mountable and provide appropriate rack mount kit.	
2	Power	The enclosure should be populated fully with power supplies of the highest capacity & energy efficiency of a minimum of 90%.	
3		The power subsystem should support N + N power redundancy (where N is at least equal to 2) for a fully populated chassis with all servers configured with the highest CPU configuration, maximum memory and IO configuration possible	
4	Cooling	Each blade enclosure should have a cooling subsystem consisting of redundant hot pluggable fans or blowers enabled with technologies for improved power consumption and acoustics	
5	Chassis connectivity	The chassis should support redundant modules for connectivity - Ethernet and Fiber Channel /Infiniband modules OR converged fabric modules in lieu thereof	
6	Ethernet Module	Chassis should have sufficient number of redundant 10gb based ethernet modules to provide a minimum of 20 Gbps per blade server and 10 Gbps sustained per blade server (with 1 module failure)for a fully populated chassis for LAN Traffic.	
7	FC Module	Chassis should have sufficient number of redundant 8gb based FC modules to provide a minimum of 16 Gbps per blade server and 8 Gbps sustained per blade server (with 1 module failure)for a fully populated chassis for FC Traffic.	
8	Converged Module	In lieu of above mentioned Ethernet and FC module, Chassis can also be provision to have sufficient number of redundant 10gb based converged modules to provide a minimum of 40 Gbps per blade server and 20Gbps sustained per blade server (with 1 module failure)for a fully populated chassis for LAN & SAN Traffic. It should also provide minimum 40Gbps FCOE downlink bandwidth from each module /switch to each x86 server	

9	Management	Must be able to show the actual power usage and actual thermal measurement data of the servers across chassis	
10		Administrators should have the ability to set a cap on the maximum power that the chassis / physical server can draw in order to limit power consumption for non-critical applications	
11		Redundancy should be built in the management subsystem so that if one management module fails other should be able to take over automatically. Management solution should be provided so that management upto 10 blade blade chassis can be done from single console.	
12		Role Based Access Control and remote management capabilities including remote KVM should be included	
13		Should support a environment where server identity including - server BIOS version, MAC ID, NIC firmware version, WWPN , FC-HBA firmware version , Management module firmware version, Server Boot Policies, KVM IP etc can be created	
14		Movement of server identity from one slot to another in the event of server failure within chassis as well as across chassis.	
15	Licensing	Should include all necessary licenses for management for a fully loaded chassis.	

7.2.2 Blade Servers for applications

7.2.2.1 Blade Server – 2 Socket

S.no.	Parameter	Description	Compliance (Yes/No)
1	Processor	Each blade server should be configured with a minimum of two (2) 2.60 GHz E5-2690 v3/ v4 processors or higher available in latest series. Proposed processor should be available in the market for atleast last 6 months.	
2	Memory	Should have at least 24 DIMM slots and should be populated with minimum 128 GB of memory Day1.	
3	HDD	The server should support a minimum of 2 hot plug SAS, SATA and SSD hard disk drives and should be populated with minimum 2 x 600 GB SAS drives of memory Day1	
4	Interface ports	The Blade server should support Ethernet and fiber channel connectivity OR Converged Network Adapters in lieu of the same. The Converged Network Adapters should aggregate both the Ethernet and FC connectivity on a single fabric	
5		The server should be configured to provide for port and card level redundancy	
6	IO bandwidth	The server should provide a minimum of 36Gb aggregate bandwidth per server (2 x 10Gb for Ethernet and 2 x 8 Gb for FC OR 4X10Gb for Converged Network adapter). Server should support the scalability to 80gb of LAN & SAN traffic.	
7		The server bandwidth should be expandable to 80Gb per server	

8	Management	It should suport remote/virtual KVM capability from an external keyboard, video monitor and mouse to all blades installed in the chassis through the management controllers and should also support virtual media for dvd access.	

7.2.2.2 Blade Server – 4 Socket

S.no.	Specifications		Compliance (Yes/No)
1	Processor	Each blade shall support up to four (4) Intel Xeon E7 - 4800/8800 V3/V4 series of CPUs. Should be populated with min two E7-4820 V3/ V4 CPUs. Proposed processor should be available in the market for atleast last 6 months.	
2	Storage	The Blade should have two front accessible hard disk drives or Solid State Drives (SSD)	
3		The Blade should have support for Boot from SAN	
4	Memory	The server should have at least 16 GB per core DDR 3/DDR 4 memory. After populating DIMMs, Each blade server should have 100% free memory DIMM slots remaining for future expansion. Server should be scalable to 96 DIMM slots per blade. Should have atleast 48 DIMMs slots with 2 CPUs populated.	
5	Network	The Blade server should support Converged Network Adapter , which aggregates both the Ethernet and FC connectivity on a single controller	
6		It should support scalability upto 160 Gb Ethernet connectivity per server. Should be provided with 80 Gbps across two or more cards.	
7	Management	It should support remote KVM capability from an external keyboard, video monitor and mouse to all blades installed in the chassis through the management controllers	
8		Remote KVM should support up to 4 active sessions	
9	Others	The Blade should be hot pluggable	

7.2.3 Data Center Switch-Type I

S. No.	Features	Specifications	Compliance (Yes/No)
1	Hardware & Performance Requirements	Chassis based Multilayer Switch with sufficient modules/line cards to fit required transceivers/UTP ports. Chassis shall have minimum 8 payload slots. The switch must have front to back airflow.	
		The total aggregate switching capacity shall be scalable to 3 Tbps or more, SI to choose the required bandwidth as per their solution.	
		There should not be any single point of failure in the switch. All the main components like CPU module, switching fabric, support module, system clock, power supplies and fans etc should be in redundant configuration. Components, like modules/power supplies/fan tray should be Hot Swappable	

		The switch should have redundant CPU's working in an active-active or active-standby mode. There should not be any traffic disruption during the CPU fail-over/change-over and the fail-over time should be less than 1 sec.	
		Should Support Hitless software upgrades (ISSU) to reduce downtime during software upgrade. The switch must support Fault isolation per process and process patching to enhance the switch availability	
		The Switch should support non-blocking Layer 2 switching and Layer 3 routing.	
		The Backplane should be 100% Passive. Preferrably back plane free design to optimize the airflow and power consumption.	
		The Switch should have a Truly Distributed Architecture. All Interface Modules should have all the resources for switching and Routing and should offer True Local Switching (Intra-Module and Inter-Module).	
		The switch must support 1/10G SFP+, 1/10 G Base-T and 40G QSFP based port line cards. The switch must scalability to support minimum 200 nos of 40 G QSFP ports or more. Bidder to choose required ports as epr their solution.	
		Support for Unidirectional Link Detection Protocol (UDLD) or equivalent, Layer 2 trace route or equivalent to ease troubleshooting	
2	Layer 2 and Layer 3 Functionality	Should support port, subnet based 802.1Q VLANs. The switch should support 4096 vlans. The switch must support Private VLAN or equivalent.	
		The switch should support 50K no. of MAC addresses	
		Switch must support spine - leaf topology based on VXLAN and create large layer 2 domains.	
		Switch must support multi chassis ether channel feature and work with any downstream switch, server from various vendors.	
		Should support routing protocol IP v4 - Static routing, OSPF v2, BGPv4, IS-IS and IP v6 - BGP, OSPF v3. The switch must support Bidirectional Forwarding detection. The total aggregate switching capacity shall be 3 Tbps or more	
		Switch should support VRF - Lite and VRF Route leaking functionality..	
		Should support minimum 32K Route entries for IPv4 and IPv6 routes.	
		Switch should support 8K Multicast route	
		Switch must support IP v4 – HSRP/ VRRP and IP v6 - HSRP v6/ VRRP v6. It must also support DHCP Relay V4 and V6.	
3	Remote Line card and Virtualization support	Switch must support IEEE 802.1BR (Bridge Port Extension) or equivalent technology, which in turn enable remote line card functionality to optimize cabling inside the data center.	

		Switch must support virtualization features like VXLAN Gateway/Bridging and routing functionality. Capability of supporting NVGRE is preferred.	
3	Minimum Port Requirement – Day 1	Switch should have minimum of 72 x 40G Ports	
4	Compliance/ Certifications	The switch should be minimum EAL2 / Applicable Protection Profile (NDPP) certified under the Common Criteria Evaluation Program. In case, the OEM has applied for the certificate, then either such OEM shall get the certificate for such switches before the date of Go-Live, or such switches has to be replaced from switches of an OEM having such certificate.	

7.2.4 Data Center Switch-Type 2

S. No.	**Features**	**Specifications**	**Compliance (Yes/No)**
1	Hardware features	Proposed network device must be 19'' rack mountable & Maximum 2 RU in size.	
		It is desirable that the network infrastructure is based on delivering front to back airflow.	
		Must have Redundancy Power Supply Units (PSUs), Hot-swappable, field-replaceable power supplies, 1:1 power redundancy and Must have N:1 fan module redundancy.	
		All components (including elements such as I/O cards, Expansion Module, power supplies and fans) must be hot swappable with zero disruption to traffic forwarding (Unicast or multicast).	
		Must have minimum 48 x 1/10 G SFP+ and 6 X 40 G QSFP port, SI to choose required transceivers as per their solution. Core/ Spine to TOR/ Leaf switch connectivity should be at multiple of 40G links.	
		Transceivers to be supplied as per minimum BOQ given in RFP.	
		Must be field upgradeable / license upgradeable to Layer 3 for investment protection.	
		Must have Line-rate traffic throughput on all ports at Layer 2.	
		Must have Line-rate traffic throughput on all ports at Layer 3.	
		Must support Bridge Extension Protocol (IEEE 802.1BR) or equivalent - to scale Gigabit & 10 Gigabit Ethernet ports	
		Must allow building very large L2 domain using Multi-Path Ethernet technologies.	
		Must support port channeling across multi chassis.	
2	Switch Features	Physical standards for Network Device	
		Must support I IEEE 802.1d, IEEE 802.1w, IEEE 802.1s, IEEE 802.1q, IEEE 802.1ab, IEEE 802.3ad, IEEE 802.1p	

		Routing protocol support when upgraded with Layer3 License	
		Must support Static IP routing, OSPF, BGPv4,	
		Must support Protocol Independent Multicast Version 2 (PIMv2) sparse mode, Source Specific Multicast (SSM), Multicast Source Discovery Protocol (MSDP), and Internet Group Management Protocol Versions 2, and 3 (IGMP v2, and v3)	
		Support for up to 8K multicast routes	
		Must support In-Service Software Upgrade (ISSU) for Layer 2	
		Must have Modular QoS classification compliance	
		It is preferred that switch must support VXLAN (Bridging and Routing) as well as NVGRE orverlay encapsulation protocol in hardware to support multiple hypervisor deployment in the Data Center	
		Must support Remote Authentication Dial-In User Service (RADIUS) and/or Terminal Access Controller Access Control System Plus (TACACS+)	
3	Security features	Must support AAA using RADIUS (RFC 2138 & 2139) and/or TACACS+, enabling centralized control of the device and the ability to restrict unauthorized users from altering the configuration	
		Must have following Access Control features	
		Must support Ingress ACLs (Standard & Extended or equivalent) on Ethernet and virtual Ethernet ports	
		Must have Egress strict-priority queuing or equivalent	
4	Quality of Service	Must support Egress port-based scheduling: Weighted Round-Robin (WRR) or equivalent	
		Must have ACL-based QoS classification (Layers 2, 3, and 4)	
5	Compliance / Certification	The switch should be minimum EAL2 / Applicable Protection Profile (NDPP) certified under the Common Criteria Evaluation Program. In case, the OEM has applied for the certificate, then either such OEM shall get the certificate for such switches before the date of Go-Live, or such switches has to be replaced from switches of an OEM having such certificate.	

7.2.5 Primary & Secondary Storage Solution

Primary Storage for DC

S. No.	**Parameter**	**Minimum Specification**	**Compliance (Y/N)**
1	Converge/ Unified Storage	Unified Storage/Truly converge Solution with NSPoF (No single point of failure) Architecture. The Storage solution should support NAS & SAN as an integrated offering with high availability at each level. The architecture should allow upgrades of hardware and software for investment protection.	
2	Protocols	Solution should be configured with required protocols for the	

		solution CIFS/SMB 3/ NFS 4/iSCSI/FCoE/FC. All required protocols required for the solution to be enabled.	
3	Controllers	System to have minimum Two controllers with NSPoF Architecture (NO single point of failure architecture). System Data mover/controller should support 2x Intel Xeon E5-2600 6-core CPU or higher. Storage should support non-disruptive online firmware upgrade for both Controllers and disk drives.	
4	Operating System	The storage array should support Operating System Platforms & Clustering including: Linux/Windows//Unix OS.	
5	Cache Memory	Cache Memory: Each controller should support 128 GB RAM with usable protected data Cache for Disk IO Operations. If NAS controllers with separate controllers additional RAM cache to be provided. The storage array must have complete cache protection mechanism either by de-staging data to disk/flash or protecting with NVRAM	
6	Host Connectivity	The storage system shall be capable of providing host connectivity as per solution offered (Unified/SAN/NAS/Scale out NAS). Minimum 4 ports per controller to be provided for host connectivity	
7	RAID Supports	RAID levels Supported: 0, 1, 5, 6, 10 (Dual parity or higher)	
8	Redundancy	Fans and power supplies: Dual redundant, hot-swappable	
9	Disk Drive Support	Storage subsystem shall support 6TB/8TB or higher NL-SAS/SATA/equivalent 7.2K drives in the same device array.	
10	Global Hot Spare	System should have the capability to designate global hot spares that can automatically be used to replace a failed drive anywhere in the system. Storage system should be configured with required Global Hot-spares for the different type and no. of disks configured, as per the system architecture best practices.	
11	Multipath	Multi-path & Load balancing, MPXIO, IPMP, LACP protocol should be supported.	
12	**Capacity**	**The storage system should be configured with 265TB usable capacity using 10TB 7.2K RPM NL-SAS disk with 6+2 disk raid (Dual parity protection) and 2 nos of global hot spare disks. Additional 14 TB usable on RAID 6 using 1.6 TB Enterprise SSD drives or higher**	
13	Thin Provisioning	Proposed array must be supplied with Thin provisioning for the configured capacity.	
14	De-duplication	Should provide de-duplication functionalities for the configured capacity.	
15	Tiering	Storage should support inbuilt automated tiering feature that migrates the most frequently accessed data to the SSD/RAM. Necessary licenses for configured capacity to be provided from day 1	
16	Snapshots	Should be able to take "snapshots" of the stored data. Offered Storage shall have support to make the snapshot in scheduled or auto snaps. Snapshot should support both block and file.	
17	Replication	The storage array must have the capability to do remote replication using IP technology.	
18	Software Licenses	All the necessary software and licenses to configure and manage the storage space, RAID configuration, logical drives allocation, snapshots, compression, de-dup, replication, auto-tiering for the configured capacity to be provided from day 1	
19	Monitoring	Should support the functionality of proactive monitoring of Disk drive and Storage system for all possible hard or soft failure.	

7.2.6 Tape Library

S. No.	Features	COMPLIANCE
1	ARCHITECTURE: a)The offered Automated tape library with Redundant Power Supply must be of latest technology and should be provided with minimum 4 nos. of LTO7 tape LTO7 SAS/FC tape drives with 50 slots or more ."	
2	SCALABILTY : The offered tape library must have modular scalability for slots scalable up to 500+ slots and 40 drives - As And When required . All the slots and Drives must be seamlessly accessible through the Same Single Robotics.	
3	DATA TRANSFER RATE : Offered LTO 7 drive should have native speed of at least 300 MB/sec and a compressed speed of at least 750 MB/sec for 2.5:1 compression.	
4	CONNECTIVITY :Should provide for 8 Gbps native FC connectivity to SAN switch & should be backward compatible to 4Gbps also.	
5	MANAGEMENT: The offered tape library must have web based remote management facility	
6	CONSUMABLES: LTO7 Data cartridges and cleaning cartridges with Barcode labels to be provided with proper bar code labels. As per solution for retention	
7	PARTITION :Should support for partitioning so that each drive can be configured in a separate partition thus providing the ability to utilize a single library in a variety of applications. All the necessary Licence or hardware for min 4 partitions must be provided along with the library . The Tape library should have provision upto 20 partitions in future.	
8	FLEXIBILITY :The Tape Library should provide feature and capabilty for the Mixed media usage. The Tape Library should provide support different LTO generation tape drives within the same library- in case required by user . Older generation LTO5/LTO6 Media and Drives must be supported.	
9	The Tape Library should have a Bar-Code Scanner/reader to accurately locate the catridges and take the desired action for backup or Restore without any manual intervention.	
10	RELIABILITY: The offered tape library must have a high reliabilty ie MCBF (mean cycles between failures) more than 2,000,000 cycles.	
11	CERTIFICATIONS: The TL must be Certified by the BIS STANDARDS (Certificate to be attached)	
12	MONITORING: The overall solution with Tape Library and the backup s/w integration should have features like Intelligent monitoring management and diagnostics & The Tape library must have features to Set alerts for backup and archive events	
13	The overall solution with Tape Library should have a Built-in Management feature to monitor the Tape Library Modules (Tape Drives, Power Supply, etc.) through a centralized Console.	
14	The Tape Library should have GUI based Operator Console along with manageability through Web Based Browser.	

15	The overall solution offered Tape Library should provide either AME or LME encryption key management . The necessary tools/Licence required must be provided by the System integrator, to keep the Encrypted keys in a Redundant and safe location.	
16	Offered Tape Library should be integrated with the Servers and Storage (HP, NetApp, IBM, DELL , FUJITSU , EMC) to back up all the data from the SAN to The Tape library using the required backup S/w , this should be LAN free and the necessary NDMP licence must be factored by the Bidder.	
17	The Tape library should provided be provided as an Integrated Solution , thus the required Backup S/w, HBA/FC and SWITCH must provided by the Bidder.	
18	Tape library should provide Barcode reader and min 10 mail slots –, to deliver easy, secure access to individual tape cartridges without interrupting library operations.	
19	The Tape Library should have LCD front panel	

7.2.7 Backup Storage

S.NO.	Parameter	Minimum specification	Compliance
1	Solution/Type	Backup Storage (Archival/Backup) should leverage advanced space efficient and faster retrieval technologies. It can be on any media such as Tapes, Disks, Disk systems, etc. or its combination. (so as to arrive at lower cost per TB)	
2		Should use de-duplication & compression technology	
3		Compatible with Primary Storage	
4	Backup Size	To store data as required, to meet the archival requirement of different logs, 90 days of storage for feeds on backup storage and post this store it on tapes for further retention.	
5	Hardware Platform	Rack mounted	
6	Software Platform	Must include backup/archive software compatible with the proposed solution	
7	Backup window	Retrieval data time should be 4/6 hours for critical data. For faster retrieval of critical data backup solution should leverage disk system technology	

7.2.8 Backup Software

Sl. No.	Technical Specification	Compliance
1	Backup software must support GUI with centralized management / Single interface for management of all backup activities.	
2	The offered software must support Advanced sharing of different media across the environment (disk, tape and optical)	
3	The offered software must support multiple level of backups including full, incremental, differential and synthetic full.	
4	The offered software must support D2D2T & D2T mechanism. It should provide deduplication and compression technologies for backup efficiency.	

5	The offered software must support following application and database backup without CLI and without the requirement of temporary disk space for Postgre SQL, 64-bit Active Directory, MS SQL, MS Exchange, Share-Point, Oracle, MySQL.	
6	Proposed capacity license must include unlimited database license including MS SQL, MySQL, PostgreSQL, Oracle, SharePoint, AD, DB2, Sybase etc. In case any database is not covered in capacity license, bidder must include 20 license for each type to avoid any challenge.	
7	The proposed software must have block level technology to store single copy collected from multiple electronic repository.	
8	The software must be able to Compress and Encrypt data at the Client-side and this feature should be available even during de-duplication.	
9	The offered software must have more than three Encryption algorithms (like 128 bit AES, 256 BIT AES etc) and it should not demand for additional license, any such license if needed should be quoted for the total backup capacity license.	
10	The offered software must provide Backup master server in HA/ DR capability. License must be included in proposed solution.	
11	The offered software must support backup of virtual environment including RHEV, Vmware, Hyper-v, OVM through integration with their hypervisor managers.	
12	Backup solution must support multi tenancy feature for creation of distinct data zones.	
13	The offered software must be able to auto discover guest VMs with database instances and dynamically protect them with application consistent recovery for MS SQL and Oracle.	
14	The software solution must provide full support for Global Filter lists.	
15	The offered software solution must support IPV4 and IPV6 addressing system.	
16	The offered software solution must have inbuilt capability to do trend analysis for capacity planning of backup environment.	
17	The offered software must support heterogeneous media server agent failover.	
18	The proposed solution must support data archival for inactive data based on age or quota with seamless access on multiplatform (Windows, Linux and Unix).	
19	The proposed solution must have inbuilt Ransom ware detection capability for clients	
20	Proposed backup solution must have inbuilt capability to protect the backed up volume from Ransom ware.	

7.2.9 WAN Services router and Internet Router

Item	**Specifications for WAN services router or Internet Router**	**Compliance (Yes/No)**
Form Factor / Dimension	General Specifications	

Architecture	The router shall facilitate all applications like voice, video and data to run over a converged IP infrastructure along with hardware assisted IPSEC & Network Address Translation (NAT),capability. The router should also support hitless interface protection, In-band and out-band management, Software rollback feature, Graceful Restart, non stop routing for OSPF, BGP, LDP, MP-BGP etc. The platform shall have modular software that will run service & features as processes having full isolation from each other	
	The router line card must support following interface: Fast Ethernet, Gigabit Ethernet, Channelized STM1, STM1, STM16, STM64, 10G Ethernet, POS, ATM, V.35 Serial Ports, E1, Chn E1, E3 Ports. Support for these port requirement can be considered optional for Internet routers	
Performance	Backplane Architecture: The back plane architecture of the router must be modular and redundant. The back plane bandwidth must be 20 Gbps from day one with minimum scalability upto 30 Gbps with minimum routing performance of 20 mpps form day one (1) scalble upto 30 mpps, with minimum three (3) open slots.	
	The Router should have individual dedicated control plane processor and data plane processor module. Data plane Processor module should be independent of the control plane Processor. Control plane Processor should have support for internal memory to support multiple software images for backup purposes and future scalability. The router processor architecture must be multi-processor based and should support hardware accelerated, parallelized and programmable IP forwarding and switching.	
	The router should support the IPv4 and IPv6 DUAL-stack in hardware and software. The router should support minimum 450k IPv4, IPv6 routes from day one (1) & scalable to minimum 1MN IPv4, IPv6 unicast routes, should have 56K Multicast routes & 500 IGMP groups from day one.	
Protocol Support	The router shall have RIPv1, RIPv2, RIPng, BGP, OSPFv2 & v3, Policy Based Routing for both IPv4 & IPv6, IP Multicast Routing Protocols to facilitate applications such as streaming, webcast, command & control including PIM SM, PIM SSM, GRE (Generic Routing Encapsulation) Tunneling with 1000 tunnels enabled from day one	
	Router should support following MPLS features – LDP, Layer 2 VPN such as EoMPLS with LDP signaling, Route Reflector (RR), Traffic Engineering with RSVP-TE, Fast Reroute Link Node & Path protection enabled from day one. Support for these features can be considered optional for Internet routers	
QoS Features	The router shall support QoS policy in the router shall support dual Strict Priority Queue or Low Latency Queue per policy so that voice and video traffic can be put in different queue. It also should have hierarchical QOS (Inbound and Outbound) to ensure bandwidth allocation for all type of traffic during congestion and non-congestion scenario.	
	The router shall perform traffic Classification using various parameters like source physical interfaces, source/destination IP subnet, protocol types (IP/TCP/UDP), source/destination ports, IP Precedence, 802.1p, DSCP and by some well-known application types through Application Recognition techniques.	

Security Feature	The router should have support for hardware enabled Network Address Translation (NAT) and Port Address Translation (PAT) . The router shall support NAT6to4 function. Mention the number of sessions that it can support. The router shall support vrf-aware NAT function.	
	The router shall meet the following requirements for security: Access Control List to filter traffic based on Source & Destination IP Subnet, Source & Destination Port, Protocol Type (IP, UDP, TCP, ICMP etc) and Port Range etc. Router should support deep and stateful packet inspection to recognize a wide variety of applications	
	The router shall support firewall service in hardware on all interfaces for enhanced security to protect the backbone from malicious activities. The firewall performance shall be at least 5 Gbps (internal/external). In case of external firewall, bidder should propose the firewall with necessary 10G interface and redundant power supply.	
	Router should have at least 1 Gbps of IPSEC throughput from day one. In case of external VPN box, bidder should propose the hardware with necessary 10G interface and redundant power supply. The proposed router should have embedded support for 2000 IPsec tunnels from day one. The router should support vrf aware IPSEC should have support for Suite-B crypto engine requirements for IKE and IPsec	
Management	The router must support management through SNMPv1/v2/v3, support RADIUS and TACACS. The router must role based access to the system for configuration and monitoring & deep and stateful packet inspection to recognize a wide variety of applications The router shall be provided with IETF standards based feature so that granular traffic analysis can be performed for advanced auditing, usage analysis, capacity planning or generating security telemetry events, also the router shall have SLA monitoring tools to measure state of the network in real time. The SLA operations shall provide information on TCP/UDP delay, jitter, application response time, Packet Loss etc.	
Interface Requirements:	Router should be provided with 6 x 1 GE port with required transceivers as per solution & one 10 gig interface	
Compliance/ Certifications	The Router should be minimum EAL2 / Applicable Protection Profile (NDPP) certified under the Common Criteria Evaluation Program	

7.2.10 Firewall

Sl.No.	Industry Certifications and Evaluations	Compliance (Yes/No)
1	The Firewall solution offered must be rated as 'leaders' or 'Challengers' in the latest Magic Quadrant for Enterprise Network Firewall published by Gartner.	
2	The Firewall offered must be given recommended status by NSS Lab Report.	
	Hardware Architecture	
2	The appliance based security platform should be capable of providing firewall, application visibility, and control, VPN functionality in a single appliance	

3	The appliance should support at least 8 * (1G / 10G) ports and 2 * 40 G ports from Day one and should be scalable to more 2 * 40G ports in future	
4	The appliance hardware should be a multicore CPU architecture with a hardened 64 bit operating system to support higher memory	
5	Proposed Firewall should not be proprietary ASIC based in nature & should be open architecture based on multi-core cpu's to protect & scale against dynamic latest security threats.	
	Performance & Scalability	
6	Should support at least 10 Gbps of production performance / multiprotocol throughput.	
7	Should support at least 8 Gbps of VPN throughput.	
8	Firewall should support at least 4,000,000 concurrent sessions	
9	Firewall should support at least 65,000 connections per second	
10	Firewall should support at least 1000 VLANs	
	Firewall Features	
11	Firewall should provide application detection for DNS, FTP, HTTP, SMTP,ESMTP, LDAP, MGCP, RTSP, SIP, SCCP, SQLNET, TFTP, H.323, SNMP	
12	Firewall should support creating access-rules with IPv4 & IPv6 objects simultaneously	
13	Firewall should support operating in routed & transparent mode	
14	Should support Static, RIP, OSPF, OSPFv3 and BGP	
15	Firewall should support manual NAT and Auto-NAT, static nat, dynamic nat, dynamic pat	
16	Firewall should support Nat66 (IPv6-to-IPv6), Nat 64 (IPv6-to-IPv4) & Nat46 (IPv4-to-IPv6) functionality	
17	Firewall should support Multicast protocols like IGMP, PIM, etc	
18	Should support security policies based on security group names in source or destination fields or both	
19	Should support capability to limit bandwidth on basis of apps / groups, Networks / Geo, Ports, etc	
	High-Availability Features	
21	Firewall should support Active/Standby failover	
22	Firewall should support ether channel or equivalent functionality for the failover control & date interfaces for provide additional level of redundancy	
23	Firewall should support redundant interfaces to provide interface level redundancy before device failover	
24	Firewall should support 802.3ad Ether channel or equivalent functionality to increase the bandwidth for a segment.	
25	Firewall should have integrated redundant power supply	
26	Firewall should have redundant hot-swappable FANs	
	Management	

27	The management platform must be accessible via a web-based interface and ideally with no need for additional client software	
28	The management platform must provide a highly customizable dashboard.	
29	The management platform must be capable of integrating third party vulnerability information into threat policy adjustment routines and automated tuning workflows	
30	The management platform must be capable of role-based administration, enabling different sets of views and configuration capabilities for different administrators subsequent to their authentication.	
31	Should support REST API for monitoring and config programmability	
32	The management platform must provide multiple report output types or formats, such as PDF, HTML, and CSV.	
33	The management platform must support multiple mechanisms for issuing alerts (e.g., SNMP, e-mail, SYSLOG).	
34	The management platform must provide robust reporting capabilities, including a selection of pre-defined reports and the ability for complete customization and generation of new reports.	
35	The management platform must risk reports like advanced malware, attacks and network	
36	The management platform must include an integration mechanism, preferably in the form of open APIs and/or standard interfaces, to enable events and log data to be shared with external network and security management applications, such as Security Information and Event Managers (SIEMs), and log management tools.	

7.2.11 Anti-APT (Advance Persistent Threat)

S No	Feature	Compliance (Yes/NO)
1	Anti-APT solution should be appliance based and should offer a minimum throughput of 2 Gbps	
2	Appliance should support at least 4 * 1Gbps ports and 2 * 10G ports and all ports should have fail-open from day one	
3	Appliance shall provide a separate management port	
4	Appliance should have dual hot-swappable power supplies	
5	Appliance should be capable of working in Inline Blocking mode without depending on other network components like a separate FW, IPS or Web Security Appliance	
6	Proposed solution should include an on-prem sandbox and no file shall be sent outside of our premises	
7	Solution should be capable of blocking callbacks to CnC Servers and threats based on both signatures and behaviour	
8	Propose solution should include On-premise Malware Analysis Solution (sandboxing) appliance should support minimum of 30 virtual machines and should have 2 x 10G ports with intergrated redundant power supply	

9	Proposed Malware Analysis Solution shall use a purpose-built hypervisor, contained in a hardened virtual environment that is designed for threat analysis with built-in countermeasures against malware.	
10	Solution should not only be dependent upon sanboxing and should use techniques like behavioural indicators to analyze action of file and other malware artificats in determining the threats	
11	Proposed solution should be capable of employing an extensive set of contextual information (e.g., pertaining to the composition, configuration, and behavior of the network and its hosts) to improve the efficiency and accuracy of both manual and automatic analysis of detected events.	
12	Proposed solution's detection rules should be based on an extensible, open language that enables users to create their own rules, as well as to customize any vendor-provided rules.	
13	Proposed solution should be capable of blocking threats on the following protocols: HTTP, HTTPS, SMTP, IMAP, POP3, FTP & NetBIOS-ssn	
14	The solution should be capable of executing MS Office Documents, Portable Documents, Archive Files, Multimedia Files and executable binaries in a virtual sandbox environment	
15	The solution should be capable of exempting specific hosts from specific compliance rules and suppressing corresponding compliance events and alerts.	
16	The solution should be capable of gathering Active Directory user identity information, mapping IP addresses to username and passively gathering information about network devices including but not limited to: ●Operating system vendor ●Operating system version ●Network protocols used, e.g. IPv6, IPv4 ●Network services provided, e.g. HTTPS, SSH ●Open ports, e.g. TCP:80 ● Client applications installed and type, e.g. Chrome - web browser ● Web applications access, e.g. Facebook, Gmail ● Risk and relevance ratings should be available for all applications ● Potential vulnerabilities ● Current User ● Device type, e.g. Bridge, Mobile device ● Files transferred by this device / user	
17	The solution should be capable of gathering Active Directory user identity information, mapping IP addresses to username, and making this information available for event management purposes as well as access control policy decisions.	
18	The solution should detect and classify mobile devices as mobile devices. For example: iPad, iPhone and Blackberry devices. These devices should be discovered and related back to the user, applications, and possible services they offer	
19	The solution should be capable of whitelisting trusted applications from being inspected to avoid business applications from being affected & in turn productivity	
20	The solution should be capable of blocking traffic based on geo locations to reduce the attack landscape and to protect communication to unwanted destinations based on geography	
21	The solution shall be able to detect attacks on 64-bit operating systems	
22	All the devices shall be managed centrally and should be capable of • Centralized, life cycle management for all sensors • Aggregating all events and centralized, real-time monitoring and forensic analysis of detected events	

	• Must provide a highly customizable dashboard	
23	The sandbox should be appliance based with the ability to run multiple versions of Windows within the same environment	
24	The Sandbox should be a proprietary custom built malware analysis solution and not open source or generic sandbox	
25	The Sandbox should be a proprietary custom built malware analysis solution and not open source or generic sandbox and should provide:	
	- analysis reports	
	- threat score of the sample	
	- ability to queue samples,	
	- impact analysis	
	- Global Threat Intelligence	
26	Sandbox shall be able to detect memory residing malware	
27	The solution shall have the capability to let the user modify parameters within the VM to observe changes in malware behavior	
28	The proposed solution shall have the capability to continuously track a file's disposition based on global intelligence and do a retrospective block and alert if the file has exhibited malicious traits globally even if the file hasn't started behaving maliciously locally	

7.2.12 Network Behavior Analysis

S. No.	Minimum Requirement Description	Compliance (Y/N)
1	Should have an automated discovery function to identify network devices and capture information such as IP address, OS, services provided, other connected hosts.	
2	Should capture signature / heuristics based alerts and block the same	
3	Should Identify the source of an attack and should not block legitimate users	
4	Should identify worms through techniques such as identifying the use of normally inactive ports or identification of network scanning activities	
5	The solution should be capable of detecting denial-of-service (DoS) and distributed denial-of-service (DDoS) attacks including floods of all types (ICMP, UDP, TCP SYN, TCP NULL, IP NULL etc.), identify the presence of botnets in the network, identify DNS spoofing attack etc.	
6	Should be capable of conducting protocol analysis to detect tunneled protocols, backdoors, the use of forbidden application protocols etc.	
7	Should utilize Anomaly detection methods to identify attacks such as zero-day exploits, self-modifying malware, attacks in the ciphered traffic or resource misuse or misconfiguration.	

8	The solution should Integrates with Microsoft Active Directory, RADIUS, and DHCP to provide user Identity information in addition to IP address information throughout the system & allow groups based on Identity or Active Directory workgroup & Provides full historical mapping of User Name to IP address logins in a searchable format	
9	Should support the capability to instruct network security devices such as firewalls to block certain types of traffic or route it to quarantine VLANS	
10	Should support the capability to alert the admin and provide mitigation action like quarantine or block the endpoint or custom scripts like ACL push or block the further spread of the malware/worm while allowing legitimate traffic to continue	
11	The system should be able to monitor flow data between various VLANS	
12	Should support the capability to identify network traffic from high risk applications such as file sharing, peer-to-peer, etc.	
13	Should support the capability to link usernames to IP addresses for suspected security events.	
14	Should support the capability to extract user defined fields (including source and destination IPs, source and destination MAC address, TCP/UDP ports or ICMP types and codes, no. of packets and no. of bytes transmitted in a session, timestamps for start and end of session etc.) from captured packet data and then utilize fields in correlation rules.	
15	Should support the capability Application profiling in the system and should also support custom applications present or acquired by the bank/customer	
16	Solution should be compatible with a virtual environment.	
17	The solution should provide access to raw as well as processed logs	
18	Dashboard should have the facility to be configured according to user profile	
19	System should support event forwarding for SMTP, SYSLOG & SNMP for high risk issues	
20	The solution must allow analysis by grouping of network segments such as User VLAN, Management VLAN, Server Farms etc.	
21	Solution should be able to track user's activities locally and remote network sites and should be able to report usage behavior across the entire network.	
22	Solution should support ubiquitous access to view all reporting functions using an internet browser.	
23	The solution should support the identification of applications tunneling on other ports	
24	Solution should be able to collect security and network information of servers and clients without the usage of agents	
25	The solution should be able to conduct de-duplication of redundant flow identified in the network to improve performance	
26	The solution should have the ability to statefully reassemble uni-directional flows into bi-directional conversations; handling de-duplication of data and asymmetry	
27	The solution should support all forms of flows including but not limited to cisco netflow, juniper jflow, sflow, ipfix for udp etc.	
28	The solution should be able to combine/stitch the flow records coming from different network devices like routers/switches/firewall that are associated with a single conversation and present them as a single bi-directional flow record	
29	The solution should be able to stitch flows into conversations even when the traffic is NATted by the firewall; clearly showing the original and translated IP address	
30	The solution should be able to leverage external threat feeds for information about known CnC connections, botnets, Tor exit nodes, etc.	

	Network performance	
1	Solution should provide application bandwidth utilization graph for various applications which should include bandwidth consumption for top hosts and trends on network bandwidth utilization.	
2	Solution should probe the network in a manner so that impact on network performance is minimal.	
3	Should support both in line and offline modes.	
4	The tool should have a system for interactive event identification and rule creation	
5	Devices / applications those do not support flows, the solution should be capable to generate its own flows for monitoring.	
6	Solution should have facility to assign risk and credibility rating to events.	
7	Solution should support traffic rate up to 1 Gbps	

7.2.13 Web Security Appliance

S. No.	Technical Specification	Minimum Requirements	Compliance (Y/N)
1	Appliance Requirement and Functionality	The solution should be a hardened Web Proxy, Caching, Web based Reputation filtering, URL filtering, Antivirus and Anti-malware appliance. All the functionalities should be in a single appliance only.	
2	Hardware	Minimum of 1 * 6-core CPUs, 2.4 TB storage, RAID 10, 32 GB or more DRAM, hot-swappable hard drive	
3	Operating System	The appliance based Solution should be provided with hardened Operating System.	
4	Operating System Performance	The underlying operating system and hardware should be capable of supporting atleast 2000 users from day with licenses & scalable upto 5000 users.	
5	Operating System Security	The operating system should be secure from vulnerabilities and hardened for web proxy and caching functionality.	
6	Forward proxy mode	The solution should support explicit forward proxy mode deployment in which client applications like browsers are pointed towards the proxy for web traffic.	
7	Transparent mode	The solution should also support transparent mode deployment using WCCP v2 and L4 switches/PBR (Policy-based Routing)	
8	Pac File support	The appliance should support hosting proxy auto-config files that defines how web browsers can automatically choose the appropriate web proxy for fetching a URL.	
9	Support multiple deployment options	The solution should allow to deploy the appliance in explicit proxy as well as transparent mode together.	
10	Proxy Chaining	The solution should support proxy configuration in a Chain. The Lower end proxies at spoke locations should be able to forward the request to an Higher end proxies at	

		Hub Location forming a Chain of Proxies	
11	DNS Splitting	The solution should support configuration to use Split DNS. It should be able to refer to different DNS for Different Domains e.g. (root dns for all external domains and internal DNS for organization domain	
12	IP Spoofing support in transparent mode deployments	The solution should have facility to do IP spoofing. When enabled, requests originating from a client should retain the client's source address and appear to originate from the client instead of the appliance. This is useful in scenarios where policies are based on original IP and logging/reporting is required to track activity of individual IP basis.	
13	High Availability	Provision of active/active High Availability is required	
14	Proxy support	The proposed solution should be a Fast Web Proxy and should support HTTP, FTP and HTTPS proxy.	
15	HTTPS Decryption	The solution should support HTTPS decryption	
16	HTTPS decrypted traffic scanning	The solution should support scanning of the https decrypted traffic by the on-board anti-malware and/or anti-virus engines.	
17	HTTPS decryption policy	HTTPS decryption should provide flexibility to have multiple decryption policies and should not be just a Global action	
18	File download and size restrictions	The solution should be capable of blocking specific files downloads and based on size and per user group basis. It should also provide option to block object using MIME File types.	
19	IP based Access Control	The solution should allow administrator to define access to internet based on IP addresses, range of IP addresses, subnet and CIDR basis. It should also support to be forced for Authentication from Specific IP addresses, Subnet or CIDR's	
20	User based Access Control	The solution should support integration with active directory and/or LDAP. This should allow administrator to define user or group based access policies to Internet	
21	Multiple Authentication Server Support	The solution should support Multiple Auth Servers / Auth Failover using Multi Scheme Auth (NTLM and LDAP). It should also support authentication exemption.	
22	Application and Protocol Control	The solution should support granular application control over web eg. Facebook controls like block file upload, block posting text, enforcing bandwidth limits on application types.	
23	Layer 4 Traffic Monitoring	Should detect Phone Home attempts occurring from the entire Network. It should support actions to allow traffic to & from known allowed & unlisted addresses & block traffic to & from known malware addresses & should support monitoring suspected malware addresses.	
24	Bandwidth restrictions	The solution should support providing bandwidth limit/cap for streaming media application traffic. This should be possible at the Global level as well as at a per policy level.	
25	Anti Malware	The appliance should support at least 2 industry known Anti Malware/Anti-Virus engine that can scan HTTP, HTTPS and FTP traffic for web based threats, that can range from adware, browser hijackers, phishing and pharming attacks to more malicious threats such as rootkits, Trojans, worms,	

		system monitors and Keyloggers and as defined by the organizations policy. Please mention the antimalware engine.	
26	Anti-Malware	With dual AV/Anti-Malware engine scanning when a URL causes different verdicts from the scanning engine the appliance should perform the most restrictive action.	
27	Web Reputation	The solution should provide Web Reputation Filters that examine every request made by the browser (from	
28		the initial HTML request to all subsequent data requests) – including live data, which may be fed from different domains to assign a web based score to determine the likelihood that it contains url-based malware.	
29	Customizable Web Reputation	The Appliance should have customizable setting in the Web Based Reputation Services, like Allow, Scan and Block based on the scoring settings by the Administrator.	
30	Incoming/Outgoing Traffic scanning	The solution should scan for Incoming and outgoing traffic.	
31	Outbound connection control on all ports and protocols	The solution shall provide option to scan all ports at wire speed, detecting and blocking spyware activity trying to connect to the outside Internet. By tracking all 65,535 network ports and all protocols, the solution shall effectively mitigate malware that attempts to bypass Port 80	
32	Custom URL filtering	The solution should support creation of custom URL categories for allowing/blocking specific destinations as required by the Organisation.	
33	Url Filtering Options	The web Proxy should support following actions like allow, monitor, block, time-based access. Should also support displaying a warning page but allows the user to continue clicking a hypertext link in the warning page.	
34	Dynamic Categorization	Provision should be available to enable Real Time Dynamic categorization that shall classify in real time in case the URL the user is visiting is not already under the pre-defined or custom categories database.	
35	Reporting Mis- categorization	The solution should have facility for End User to report Mis-categorisation in URL Category.	
36	URL check & submission	Support portal should give facility to end user to check URL category and submit new URL for categorization	
37	Filtering Content	Solution should support filtering adult content from web searches & websites on search engines like Google.	
38			
39	Signature based application control	The solution should support signature based application control.	
40			
41	End User Notification	Solution should support following end user notification functionalities.	
42		The proxy should support the functionality to display a custom message to the end user to specify the reason the web request is blocked.	

43		When the website is blocked due to suspected malware or URL-Filters it should allow the end user to report that the webpage has been wrongly misclassified.	
44		The solution should support the functionality of redirecting all notification pages to a custom URL to display a different block page for different reasons.	
45		Should support the functionality to force users to explicitly agree to the terms and conditions for browsing the World Wide Web from the organization's network to let the user know that the Organisation is monitoring their web activity.	
46	Remote support	The remote support from principal company should be available via India Toll Free and Email. The Support Portal access should be provided for Case management, knowledgebase, new version information, tools etc.	
47	Secure Remote Access	The Support Engineers should be able to login to appliance using secure tunneling methods such as SSH for troubleshooting purposes	
48	Diagnostic Tools	The appliance should have diagnostic network utilities like telnet, traceroute, nslookup and tcpdump/packet capture.	
49	Updates and Upgrades	The appliance should provide seamless version upgrades and updates.	
50	Secure Web Based management	The appliance should be manageable via HTTP or HTTPS	
51	CLI based management	The appliance should be manageable via command line using SSH	
52	Serial Console access	For emergency, the appliance should have serial console access	
53	Ethernet Management	Should have provision for separate Ethernet for managing the appliance	
54	Web Logs	The Proxy Log should be scalable. The log formats shall include Apache, Squid and W3C.	
55	Retention Period	The retention period should be customizable. Options should be provided to transfer the logs to an FTP server using FTP or SCP.	
56	User Reports	Informative and exhaustive set of reports on User Activity and URL filtering activities (GUI to report past activity, top usage users and top malware threat)	
57	Bandwidth Reports	Reports on Bandwidth Consumed / Bandwidth Saved	
58	Detailed logging	Product to maintain detailed proxy access logs that can be searched via filters, for easy location of any desired access of the user and to see how the product dealt with it	
59	Blocked by reputation &malware reports	It should support reporting web requests blocked due to web reputation & blocked by malware	
60	Report Formats	Solution should support generating a printer-friendly formatted pdf version of any of the report pages. Should also support exporting reports as CSV files.	

61	Scheduling of Reports	Solution should support to schedule reports to run on a daily, weekly, or monthly basis.	
62	System Reports	Should support system reports to show CPU usage, RAM usage, percentage of disk space used for reporting & logging.	
63	Updates and Upgrades	Support should cover all upgrades for the time period the licenses and support purchased from principal vendor	
64	IP V6 Support	Should have the ability to proxy, monitor, and manage IPv6 traffic.	

7.2.14 IPS

S. No.	**Specifications**	**Compliance (Yes/No)**
1	Advanced Threat Protection	
1.1	The proposed solution must be based on standard computer technology (not ASICs) so that future enhancements and protocols do not require hardware refresh to support. The proposed solution platforms must be based on a hardened operating system.	
1.2	The detection engine must be capable of operating in both passive (i.e., monitoring) and inline (i.e., blocking) modes.	
1.4	Detection rules must be based on an extensible, open language that enables users to create their own rules, as well as to customize any vendor-provided rules.	
1.5	The detection engine must be capable of detecting and preventing a wide variety of threats (e.g., malware, network probes/reconnaissance, VoIP attacks, buffer overflows, P2P attacks, zero-day threats, etc.).	
1.6	The detection engine must incorporate multiple approaches for detecting threats, including at a minimum exploit-based signatures, vulnerability-based rules, protocol anomaly detection, and behavioral anomaly detection techniques. Identify and explain each type of detection mechanism supported.	
1.7	The detection engine must inspect not only Network Layer details and information resident in packet headers, but a broad range of protocols across all layers of the computing stack and packet payloads as well.	
1.8	Sensors must be capable of performing packet-level forensics and capturing raw packet data in response to individual events without significant performance degradation.	
1.9	The solution must be capable of detecting and blocking IPv6 attacks.	
2	Advanced Malware Protection	
2.1	The solution must be capable of providing network-based detection of malware by checking the disposition of known files in the cloud/on premises using the SHA-256 file-hash as they transit the network (SHA-256 and target IP address should be given to aid remediation efforts).	
2.2	The solution must provide full contextual awareness (user, application & content) with respect to malware detection, propagation and retrospective remediation	
2.3	The solution must be able to track APTs that involve multiple threat elements and associate malware child processes to their parents	
2.4	The solution must run in a stylized sandbox environment that can be used to identify the	

	unknown malwares.	
3	Application visibility and URL Filtering	
3.1	Should support Application Visibility and Control (AVC) supports more than 10000 application-layer and risk-based controls that can invoke tailored intrusion prevention system (IPS) threat detection policies to optimize security effectiveness.	
3.2	Proposed appliance should also provide Reputation- and category-based URL filtering offers comprehensive alerting and control over suspect web traffic and enforces policies on hundreds of millions of URLs in more than 50 categories	
4	Real-Time Contextual Awareness	
4.1	The solution must be capable of passively gathering information about network hosts and their activities, such as operating system, services, open ports, client applications, and vulnerabilities, to assist with multiple activities, such as intrusion event data correlation, elimination of false positives, and policy compliance.	
5	Intelligent Security Automation	
5.1	The solution must be capable of employing an extensive set of contextual information (e.g., pertaining to the composition, configuration, and behavior of the network and its hosts) to improve the efficiency and accuracy of both manual and automatic analysis of detected events.	
5.2	The solution must be capable of dynamically tuning IDS/IPS sensors (e.g., selecting rules, configuring policies, updating policies, etc.) with minimal human intervention.	
5.3	The solution must be capable of automatically providing the appropriate inspections and protections for traffic sent over non-standard communications ports.	
6	Control Compliance	
6.1	The solution must support creation of user-defined application protocol detectors.	
6.2	The solution must have content awareness with comprehensive file detection policies and blocking of files by types, protocols and directions.	
6.3	- Protocols: HTTP, SMTP, IMAP, POP	
6.4	- Direction: Upload, Download, Both	
6.5	- File Types: Office Documents, Archive, Multimedia, Executable, PDF, Encoded, Graphics, and System Files.	
7	Reporting and Alerting	
7.1	The management platform must provide robust reporting capabilities, including a selection of pre-defined reports and the ability for complete customization and generation of new reports.	
	Availability	
9.1	Sensors must support built-in capability of failing open, such that communications traffic is still allowed to pass if the inline sensor goes down.	
8	Performance	
8.1	Should have minimum Inspected throughput of 10 gbps for all kinds of real word traffic, this is minimum performance required though the required throughout need to be sized by bidder as per their solution.	
8.2	Should support minimum 3,500,000 Concurrent Connections and atleast 180,000 new connections per second	

8.3	Should have minimum 8 monitoring interface of 4x 1 Gbps Copper + 4 x 10G SR	
8.4	Latency should be < 150 microseconds.	
8.6	Must have dedicated 10/100/1000 RJ45 Management Interface.	

7.2.15 Network Management System for LAN Switches

S. No.	Network Management System for LAN Switches	Compliance (Yes/ No)
1	Management system should provide a single integrated solution for comprehensive lifecycle management of the wired and wireless LAN (of same OEM), and should support rich visibility into end-user connectivity and application performance assurance issues	
2	The NMS should support an open database schema, configuration, administration, monitoring and troubleshooting of Switches, guided workflows based on best practices with built-in configuration templates, the capability to view the network topology, Layer 2 Services and Fault Management	
3	The NMS should automatically discover IP devices, SNMP compliant network devices on the network	
4	The NMS should support Inventory management of Network devices, should support Monitoring and troubleshooting of Devices, should support configuration management and reporting.	
5	The NMS should support flexible reporting for inventory, user tracking, compliance, switch port usage and end-of-sale	
6	The NMS should provided on dedicated appliance/ installed as a virtual appliance/ Intel based severs/ AMD based server and should support installation on Windows/ Linux	
7	**Support for Wireless Management Features (Same functionality can be provided via separate Wireless management system but same should be able to integrate with Wired Management system to implement unified policies)**	
8	Must show location information of clients, infrastructure Access Points, Rogue Access Points, and RF tags in a map format.	
9	Must support following features	
10	Wireless LAN Planning and Design, Network Monitoring and Troubleshooting, Indoor location monitoring capability, Wireless IPS management, Centralized Software updates, Network mapping with floor plans for easier automated site survey	
11	Shall provide in-depth visibility of finding, classifying, correlating, and mitigating interference from Wi-Fi and non-Wi-Fi sources such as rogue access points, microwave ovens, Bluetooth devices, and cordless phones.	
12	Should provide deep integration with the authentication; authorization, posture & Profiler to further extend the visibility across security and policy-related problems, presenting a complete view of client issues with a clear path to solving them.	

13	Must support virtualization, whereby wireless resources (APs, controllers, geographical areas) can be divided into logical domains and administrator access limited to specific domains.	
14	NMS has to be from the same OEM as of Switches	

7.2.16 DG Set
(for Electric load of ICCC & DC including air-conditioning)

#	Item	Minimum Specifications
1	General	□ Auto Starting DG Set mounted on a common base frame with
	Specifications	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 ICCC
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

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.

7.2.17 Purpose Built Backup Appliance (PBBA) Features

The minimal specifications of PBBA are as below -

- The Disk to disk proposed Backup Appliance shall be modular in design. Scale up to 200 TB and scale out when the data size grows beyond 200 TB.
- The proposed device shall support Deduplication Disk. i.e. providing multiple types of workloads (backup, replication) and interfaces (NFS, CIFS, VTL, OST) to a single deduplication system.
- The proposed device shall have the capability to deliver selective restore from disk Library itself.
- The proposed device shall have integrated de-duplication license for the suggested capacity for Deduplication disk as well as NAS and shall have support for replication to remote location in a WAN optimization mode.
- The proposed device shall support intelligence to understand Source based (at client application level, backup server level and media server level) de-duplication so that only
- unique non-duplicated data is copied to the proposed device.
- The proposed device should offer mechanism for taking the backup on a physical tape library from the appliance / management console seamlessly. Consider license/hardware if required.
- The proposed device shall have a minimum of 4 x 1G Ethernet, 4 x 8Gbps Fibre Channel and 4 x 10Gbps Ethernet (Fiber SFP) connections fully populated with modules and connecting cables of 15 mtr.
- The proposed disk based backup device shall also support encryption functionality. To ensure data security, the solution should support data encryption in flight and at rest. The solution should offer data encryption in the physical tape library.
- The proposed disk based backup appliance shall have flexibility to enable or disable the de-duplication for a given duplicated disk.
- The proposed disk based backup appliance shall support VLAN tagging. The proposed IP ports shall also support Port bonding in Adaptive Load balancing, LACP and as well as in Active-backup mode
- The proposed device shall support rated write performance of minimum 10 TB per hour and when enabled with source level de-duplication, shall have rated performance of at least 30 TB/hr.
- The Backup software running on the proposed backup appliance must be industry proven and must have been generally available in the market for at least 5 years.
- It is preferred that proposed backup solution may provide a -turnkey|| fully integrated backup solution (Backup Appliance and Backup Software) from a single OEM.
- It is preferred that the Proposed Backup solution may provide management of the backup software and dedupe appliance from the same console.
- The proposed disk based backup appliance must be capable to act as a Backup Controller/Backup Server, Data Mover/Media Server simultaneously.
- The appliance must offer multiple levels of deduplication optimizations, including intelligent, application aligned deduplication.

- The Proposed Backup dedupe Appliance license should not be tied to the storage device. This means if another appliance is installed at the DR site, then the appliance will not need separate dedupe license or any other software license.
- The proposed Appliance should have inbuilt WAN optimization capabilities and also be tolerant to complete or intermittent network failures or TCP packet drops.

7.2.18 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

7.2.19 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.

7.2.20 Meeting Room Based Video conferencing Solution

Features	Specifications	Complied (Yes/No)
Form Factor	The solution should be an OEM integrated system with a single 55" LCD display, codec, camera, Microphones and touch panel. All the components 55" LCD display with floor mounting kit, codec, camera, microphones, and touch panel should be from the same OEM. The OEM website should have information of the quoted product along with the brochures	
Video Standards	H.263, H.264	
	H.264 should be possible when sending or receiving two live video sources e.g. Presenter and Presentation.	
Video Frame Rate	Should support 60 fps with 1080p resolution from day one	
Video Features	Ability to send and receive two live simultaneous video sources in a single call, so that the image from the main camera and PC can be seen simultaneously.	
	Should support H.239 and BFCP protocols with High definition resolution for presentations	
Video Output	The system should be an OEM integrated solution with a single 55" LCD Monitor	
Video Input (2 HD Video Inputs)	Should have at least one HD video Input to connect HD camera with full functionalities as mentioned in the camera specifications below.	
	Should have DVI (Digital Video Interface)/HDMI input to connect PC / Laptop directly to the Video conferencing system and display resolutions WXGA / HD720p along with PC Audio.	
Audio standards supported	G.711, G.722, G.722.1, 64 kbps MPEG-4 AAC-LD or equivalent standard must be supported..	
Other Desirable features	Noise Reduction, Automatic Gain control, Acoustic Echo Canceller	
Audio Interfaces	The system should have 2 table top microphones day one.	

	The microphones must be standard based microphones.	
	The pickup of the microphones should be at least 10 feet from the microphone.	
	Echo Cancellation for every input must be available.	
	The system should have integrated speakers as part of the display	
Network Interfaces	1 LAN / Ethernet - 10/100/1000 Mbps full duplex	
Bandwidth	IP bandwidth upto 4Mbps	
Network Capabilities	Packet Loss Based Down-speeding	
H.323/ IP Features	Differentiated Services(QOS):	
	Auto Gatekeeper discovery	
	Auto Network Address Translation(NAT) support	
	Standards based- Packet Loss Recovery feature on H.323 call	
	Should support URL Dialing	
SIP Features	The endpoints must support SIP in addition to H323 protocol	
Security		
Menu Control	Password protected system menu	
Encryption of video call	ITU-T standards based Encryption of the video call	
	Call should be encrypted end-to-end on IP	
	Should support Standards-based: H.235 and AES Encryption via Automatic key generation and exchange.	
	Ability to manually turn encryption On or OFF should be there.	
	Automatic key generation and exchange	
Camera	CMOS or equivalent	
	Minimum of 8x or more zoom	
	1920 x 1080 pixels progressive @ 60fps	
	Should have at least 65 degrees field of view (horizontal)	
Directory services	Should support Local and Global directories.	
	Should support LDAP and H.350 protocols for directory transfer.	

7.3 Centralized Video Portal with Centralized distribution engine

S.N.	**Feature Description**	**(Yes / No)**
1.	**System Architecture**	
	Should have active-active High Availability	
	Solution should support load balancing between redundant servers and set failover paths	
	Should support virtualization based servers and provide for dynamic resource allocation of hardware	
	Should support auto retry by client in case of connection failure or interruption in the flow of video stream	
	Should support multi-tenancy	
	Integrated encoder support	
	Should support user defined branding / skinning to provide customer environment look	
	Should support 40 classrooms to start and capable of expanding to 500 classrooms in future by just adding required licenses	
	Should provide native integration to Active Directory environment for security and user authentication	
	Should support allocation / Access rights of media to selective AD Users & Groups. This ensures that only content pertinent to a specific AD user/Group is viewable	
	Portal should allow authorized users to both upload and view content via an intuitive and device agnostic browser based flexible UI	
	Should have the capability of configuring and managing the components like Remote Distribution servers for directing the users to local server for bandwidth optimization	
	All video content shall be managed and delivered via the Video Portal application, including:	
	Existing video media archives, with ability to upload and transcode in batches	
	Live Webcasts and subsequent recordings	
	New VOD video media uploaded from various sources, including encoders, mobile, tablet & desktop devices and 3rd party sources	
	Professional cameras / IP Camera / Video Conferencing feeds if required	
	Integration with the proposed recording servers, Video conferencing ends and MCU's	
	Solution should support segregating User access depending on department or organization or role. Users will be members of a corresponding group and specifically have access only to a collection containing content for that group	
	One user can be part of multiple groups and should be able to view and publish the videos to all its member groups	
	User should be able to define the content as public or private. Public content shall be viewable to everyone, where as Private content should be viewable to only designated groups or users	

	Should support all the major browsers like Internet Explorer, Firefox, Chrome and Safari	
	Should have inbuilt transcoding functionality and system should do the transcoding as per the device profile (like Web, mobile)	
	Should support embedding of the video content on a web page by taking the embed code and inserting content into another site or web page	
	Integrated video and webcast recording	
	PLAYBACK and STREAMING: Should have inbuilt media player and streaming server for VoD playback and live streaming	
	Playback should happen on the portal page only. Application should not ask for opening any specific media / video player	
	Inbuilt player should support the following	
	Full Screen viewing	
	Slider functionality for forward, rewind of video	
	Sound level adjustment	
	Pause / Resume	
	Duration	
	Flexible architecture that allows dynamic addition of compute resources and customizable services running on the various different servers (Authentication, Transcoding, Web services, etc.)	
2.	**Content Management**	
	User should be able to publish content from Desktop/Laptop, Mobile Device or External hardware encoders. This should be for both VoD and Live Streaming	
	Allow users to upload a pre-recorded content and define access to specific groups or public channels	
	Should support ingest of live video from Video conferencing devices over H.264/SIP	
	Should support various formats of pre-recorded video content (Wmv, avi, mp4, mpg, mov, mpeg, FLV etc) to be uploaded to the portal. If system stores the content in one type of format only (say mp4), then format conversion should be done the system automatically, without any additional work to user	
	The solution should include recording server to enable the video systems reach the wider audience by streaming or recording content of a videoconference	
	Should support Create, update, delete a video by user	
	Allow user to edit the thumbnails of the video	
	Should have control functionality for downloading of content by the users	
	There should be option to enable approval of content prior to publication	
	Administrator should be able to override the workflow to publish or remove content on ad-hoc basis	
3.	**Integration**	

	Integration support via open APIs	
	Should integrate with LDAP/AD for user authentication, SSO and user group access	
	Should provide for APIs to integrate with 3rd party frontend to video solution for content uploading, managing/editing, deleting, viewing, searching etc	
	Should allow user to share the video by sending link to video by email/chat to others	
	Should support modern web technologies like web sockets/ CSS3/ HTML5 etc	
	Users should be able to rate the video content (on a scale of 1-5 or equivalent)	
	Allow users to comment on the video	
4.	**Administration & Monitoring**	
	Should provide for GUI based setup and management engine	
	Should provide for User Management (Add, Edit, Access rights etc..), Video Management (Add, Edit, Delete, Highlight, Expire etc..)	
	Should provide for system alerts (via monitoring module or SNMP traps to Central NMS)	
	Single pane of glass to administer Portal and content distribution (configure IP ranges and distribution rules from portal interface)	
5.	**User Access**	
	Each user should have their own home page if required. User shall be able to upload videos and share with others using options on home page	
	Home page shall have clearly defined preferences / settings tab to enable user to administer their preferences, edit content etc	
	Access to self portal should be via browser to enable cross device support (like responsive UI, video type support across Mac, Windows, Mobile devices)	
	Home page should display contents of all the groups/channels the user have access to, with clear separation of each channel content	
	User access should be based on LDAP/AD	
	User should be able to search content based on various parameters like:- Name, Upload Date range, Group, Topic etc	
6.	**Storage, Archiving & Security**	
	System should have robust backup functionality for content/videos, user profiles, stats, preferences and customizations	
	Provide ability to bring back the system in minimal time in case of any exigency	
	Should support SAN/NAS for content storage	
	Should support encryption (min AES-128 bit) with integrated key management	
	Should have automated process of data achieving as per the defined parameters	
7.	**Reporting, Monitoring & Analytics**	
	Should provide detailed reports based on users, groups/channels and site basis	

	There should be standard reporting templates available in the system, with the option to customize the reports as per the need	
	Should provide real-time system health analytics	
	Administrator should be able to define thresholds for various critical events, and system should alert once the thresholds are breached	

7.4 High end Interactive Conferencing Device at Central Location

High end Interactive Conferencing Device with 2 Cameras - 1 No. at Central Location

S.N.	Specifications	(Yes / No)
1.	**Video Standards**	
	H.263, H.264	
	H.264 in an Encrypted call should be possible	
	H.264 should be possible when sending or receiving two live video sources e.g. Presenter and Presentation.	
	Should support 30 fps & 60fps (frames per second) with 1080p resolution from day one	
2.	**Video Features**	
	Ability to send and receive two live simultaneous video sources in a single call, so that the image from the main camera and PC or document camera can be seen simultaneously.	
3.	**Video Output**	
	Should have at least 3 nos. of HD (High Definition) output to connect Full High Definition display devices such as plasma and projectors for both Video and content.	
	The unit must provide the flexibility to display video or content one any of the video output.	
4.	**Video Input**	
	Should have at least 3 HDMI inputs to connect multiple HD cameras.	
	Should have one HDMI / DVI (Digital Video Interface) input to connect PC / Laptop directly to the Video conferencing system and display resolutions from WXGA (1280 x 768) to 1080p (1920 x 1080)	
5.	**Audio standards supported**	
	G.711, G.722, G.722.1, 64 kbps MPEG-4 AAC-LD or equivalent standards must be supported.	
6.	**Audio Inputs**	
	Should support minimum 8 Microphone inputs.	
	The system must have the capability to mix the audio from all the microphones and the line input and send the same to the far end side.	
7.	**Network Interfaces**	

	1 LAN / Ethernet - 10/100/1000 Mbps full duplex	
	Should have support for IPV4 and IPV6	
8.	**Bandwidth**	
	IP - at least 6 Mbps	
9.	**SIP Features**	
	The endpoints must support SIP in addition to H323 protocol. Calls can be made on SIP or H323 without having to restart or reconfigure the endpoint.	
	The endpoint must register with any standard SIP server.	
10.	**Security**	
	Password protected system menu	
	ITU-T standards based Encryption of the video call	
	Call should be encrypted end-to-end on IP	
	Should support Standards-based: H.235 v3 and AES Encryption via Automatic key generation and exchange. The same should be available in a call with Video with presentation (dual video)	
11.	**Cameras**	
	1/3" CMOS or better, 2 cameras to be given from day one.	
	Minimum of 10X Optical zoom	
	1920 x 1080 pixels progressive @ 60fps	
	The Camera and codec should be from the same manufacturer.	
	Should have at least 70 degrees field of view (horizontal)	

7.5 Audio Video Bridging Unit at Central Location

S.N.	**Feature Description**	**(Yes / No)**
1.	**System Capacity**	
	Conferencing System should have minimum 40 ports at 1080p 60fps on IP in continuous presence mode with 60fps and H.264 resolution and AES encryption.	
	It should as well provide network flexibility for a reliable distributed architecture and cost-effective scalability for future requirements.	
	Conferencing System should be deployed in High Availability and should be redundant (1:1)	
	It should have internal inbuilt hot swappable redundant power supply.	
	It should provide flexibility to the schools, where they can join the online fully two-way interactive live session using WebRTC compatible browser. This facility should be available from day one.	

	It should be possible for 20 schools to join with WebRTC compatible browser, where following features should be available.	
	1080p, 720p & SD should be supported over WebRTC	
	Users should be able to connect at 250kbps (lowest bandwidth) over video using WebRTC	
	Support content sharing, desktop sharing & application sharing, XMPP registration	
	Should support audio protocol OPUS and video protocol VP8 over WebRTC	
	Should be able to add participants to the call through the WebRTC	
	Video Call connected on browser, should be easily moved to the external VC endpoint	
2.	**Video Standards and Resolutions**	
	It should support H.263, H.264, WebRTC	
	It should support 1080p 60fps, 30 fps, 720p 30 and 60 fps.	
3.	**Content Standards and Resolutions**	
	Content sharing should be possible at 1080p 30fps	
	It should support H.239 and encryption in SIP & H.323 modes	
4.	**Audio Standards and Features**	
	It should support G.711, G.722, G.722.1	
	It shall support aspect ratio of 16:9 and 4:3.	
	It shall support a mix of resolutions in both Voice activated mode and Continuous Presence. Each endpoint shall receive at the maximum of its capacity without reducing the capacity of another.	
	Dynamic CP layout adjustment (it will choose the best video layout according to the number of participants in the conference).	
	It should support distributed architecture with intelligent and automatic call routing. It must support load balancing such that in case there are two instances, conference participants can get distributed across these two instances based on their locations and still join into the same conference.	
5.	**Network and security features**	
	It shall support AES encryption 128 bit or above for every participant without affecting any other feature, functionality or port count.	
6.	**Interoperability**	
	Bridging infrastructure should be standards based and should be compatible with other open standards H.264 AVC based solutions.	
	General: OEM of the bridging Unit, Conferencing device, management, scheduling must be in leaders’ quadrant of latest Gartner Magic Quadrant report for Group video systems.	

7.6 Management & Scheduling at Central Studio Location

S.N.	Feature Description	(Yes / No)
1.	**System**	
	The central management solution should be able to schedule meeting quickly and easily manage conference infrastructure device configuration and provision of endpoint.	
2.	**System Capacity**	
	The Central management server must support 100 devices capacity from day one and must be scalable to support minimum 250 devices in future through software license.	
3.	**Provisioning**	
	The administration should be able to configure individual end points or group of end points using user policy from single management console.	
	It should be possible for the endpoint to automatically pull the device and site provisioning information from the system while start up.	
4.	**Software Update**	
	It should be capable of automatic and scheduled mechanism to upgrade the software on one or more endpoints with a standard software package thereby eliminating the need to upgrade each endpoint individually.	
5.	**Scheduling**	
	The system should support schedule video conference meetings.	
6.	**Directory Services**	
	Should support integration with the corporate Active Directory for scheduling the video conference calls.	
	The system should store video dialing information.	

7.7 Recording Platform

S.N.	Feature Description	(Yes / No)
	The recording solution must be standards based. The solution server should be from the same OEM.	
1.	**Application Features**	
	Records single point and multipoint conferences with full H.239 and BFCP content capture	
	High definition (HD) support with 720p or better H.264 video	
	API support for third party integrations	
	H.323 or equivalent standards-based for use with third party conferencing systems	
	Integrates with MCU for simple recording of multipoint video conferencing	
2.	**Audio / Video Support**	

	Live Video Resolutions: C(S)IF, 4CIF, SD, 720p HD or better	
	Video Support: H.261/ H.263/H.263+/H.263++/ H.264	
	Audio support: G.711 / G.722 /G.722.1 or better	
3.	**Recording**	
	Should support minimum 5 concurrent multi party HD720p video conferencing recording sessions with full video, audio and content.	
	Records video at varying bit rates -128 Kbps to 2 Mbps	
	System should support Multiple methods for recording – directfrom a Room based endpoint, Desktop endpoints, MCU / bridge or from the admin user interface	
	All of the Media Library should be exportable a CD/DVD	
4.	**Security**	
	AES media encryption	
	TLS/SSL and HTTPS Support	
	Should be "19" Rack mountable and Dual redundant power supply	
5.	**Management**	
	A separated Web Interface for the Administration is required.	
	The Administrator must be able to upgrade each server / appliance component using the WebUI	
	The appliance has to be centralized configured and managed by theManagement System	

7.8 Online UPS

S.No.	**Parameter**	**Minimum Specifications**	**Compliance (Yes/No)**
1.	Capacity	Adequate capacity to cover all above IT Components at respective location	
2.	Output Wave Form	Pure Sinewave	
3.	Input Power Factor at Full Load	>0.90	
4.	Input	Three Phase 3 Wire for over 5 KVA	
5.	Input Voltage Range	305-475VA Cat Full Load	
6.	Input Frequency	50Hz+/-3 Hz	
7.	Output Voltage	400 VAC, Three Phase for over 5KVA UPS	
8.	Output Frequency	50Hz+/-0.5%(Free running);+/-3%(Sync. Mode)	
9.	Inverter efficiency	>90%	
10.	Over All AC-AC Efficiency	>85%	

11.	UPS shutdown	UPS should shut down with an alarm and indication on following conditions 1) Output over voltage 2) Output under voltage 3) Battery low 4) Inverter over load 5) Over temperature 6) Output short	
12.	Battery Backup	30 minutes in full load	
13.	Battery	VRLA(Valve Regulated Lead Acid) SMF (Sealed Maintenance Free) Battery	
14.	Indicators & Metering	Indicators for AC Mains, Loadon Battery, Fault, Load Level, Battery Low Warning, Inverter On, UPS on Bypass, Overload, etc. Metering for Input Voltage, Output Voltage and frequency, battery voltage, output current etc.	
15.	AudioAlarm	Battery low, Mains Failure, Over temperature, Inverter overload, Fault etc.	
16.	Cabinet	Rack/Tower type	
17.	OperatingTemp	0 to 40 degrees centigrade	

7.9 KVM Module

S.N.	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	US BorKVM over IP.
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 fail over and built-in surge protection
10.	Multi-User support	It should support multi-user access and collaboration

7.10 Surveillance solution requirement

7.10.1 Type 1- 360° Panoramic Camera

S.NO.	Camera Characteristics	Compliance (Yes/No)

1	General Requirements	Multi-view layouts: 360° surround views and multi-region client dewarped views, with Digital PTZ functionality.	
2	General Requirements	The camera should be based upon standard components and proven technology using open and published protocols. Device functionality can be extended by installing and running applications directly on the camera, for example SIP client, video analytics, audio analytics, etc.	
3	Image Sensor	1/2.5″ Progressive	
4	Lens Specs	Focal length: 1.5mm, Maximum aperture: F2.8	
5	Resolution	Active Pixels 1920(w) x 1920(h)	
6	Minimum illumination	Color mode: 0.6 lux Black/White mode: 0.01 lux, 0 lux with illuminator active, The infrared illuminator should light an area up to 33 feet (10 meters) away	
9	Day/Night	Automatic, Manual, Scheduled	
10	Image Compression	H.264 and Motion JPEG	
11	Frame Rate	25fps for PAL mode	
12	Local Storage	32GB	
13	Streaming	The camera shall be able to setup and stream out two (2) stream profiles.	
14	White Balance	Auto / Manual	
15	Wide dynamic range	70dB	
16	Shutter Speed	1/5 second to 1/32,000 second	
17	Ethernet	10/100/ Base-T (RJ45)	
18	Field of view	180° horizontal, 180° vertical, 180° diagonal	
19	Protocols	TCP/IP, DHCP, HTTP, HTTPS, NTP, RTP, RTSP, SMTP, SSL/TLS, SRTP, CDP, Bonjour, SNMP, and SSH	
20	Power Supply	Max 23W consumed with a PoE+ (802.3at-compliant) source	
21	Security	Security Password protection, IP address filtering	
22	Miscellaneous	Housing IK10 and IP66-rated	

23		Detection of camera tampering and Detection of Motion should be possible using camera	
24		Should support edge based audio analytics.	
25		ONVIF 2.X' or 'S' compliant. Certifications: UL, EN, FCC, CE	
26	Certifications Safety	UL60950-1 second edition CSA22.2-No.60950-1 IEC/EN60950-1 second edition	
27	Certifications EMC-Requirements	CISPR22 Class B ICES-003 EN50121-4 EN50155 EN50130-4 EN55022 EN55024 EN61000-3-2/-3-3 VCCI Class B KN22 Class B KN24 CISPR 24 AS/NZS CISPR 22 FCC CFR Title 47 Part 15 Subpart B	
28	OEM Criteria	All proposed Cameras should be from single OEM and OEM should have Registration in India min from 10 Years	

7.10.2 Type 2- Fixed IR Camera

S.NO.	**Camera Characteristics**	**Description**	**Compliance (Yes/ No)**
1.	Requirement Overview	High-definition Bullet outdoor IP Camera, integrated infrared illuminator	
2.	Sensor Type	1/2.7" Progressive Scan CMOS	
3.	Max Resolution	1920x1080 @ 30fps	
4.	Dynamic Range	69db	
5.	IR	Yes, Infrared illuminator with illumination capabilities up to 30 Mtrs	
6.	Lens/Iris	3.6 to 9 mm or better with Motorized Zoom Lens	
7.	Field of View	37.5°-95.98° Horizontal	
8.		21.6°-53.8° Vertical	
9.		42.6°-109.46° Diagonal	

10.	Audio I/O	The camera supports full-duplex audio and options for half-duplex operation, Camera should allows the connection of an optional Y cable or mini cable with BNC connector. Camera should allow to connect a video monitor to the mini cable with BNCconnector. Camera should have option to connect an external microphone. Camera should have Focus assist button, which will use in conjunction with an analog display to fine-tune the IP camera focus at local site. Audio in x 1	
11.	Digital I/O	(3.5-mm miniature jack)	
12.		Audio out x 1	
13.		(3.5-mm miniature jack)	
14.		DI x 1	
15.		DO x 1	
16.	Max Illumination	Color: 0.5 lux	
17.		B/W: 0 lux w/Illuminator Active	
18.	Day/Night	Automatic, manual, scheduled	
19.	Local Storage	Should support MicroSD -min 32 GB	
20.	Video Compression & Video Streaming	• Single-stream H.264 or MJPEG up to 1080p (1920 x 1080) at 30 fps • Dual-stream H.264 and MJPEG ◦ Primary stream programmable up to 1280 x 720 at 30 fps ◦ Secondary stream programmable up to 960 x 544 at 15 fps	
21.	ONVIF	Should support for ONVIF 2.0 allows for standards based interoperability	
22.	POE and External Power	12V DC, 24V Ac and PoE- 802.3af compliant (Class 3)	
23.	Power Consumption (in watts)	Max 10 Watt at DC	
24.	Supported Protocol	Dynamic Host Control Protocol (DHCP), Hypertext Transfer Protocol (HTTP), Secure HTTP (HTTPS), Network Time Protocol (NTP), Real-Time Transport Protocol (RTP), Real-Time Streaming Protocol (RTSP), Simple Mail Transfer Protocol (SMTP), Secure Sockets Layer/Transport Layer Security (SSL/TLS), TCP/IP, Secure Real-Time Transport Protocol (SRTP), Bonjour, Simple Network Management Protocol (SNMP),and Secure Shell (SSH) Protocol. Differentiated-services-code-point (DSCP) marking and class-of-service (CoS) marking	

25.	Environmental Certification	IIP67- and IK10-rated housing, Camera should have sun shield, wall mount bracket and waterproof Ethernet Cable form same OEM	
26.	Operating Temperature	40° to 122°F (-40° to 50°C)	
27.	Certifications Safety	UL60950-1 2nd edition CSA22.2-No.60950-1 IEC/EN60950-1 2nd edition IEC/EN60825	
28.	Certifications EMC-Requirements	CISPR22 Class B ICES-003 EN55022 EN55024 EN61000-3-2/-3-3 Class A VCCI Class B KN22 Class B KN24	
29.	Light sensor	Senses the level of ambient light to determine when to switch day/night mode.	
30.	Auto Detection & Configuration	The camera should be automatically discovered and configured when connected to VMS or Network Switch, to set the right network parameters for the video stream on the network .	
31.	OEM Criteria	All proposed Cameras should be from single OEM and OEM should have Registration in India min from 10 Years	

7.10.3 Type 3- Fixed Box Camera

S.NO.	Camera Characteristics	Description	Compliance (Yes/ No)
1.	Requirement Overview	High-definition IP Box Camera for outdoor	
2.	Sensor Type	1/2.7" Progressive Scan CMOS with additional digital signal processor (DSP) to support complex applications such as real-time video analytics	
3.	Max Resolution	1920x1080 @ 30fps	
4.	Dynamic Range	69db	
5.	Lens/Iris	3.1- 8mm- P-Iris	
6.	Audio I/O	The camera supports full-duplex audio and options for half-duplex operation. Should support Audio compression G.711 A, Law, G.711 U, Law, G.726, Audio in x 1	
7.	Digital I/O	(3.5-mm miniature jack)	
8.		Audio out x 1	
9.		(3.5-mm miniature jack)	
10.		DI x 1	
11.		DO x 1	
12.	Max Illumination	Color: 0.3 lux	
13.		B/W: 0.05 lux	

14.	Day/Night	Automatic, manual, scheduled	
15.	Local Storage	Should support MicroSD -min 32 GB	
16.	Video Compression & Video Streaming	- Single stream H.264 or MJPEG up to 1080p (1920 x 1080) @ 30 fps - Dual stream H.264 and MJPEG ◦ Primary stream programmable up to 1280 x 720 @ 30 fps ◦ Secondary stream programmable up to 960 x 544 @15 fps	
17.	ONVIF	Should support for ONVIF 2.0 allows for standards based interoperability	
18.	POE and External Power	12V DC, 24V Ac and PoE- 802.3af compliant (Class 3)	
19.	Power Consumption (in watts)	Max 10 Watt at DC	
20.	Supported Protocol	Dynamic Host Control Protocol (DHCP), Hypertext Transfer Protocol (HTTP), Secure HTTP (HTTPS), Network Time Protocol (NTP), Real-Time Transport Protocol (RTP), Real-Time Streaming Protocol (RTSP), Simple Mail Transfer Protocol (SMTP), Secure Sockets Layer/Transport Layer Security (SSL/TLS), TCP/IP, Secure Real-Time Transport Protocol (SRTP), Bonjour, Simple Network Management Protocol (SNMP),and Secure Shell (SSH) Protocol. Differentiated-services-code-point (DSCP) marking and class-of-service (CoS) marking	
21.	Operating Temperature	14° to 122°F (-10° to 50°C)	
22.	Certifications Safety	UL60950-1 2nd edition CSA22.2-No.60950-1 IEC/EN60950-1 2nd edition IEC/EN60825	
23.	Certifications EMC-Requirements	CISPR22 Class B ICES-003 EN55022 EN55024 EN61000-3-2/-3-3 Class A VCCI Class B KN22 Class B KN24	
24.	Auto Detection & Configuration	The camera should be automatically discovered and configured when connected to VMS or Network Switch, to set the right network parameters for the video stream on the network .	
25.	OEM Criteria	All proposed Cameras should be from single OEM and OEM should have Registration in India min from 10 Years	

7.10.4 Type 4- Camera- High Definition

S.NO.	Camera Characteristics	Description	Compliance (Yes/ No)
1.	Requirement Overview	High-definition Outdoor IP Camera	
2.	Sensor Type	1/2.5" Progressive Scan CMOS with additional digital signal processor (DSP) to support complex applications such as real-time video analytics	
3.	Max Resolution	2560 x 1920	
4.	Dynamic Range	80db	
5.	IR	Yes, Infrared illuminator with illumination capabilities up to 20 Mtrs	
6.	Lens/Iris	3 to 9 mm P-Iris/DC-Iris or better with Motorized Zoom Lens and Vandal-Resistant Dome	
7.	Field of View	35.45° to 88.90° (horizontal)	
8.		26.69° to 67.01° (vertical)	
9.		43.99° to 111.00° (diagonal)	
10.	Audio I/O	The camera supports full-duplex audio and options for half-duplex operation. Suould support Audio compression G.711 A, Law, G.711 U, Law	
11.	Digital I/O	(3.5-mm miniature jack)	
12.		Audio out x 1	
13.		(3.5-mm miniature jack)	
14.		DI x 1	
15.		DO x 1	
16.	Max Illumination	Color: 0.1 lux	
17.		B/W: 0 lux w/Illuminators Active	
18.	Day/Night	Automatic, manual, scheduled	
19.	Local Storage	Should support MicroSD -min 32 GB	
20.	Video Compression & Video Streaming	• Single-stream H.264 up to 2560 x 1920 @ 5 frames per second (fps) • Single-stream MJPEG up to 1920 x 1080 @ 30 fps • Dual-stream H.264 and MJPEG: ◦ Primary stream programmable up to 1280 x 720 @ 30 fps ◦ Secondary stream programmable up to 960 x 540 @ 15 fps	
21.	ONVIF	Should support for ONVIF 2.0 allows for standards based interoperability	

22.	POE and External Power	24V Ac and PoE- 802.3af compliant (Class 3)	
23.	Power Consumption (in watts)	Max 15 Watt at PoE or 30watt at AC	
24.	Supported Protocol	Dynamic Host Control Protocol (DHCP), Hypertext Transfer Protocol (HTTP), Secure HTTP (HTTPS), Network Time Protocol (NTP), Real-Time Transport Protocol (RTP), Real-Time Streaming Protocol (RTSP), Simple Mail Transfer Protocol (SMTP), Secure Sockets Layer/Transport Layer Security (SSL/TLS), TCP/IP, Secure Real-Time Transport Protocol (SRTP), Bonjour, Simple Network Management Protocol (SNMP),and Secure Shell (SSH) Protocol. Differentiated-services-code-point (DSCP) marking and class-of-service (CoS) marking	
25.	Environmental Certification	IIP67- and IK10-rated housing, Camera should have sun shield, wall mount bracket and waterproof Ethernet Cable form same OEM	
26.	Operating Temperature	-25 to 50°C (-13 to 122°F) using PoE -40 to 50°C (-40 to 122°F) using AC	
27.	Certifications Safety	UL60950-1 2nd edition CSA22.2-No.60950-1 IEC/EN60950-1 2nd edition IEC/EN60825	
28.	Certifications EMC-Requirements	CISPR22 Class B ICES-003 EN55022 EN55024 EN61000-3-2/-3-3 Class A VCCI Class B KN22 Class B KN24	
29.	Light sensor	Senses the level of ambient light to determine when to switch day/night mode.	
30.	Auto Detection & Configuration	The camera should be automatically discovered and configured when connected to VMS or Network Switch, to set the right network parameters for the video stream on the network .	
31.	OEM Criteria	All proposed Cameras should be from single OEM and OEM should have Registration in India min from 10 Years	

7.10.5 Video & Audio Analytics

The System should support Video Analytics at camera edge or at server level, These video analytics should enable an IP camera to perform various analytic functions. Analytic functions trigger events when a camera detects activities or behaviors that match predefined rules. Counting functions count people.

Leave behind event - Camera should have provision to enable the following video analytics, system software to be provided as per RFP requirement: This Analytics will required for Type 3/4 Cameras; The Video Analytics should include the following:

Feature	**Analytics**
Object classification	Yes

Tripwire event	Yes
Exits Event	Yes
Appears event (full view)	Yes
Appears event (area of interest)	Yes
Disappears event (full view)	Yes
Disappears event (area of interest)	Yes
Loitering event	Yes
Leave behind event (full view)	Yes
Leave behind event (area of interest)	Yes
Configurable leave behind time	Yes
Object size filters	Yes
Object size change filters	Yes

Crowd Monitoring—Camera should provide below features for estimating the size and the relative density of a crowd of people. This Analytics will required for Type 4 Cameras;

Feature	**Analytics**
Object Size Filters	Yes
Object Density Level	Yes
Flow Violation	Yes

Audio Analytics

The System should support Audio Analytics at camera edge or at server level, should have provision to enable the following audio analytics with any camera, system Gunshot software shall be provided as per RFP requirements:

Gunshot—Detects a variety of firearms being discharged. The following general guidelines should apply to the Audio Analytics:

The Gunshot Audio Analytics should detect a variety of firearms being discharged.

Gunshots should be characterized by unique muzzle blasts that are associated with a range of unsilenced weapons that are typically used in civilian gun crimes. Types of weapons that this app can detect being discharged are handguns (including 9 mm automatics and revolvers with or without muzzle diffusers), shotguns (including 20 gauge, .410 and 12 bore), bolt-action rifles (.22 mm and 7.62 mm), and automatic rifles (including AK-47, AR-15 and Uzi submachine gun).

IP camera should detect a gunshot from a sound source that is up to 50 meters away from the microphone.

7.10.6 Industrial Grade Switch – Type 2

1	Switch Architecture and Performance	The switch should provide 8 port 10/100 Mbps FE ports downlink out of which minimum four should be POE+ and switch should additionally have 4 GE SFP uplinks. Should be proposed with ruggedized transceivers as per SI solution.	**Compliance (Yes/ No)**
2		Switch should have wire rate switching fabric of minimum 9.6 Gbps or more.	
3	Layer 2 Features	802. 1Q VLAN on all ports with support for minimum 255 active VLANs and minimum 1K Mac addresses or higher	
4		Spanning Tree Protocol as per IEEE 802.1d, 802.1s and 802.1w	
5		Should support Improved resiliency with the support of Resilient Ethernet Protocol (REP) or equivalent for ring topology	
6		Link Aggregation Control Protocol (LACP) as per IEEE 802.3ad.	
7		Switch should support IGMP v1/v2/v3 as well as IGMP snooping and minimum 255 IGMP Multicast Groups	
8	Quality of Service (QoS) Features	Switch should support classification and scheduling as per IEEE 802.1P on all ports and four egress queues per port. Switch should also support mechanism of applying Automatic QoS or equivalent mechanism	
9		Switch should support strict priority queuing or equivalent to guarantee that the highest-priority packets are serviced ahead of all other traffic.	
10	Security Features	Switch should support ACLs, TACACS+, RADIUS, IP Route Filtering, ARP spoofing, DHCP snooping, DHCP Option 82, Dynamic ARP Inspection (DAI), IP source guard and BDU Guard or equivalent	
11	Management, Easy-to-Use Deployment and Control Features	Switch should have a console port, support for SNMP Version 1, 2 and 3, TELNET, SSHv2, 4 groups of embedded RMON, UDLD, Layer 2 Traceroute or equivalent, DHCP server	
12		The switch should support following IPv6 Features: 128-Bit Wide Unicast Addresses, DNS for IPv6, ICMPv6, Neighbor Discovery, IPv6 Stateless Auto-configuration and Duplicate Address Detection, SNMP and Syslog Over IPv6, HTTP over IPv6 and IPv6 MLD snooping	
13	Standards	RoHS Compliant, IEEE 1588v2 hardware ready - Precision Time Protocol, IEEE 802.3af, 802.3at, NTP, PTP	
14	Industry Standards:	• KEMA,NEMA TS-2, ODVA Industrial EtherNet/IP, PROFINETv2, ABB IT Certificate, IP30	
15	Safety & Hazard	• UL 508, CSA C22.2 No.142, UL/CSA 60950-1, EN60950-1, CB to IEC 60950-1, ANSI/ISA 12.12.01 (Class 1, Div 2 A-D), EN 60079-0, -15 ATEX certification (Class I, Zone 2 A-D) with cabinet enclosure	
16		DIN rail mount	

17	EMC Compliance	• FCC, IEC/EN 61000-(4-2 to 4-6, 4-8, 4-9, 4-11, 4-29), RoHS	
18	Operating Temperature	• -40C to +70C with Enclosure	
19	Shock and Vibration	• IEC 60068-2-27 (Operational Shock, Non-Operational Shock)	
20		• IEC 60068-2-6, IEC 60068-2-64, EN61373 (Operational Vibration, Non-operational Vibration)	
21	Relative Humidity	• Relative Humidity of 5% or 95% Non-condensing, IEC 60068 -2-3, IEC 60068-2-30, IEC 60068-52-2	

7.10.7 Industrial Grade Switch – Type 3

1	Switch Architecture and Performance	The switch should provide 4 port 10/100 Mbps FE ports downlink and switch should additionally have 2 GE SFP uplinks. Should be proposed with ruggedized transceivers as per Concessionaire solution.	**Compliance (Yes/ No)**
2		Switch should have wire rate switching fabric of minimum 4.8 Gbps or more.	
3	Layer 2 Features	802. 1Q VLAN on all ports with support for minimum 255active VLANs and minimum 1K Mac addresses or higher	
4		Spanning Tree Protocol as per IEEE 802.1d, 802.1s and 802.1w	
5		Should support Improved resiliency with the support of Resilient Ethernet Protocol (REP) or equivalent for ring topology	
6		Link Aggregation Control Protocol (LACP) as per IEEE 802.3ad.	
7		Switch should support IGMP v1/v2/v3 as well as IGMP snooping and minimum 255 IGMP Multicast Groups	
8	Quality of Service (QoS) Features	Switch should support classification and scheduling as per IEEE 802.1P on all ports and four egress queues per port. Switch should support mechanism of applying Automatic QoS or equivalent mechanism	
9		Switch should suport strict priority queuing or equivalent to guarantee that the highest-priority packets are serviced ahead of all other traffic.	
10	Security Features	Switch shoud support ACLs, TACACS+, RADIUS, IP Route Filtering, ARP spoofing, DHCP snooping, DHCP Option 82, Dynamic ARP Inspection (DAI), IP source guard and BDU Guard or equivalent	
11	Management, Easy-to-Use Deployment and Control Features	Switch should have a console port, support for SNMP Version 1, 2 and 3, TELNET, SSHv2, 4 groups of embedded RMON, UDLD, Layer 2 Traceroute or equivalent, DHCP server	
12		The switch should support following IPv6 Features: 128-Bit Wide Unicast Addresses, DNS for IPv6, ICMPv6, Neighbour Discovery, IPv6 Stateless Auto-configuration and Duplicate Address Detection, SNMP and Syslog Over IPv6, HTTP over IPv6 and IPv6 MLD snooping	
13	Standards	RoHS Compliant, IEEE 1588v2 hardware ready - Precision Time Protocol, IEEE 802.3af, NTP, PTP	

14	Industry Standards:	• KEMA,NEMA TS-2, ODVA Industrial EtherNet/IP, PROFINETv2, ABB IT Certificate, IP30	
15	Safety & Hazard	• UL 508, CSA C22.2 No.142, UL/CSA 60950-1, EN60950-1, CB to IEC 60950-1, ANSI/ISA 12.12.01 (Class 1, Div 2 A-D), EN 60079-0, -15 ATEX certification (Class I, Zone 2 A-D) with cabinet enclosure	
16		DIN rail mount	
17	EMC Compliance	• FCC, IEC/EN 61000-(4-2 to 4-6, 4-8, 4-9, 4-11, 4-29), RoHS	
18	Operating Temperature	• -40C to +70C with Enclosure	
19	Shock and Vibration	• IEC 60068-2-27 (Operational Shock, Non-Operational Shock)	
20		• IEC 60068-2-6, IEC 60068-2-64, EN61373 (Operational Vibration, Non-operational Vibration)	
21	Relative Humidity	• Relative Humidity of 5% or 95% Non-condensing, IEC 60068 -2-3, IEC 60068-2-30, IEC 60068-52-2	

7.10.8 Enterprise Grade Layer 2 PoE Switch

S-No		Required Minimum Specification	Compliance (Yes/ No)
1	Switch Architecture & Performance	Switch should have 8 X 10/100/1000Base-T plus 2 x SFP uplink ports. Transceivers to be supplied as per minimum BOQ given in RFP.	
2		The switch should have 124W of Available PoE Power and should support both POE and POE+ standard. The switch should support all the options either configuring 8 ports up to 15.4W or 4 ports up to 30W or combination of two	
3		Switch should have non-blocking wire-speed architecture.	
4		Switch should support IPv4 and IPv6 from day One	
5		Switch should have non-blocking switching fabric of minimum 20 Gbps or more and should have Forwarding rate of minimum 14 Mpps..	
6	Layer 2 Features	IEEE 802.1Q VLAN tagging with support for minimum 250 active VLANs and 4k VLAN ids	
7		Should support Spanning Tree Protocol as per IEEE 802.1d, Multiple Spanning-Tree Protocol as per IEEE 802.1s, Rapid Spanning-Tree Protocol as per IEEE 802.1w	
8		Switch should support IGMP v1/v2/v3 as well as IGMP v1/v2/v3 snooping.	
9	Network Security Features	Switch should support MAC address based filters / access control lists (ACLs) on all switch ports.	
10		Switch should support Port as well as VLAN based Filters / ACLs.	
11		Switch should support RADIUS and TACACS+ for access restriction and authentication.	
12		Secure Shell (SSH) Protocol, HTTP and DoS protection	

13		Should support DHCP snooping, DHCP Option 82, Dynamic ARP Inspection (DAI)	
14		The Switch should support IPv6 RA Guard, DHCPv6 guard, IPv6 Snooping to prevent any Man-in-middle attack.	
15	Quality of Service (QoS) & Control	Switch should support classification and scheduling as per IEEE 802.1 P on all ports.	
16		Switch should support DiffServ as per RFC 2474/RFC 2475.	
17		Switch should support QoS configuration on per switch port basis support four queues per port.	
18	Management, Easy-to-Use Deployment and Control Features	Switch should have a console port with RS-232 Interface for configuration and diagnostic purposes.	
19		Switch should be SNMP manageable with support for SNMP Version 1, 2 and 3.	
20		Switch should support TELNET and SSH Version-2 for Command Line Management.	
21		Switch should support 4 groups of embedded RMON (history, statistics, alarm and events).	
22		Support for Unidirectional Link Detection Protocol (UDLD) or equivalent feature to detect unidirectional links caused by incorrect fiber-optic wiring or port faults and disable on fiber-optic interfaces	
23		Layer 2 trace route eases troubleshooting by identifying the physical path that a packet takes from source to destination.	
24		Should support DHCP Server feature to enable a convenient deployment option for the assignment of IP addresses in networks that do not have without a dedicated DHCP server.	
25	Standards & Compliance (Switch Should support all the mentioned Standards)	Should be RoHS Compliant.	
26		Should support IEEE 802.1x support.	
27		Should support IEEE 802.3x full duplex on 10BASE-T and 100BASE-TX ports.	
28		Should support IEEE 802.3u 10 BaseT /100 Base Tx /1000 Base Tx.	

7.11 Solid waste Management Solution requirement

7.11.1 SWM Application

S-No	Required Minimum Specification	Compliance (Yes/ No)
1	GPS tracking of the waste pick up vehicle for real time tracking	
2	Route Optimization which shall help in reduction of trip time, fuel saving and serving more locations	
3	Manage routes and vehicles dynamically through an automated system	
4	Efficient monitoring and management of waste collection bins	
5	Ensure complete coverage of door to door and community collections served	

	by vehicles	
6	Monitor and track other municipal corporation vehicles under Solid Waste Management Dept.	
7	Record history of vehicle routes, attended sites and other details	
8	RFID devices with vehicle and RFID tagging of Bin to ensure serving by requisite vehicle	
9	Weight & Volume Sensor based bin to indicate maximum utilization status and trigger vehicle pick up	
10	Alert / Alarm management - Real time management of missed garbage collection points	
11	Monitoring & Reporting Application - reports of vehicles, garbage collection status, bin status etc.	

7.11.2 AVLS Application

S-No	**Required Minimum Specification**	**Compliance (Yes/ No)**
1	Web Based Vehicle Tracking and Monitoring Application customized to meet the functional requirements of the solution is envisaged.	
2	Automated Vehicle Locator Management System with requirement of customized dashboard specific for monitoring and tracking of solid waste management activities and integration with the RFID system & weight and volume sensor system for bin collection management.	
3	The application shall be hosted in the City Operation Center. The application shall leverage on the advanced GPS and GIS technologies for route scheduling, route monitoring, reporting and providing a quick dashboard.	
4	The software application shall be developed on a GIS map based platform on which geo-location of all the bins and collection vehicles shall be displayed in real time. This application shall be built on the AVL application being developed as part of the overall AVL system.	
5	The application should have the following features:	
5.1	· Geo-fencing reporting portal	
5.2	· Spatial database and integration with the data captured for geographic queries and normal data queries	
6	Monitor the performance of entire waste collection system and to improve the maintenance activities to reduce downtime and thus improving the efficiency of the system.	
7	Generate analytical reports in order to improve the efficiency of the system in near future. Through this feature, effective planning and management of solid waste management services shall be done by tracking the total waste generated, type of waste generated and	

	identification of higher waste generation areas.	
8	Publishing of various MIS reports consolidating the work done by AITL including but not limited to:	
8.1	· Daily, weekly, monthly reports (database) on item-wise, dept. wise and activity wise details.	
8.2	· Consolidated Report generation on solid waste management site activity.	
8.3	· Other reports as generated through integration with AEE and ACC systems.	
9	Generate schedules using Computer Aided Dispatch (CAD) system predictive algorithms.	
10	The software platform shall be able to visualize the capacity of each trash bin and shall indicate it with different colour codes. For example, green colour to signify that the waste container has plenty of space, and red colour to give an indication to the operator that the threshold level of a particular bin has been reached and collection is required.	
11	The platform shall also be able to assist in defining the optimal collection routes for the trucks which will help in reducing the collection time of the waste by the trucks thus reducing the unnecessary traffic of trucks in the city	
12	The platform shall have built in security for data capturing and transfer including devices used i.e. restricting to the authenticated devices only.	
13	Encryption techniques if used for data security shall be of minimum 128-bit encryption.	

7.11.3 Bin Management System

S-No	**Required Minimum Specification**	**Compliance (Yes/ No)**
1	The waste collection vehicles shall be fitted with RFID readers. The RFID readers identify the RFID tags installed in the each of the collection Bins and read the Bin details.	
2	This data shall be transferred through the GPS device unit GSM/GPRS connectivity to the integrated application. The RFID readers shall be integrated to the vehicle GPS device unit to achieve this functionality.	

7.11.4 RFID Reader

S-No	**Required Minimum Specification**	**Compliance (Yes/ No)**
1	RFID Reader shall have operating frequency range of 865 MHZ to 867 MHZ.	
2	The RFID reading range of the transceiver antenna mounted on the vehicle at an average height of 3m above the road surface shall be upto 5m.	

3	RFID Reader antenna type shall be Circularly Polarized.	
4	RFID Reader shall comply with the protocols: EPC Gen 2, ISO 18000-6C and shall comply with the general conformance requirements of the standard.	
5	RFID Reader enclosure shall be light weight.	
6	RFID Reader technology deployed should have the capability to optimize read rates for the bin identification application and adapt to instantaneous noise and interference level.	
7	RFID Reader shall have capability of diagnostic and reporting tools.	
8	The firmware should be upgradable to support future protocols.	
9	Reading of Tag & EPC memory for at least 2 tags per second for a moving vehicle with a speed limit of up to 40 kilometres/ hour.	
10	It shall support RF Power of minimum 0~30dBm and shall be software programmable.	
11	RFID readers shall communicate over TCP/IP and GPRS or higher.	
12	It shall support communication interface RS232 at minimum.	
13	Readers shall be IP 65 rated.	
14	RFID readers shall be capable of withstanding standard material handling vehicle environments. It shall meet or exceed MIL STD 810F.	
15	Readers shall be powered by Vehicle DC Power 12 to 60V, 4.5A maximum.	

7.11.5 RFID Tag

S-No	**Required Minimum Specification**	**Compliance (Yes/ No)**
1	The tag shall be anti-metal, and can be mounted on the metallic surface.	
2	The tag shall be high temperature resistant and shall be capable of withstanding harsh or challenging conditions.	
3	The tag shall have long read and write distance.	
4	The tag shall be durable, reusable.	
5	The frequency range of the tag shall be between 865~867MHz.	
6	The tag shall support operation mode of Fixed Frequency or FHSS Software Programmable.	
7	The tag protocol shall be ISO 18000-6C & EPC CLASS1 GEN2.	

8	The tag memory configuration shall be EPC: 96bit (H3) and User: 512bit (H3).	
9	The tag material compatibility shall be metallic and non-metallic substrates.	
10	The read range (m) on metal surface shall be max. 7.5m for Fixed Reader and max. 3m for handheld reader.	
11	The Mounting of tag shall be of screw, rivet, superglue, ribbon, double faced adhesive tape type.	
12	Tags shall be IP 68 rated.	

8 *Works related to Civil, Electrical, Furniture & Air conditioning for Command & Control Centre.*

The scope of the project includes designing, engineering, supply & installation of 24X7 mission critical Command & Control Center Interiors. As the Command and Control room is a significant place, it is imperative that it is designed properly in terms of Aesthetics, Ergonomics and Functionality. Various aspects should be considered while designing Command and Control room area to create ideal work place, considering physiological aspects such as line of sight and field of vision and cognitive factors such as concentration and perceptivity as per ISO 11064.

8.1 The design of systems, equipment and facilities shall reflect human factors requirements including the following:

I. Satisfactory environmental conditions for operator personnel. Including noise, air flow, temperature and humidity, and precautionary measure under uncontrolled conditions (like fire) beyond acceptable limits.

II. Adequate space for personnel and equipment for the movements and activities they are required to perform during operation and maintenance, under both normal and emergency conditions.

III. Adequate visual / auditory status information and other communication links between personnel and equipment under normal and emergency conditions.

IV. Adequate illumination for the performance of operation, control, maintenance and training.

V. The control room shall be built as per the criteria of “Human Factor Engineering” to improvise the efficiency utilization of the operators and provide them Fatigue free working environment.

VI. Objective: -

i. Ensure maximum standard of safety.

ii. Allow Flexibility

iii. Minimize maintenance

iv. Improve operator’s efficiency & alertness.

VII. Designing, manufacturing, testing, integration etc., all complete, preparation of the related drawings, documents, etc. of the Command and Control room shall be in the SI scope. The design shall confirm the requirements & specifications of this RFP document.

VIII. In broad, the scope of work and supply shall consist of the following parts: -

i. Interior Design, engineering of Command and Control room.

ii. All related services for supply, installation, testing.

iii. Spares & Documentation

IX. Detailed scope of work and supply shall include but not be limited to the following: -

i. Data Collection: Gather all information related to design of the Command and control rooms.

ii. Design Proposal: - Submission of various options of Command and Control room layout for client's approval, strictly complying to ISO 11064.

X. General: -

i. The tentative room area shall be provided to the Command and Control room designer to develop the various options.

ii. Supply of the product catalogue, technical proposals including but not limited to drawings, documentation, 3D views, colour pallets, for the complete solution.

iii. Spares: -A list of manufacturer's recommended spares for operation and maintenance shall be provided.

iv. Quality assurance & commissioning of the complete system at site to the complete satisfaction of the Owner/Consultant.

a. Building design must be in accordance with international standards.

b. SI 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. SI should define the standard of on building construction.

f. It is expected that design of ICCC building is demonstrated through 3D video.

g. SI 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 Centre.

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 NDMC systems within ICCC premises.

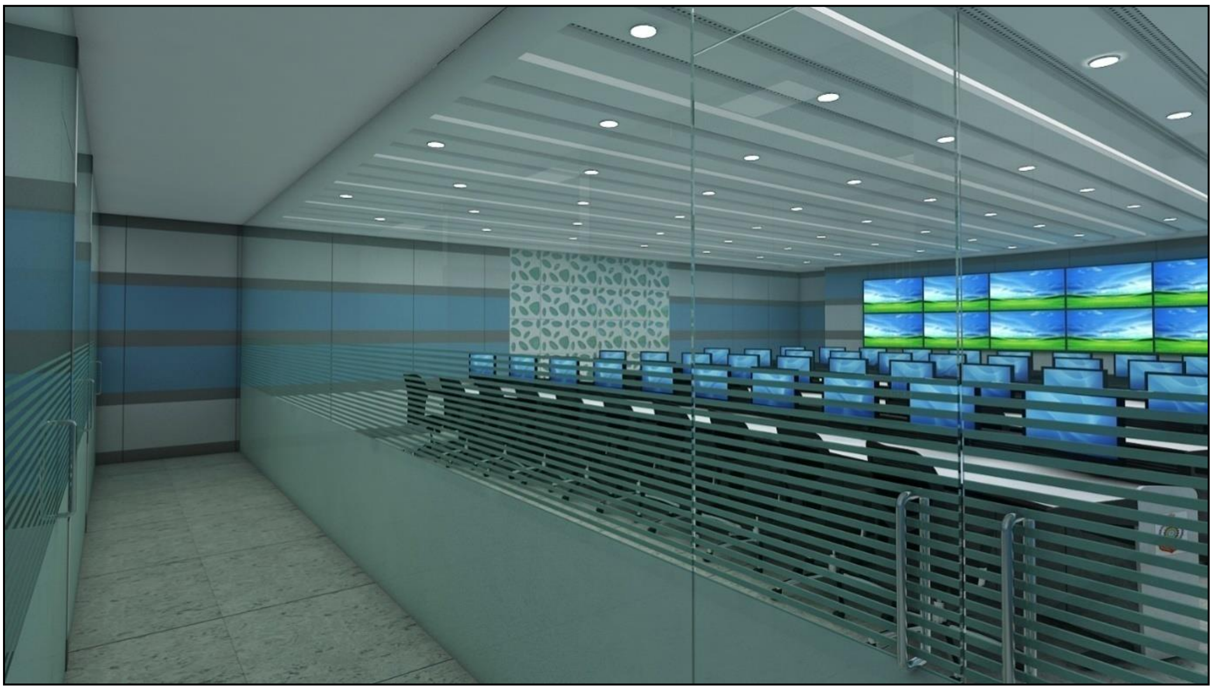
j. SI will be required to get approval on engineering drawings of ICCC from NDMC.

k. During the review of design documents, NDMC may suggest some changes or provide feedback on design parameters. SI will be required to incorporate such inputs.

l. NDMC may authorize any third party do to review of design documents.

m. After final approval of NDMC on design documents, SI will start the work.

General View of Command and Control Room from Entrance



8.2 Acoustic Requirements of Control room

XI. Command and Control room being dead zone in acoustical terms, threshold should be lower than the normal.

XII. Use of Acoustics and psychoacoustics measurements are must. SI to highlight the same in drawings.

XIII. Materials which define acoustics; it’s the detailing which ensures controlled reverberations & resonances and reflections.

XIV. Selection of fire retardant/rated material is must.

8.3 Mandatory Requirement:

The project demands for a contemporary, aesthetically appealing, ergonomically designed, safe and 24X7 working facility. Conventional wooden cladding, painting, gypsum, 2’X2’ Metal, POP ceilings (for Command Control Room area) shall not be accepted.

This facility being the first of its kind, scale & prestige it is mandatory for the SI to provide Designer Command and Control interiors without compromising on the safety and functionality of the facility. Also, this being a Green Building; materials having the adverse impact on the environment and nature shall not be accepted.

Submittals (Bidder to produce these documents from control room interior Manufacturer or supplier along with the bid): -

To arrange factory and product inspection before placement of order, to ensure that the material to be supplied and installed is of good quality and asthetics.

To prove supplier's seriousness in the business; Printed Catalogues and Locations of Demo rooms to be furnished.

Design Criteria: -

The ceiling, panelling and partition must be of modular design, facilitating future equipment retrofits and full reconfigurations without requiring any major modification to the structure.

Product Specific Mandatory Requirement

Copy of Test certification for ASTM E84 (from UL) for the surface burning characteristics of wall panelling tiles and ceiling tiles to be submitted along with the bid. This is mandatory requirement from Fire safety point of view.

Raw-material supplier data alone is not acceptable.

8.4 PANELING

Straight Metal Panelling

Panel should comprise of perforation for making the cladding and partitions acoustically sound. Min 20% panels shall be perforated or as specified by the consultant.

There should be possibility of wide variety of colors and images to be used on the wall elements to give the aesthetic and state of the art look to the control room.

Panel design to support proper LVS integration.

Gluing, screwing, ACP, Laminates are not allowed.

Panel design should ensure that when the tiles need to be removed for service maintenance of Lighting & AC ducts & itself cleaning, the risk of tile damage is minimized.

Structure should allow uninterrupted flow of wires/cable/tubes of max. dia 25mm.

Design & Material Specification for Panelling

Factory made removable type self inter lockable metal panels of Preformed textured Hot dip galvanized strips and sheets of low carbon steel coated on one side with rigid polyvinylchloride (PVC) film and on the other side a coating based on cross linkable polyester resins (sheet thickness 0.6mm & PVC Coating 0.15mm). Make shall comprise of specially designed combination of perforated and non-perforated panels through CNC laser Cutting, bending & punching. Panel shall be of 0.75mm thick galvanized metal of approved color. Panels shall be designed to achieve shape and design as per the design consultant. Panels shall be fixed using hook fitting on structure. Overall system thickness for paneling shall be 70mm to 85mm and for partition shall be 85mm to 110mm.

As per design panel shall comprise of hexagonal perforation for making paneling and partitions acoustically sound. Acoustic grade fire retardant fabric (min 1.5mm thick) will be fixed at some parts of the control room.

Panel shall be design in such a manner that it takes care of undulation of civil walls and gives perfect flat surface finish and compile easy service & maintenance procedure.

Design:

The cladding panels shall be made up of combination of two sheets locked and riveted together and polystyrene shall be used as infill to achieve strength and acoustics. The front tile (PVC pre-coated metal sheet) shall be perorated/ non-perforated as per the design requirement and the back tile (Powder coated 0.6mm GI sheet) shall be designed in such a manner that it fits on the back portion of the front tile. Once the tiles are fitted together then these will be manually riveted. These tiles shall be bend through CNC, machine punched & laser Cut to achieve perfect accuracy.

Structure Shall be made from heavy duty powder coated modular steel frame (minimum sheet thickness 1 to 1.6mm) and shall allow uninterrupted flow of wires/cable/tubes of max. dia. 25mm.

Structure Shall be securely grouted from wall, roof and floor. It shall be made up of 1-1.6mm thick vertical Slotted rolled C sections (Upright) and horizontal rolled 'C' connectors. Grid of desired dimension shall be formed by Vertical and horizontal sections having 50mm pitch.

Surface Finish:

For Panels:

a) **Front Panel:** PVC pre-coated GI sheet (sheet thickness: 0.6mm and PVC coating: 0.15mm)

b) **Back Cover:** Powder coated GI sheet. (sheet thickness: 0.6mm with powder coating:)

For Structure:

Powder coated sheet. (sheet thickness: 1.0mm to 1.6mm with powder coating)

The metal sheet shall have possibility of being formed mechanically per the specific needs of the project.

Panel shall provide better thermal, electrical insulation as compared to normal GI panels. It shall be non-reflective/glare free and be eligible for food contact.

Material Selection:

Available Width- 300mm to 1200mm (in multiples of 150mm).

Available Height- 150mm to 750mm (in multiples of 150mm).

Thickness- 10mm to 15mm for perforated tiles with acoustic fleece without back cover

25mm to 30mm for non-perforated tiles with back covers

Component Specification:

Floor Mounting: -

3mm thick C channels are welded together to form a 'I' section having minimum height of 150mm. This I section shall be welded on 3mm thick MS grouting plate.

This assembly shall be grouted on the floor with the help of M10 Anchor Fasteners.

These Floor Mountings shall be the base support to the vertical uprights spaced at a center to center distance of 1200mm maximum.

Contractor must ensure proper marking and leveling before proceeding with any floor grouting.

C Section (Upright) fixing: -

56 mm wide Slotted rolled C section (UPRIGHT) (1 to 1.6 mm thick CRCA). Maximum single piece Length shall not exceed 2700mm.

All sections will be dual slotted with 50 mm pitch.

These Uprights shall be mounted over the floor mountings and shall be connected by C connectors made up of 1.0mm to 1.6mm thick cold rolled ‘C' sections.

The installation to be carried out with Uprights spaced at 1200 mm (centers to center) securely fixed to the floor slab by means floor mountings.

The uprights shall be firmly held with L shaped wall mounts made up of 2 mm thick MS sheet duly powder coated. One portion of L mount shall be grouted with wall and other will be having a minimum slot length of 75mm.

The L clamp and the upright will be bolted together with M6 bolts.

End Cap

0.6mm to 0.75mm thick C shaped tile; like the panel tile will be bolted on the extreme end Uprights to hide the grid structure.

Panel:

The panels shall be hooked on the uprights.

Panels shall have integrated hooks (which shall cut and bend on high precision laser machines).

The panels shall have minimum gap of 5mm between two tiles (on vertical and horizontal edges) so that the tiles can be replaced and installed easily.

The hooks of the Panels shall have a length of 20mm (for the upper hook) and 10 mm (for the bottom hook). So that these panels are firmly held on the uprights.

The panel shall have HOOK in arrangement (With gravity lock).

Corner Cap:

On extremes ends of control room the wall connector (L- profile) shall be fixed on the perimeter walls. This L-section shall be snap fitted and then bolted to the walls.

Door Profile:

Door frame shall be fixed with these profiles only to have proper integration of doors with the overall system.

Feature:

Raw material for tile & powder coating should not affect environment, vendor to provide necessary test certificate.

Color should not fade over 10 years.

No sagging

Easy and quick installation

Low cleaning effort

Vendor to demonstrate one portion at wall paneling& ceiling at their premises before dismantling & shipping to site. In short, a FAT (Factory acceptance test) to be carried out at vendors works for ceiling &paneling.

100 % modular design. At site, no cutting, chipping work is allowed.

The tile shall be bend resistant

8.5 PARTITION

Straight Metal Partition–

All the properties and MOC shall be like straight Metal paneling but the partition shall have metal cladding on either side of the frame.

Curvilinear Metal Partition:-

All the properties and MOC shall be like Metal paneling/partition but the front tiles shall be having perfect curve to meet the aesthetical requirement of the Command and Control room and shall allow easy installation of the LVS/Screens on it.

GLASS PARTITION

Full glass wall partitions will be made of 12mm Toughened laminated glass with frame-less structure. The glass partition shall be supported by 600mm high Modular metal partition (having the same finish as that of wall cladding) from the floor. Proper structure shall be made to ensure the fixing of glass from RCC slab above false ceiling and flooring.

No straight and vertical structural members shall be visible. Safety film shall be applied on the glass to avoid shattering. Glass shall be fitted on anodized extrusion with tool less technology and having a provision for replacing glass with perforated sheet/acoustic tile by removing the glass.

NOTE: - The nature of installation should be replaceable, expandable and flexible to cater the future expansion/technical up-gradation.

8.6 Lattice Paneling

All the properties shall remain like Metal paneling. The tile size shall be 2’X2’ or 1M X 1M. The front tile shall have laser cut designs (as per approval) and another tile shall be fitted into it to have Highlighter view.

The tiles will be having cut-outs in such a way that when the tiles are rotated by 90 degrees the design pattern of the entire wall shall be changed. Using the same tiles and different orientations we will have multiple design possibilities.

The aim is to provide a contemporary look to the CCR.

It shall be a tool less & screw less fixing.

8.7 DOORS& WINDOWS

Metallic Door

With door spring and locking arrangements and both way handle. Prepare with rigid thermo fused film metal panels. Specification: 0.6mm thick Metal panel sheets, cavity filled with glass wool insulation of density 24kg/cum in roll form of make inside adequate quantity. Material of the partition and that of metal door will remain the same.

Metal door with Toughened Glass Vision Panel: -

The door shall have 100mm frame (made of same material as that of wall paneling/partition) and shall have 12mm thick glass pane in between.

12mm thick tempered clear glass door with door spring and locking arrangements and both way handle and patch fittings.

Glass Properties:

Safety (tempered): when broken, must split into tiny harmless pieces.

8.8 False Ceiling:

Designer Acoustic Metal False ceiling with Straight/Curvilinear linear Plank Ceiling

Factory made acoustic modular metal false ceiling of powder coated panels. Make shall comprising of perforated and non-perforated metal panels made through CNC laser Cutting, bending & punching. Panel shall be of 0.6mm galvanized metal of approved color. Panels shall be designed to achieve shape and design as per the design consultant with the combination of acrylic panels with lights, designed to enhance visual feel, with provision for easy installation and maintenance, integrated lighting and scope for integration of building services like HVAC and fire detection/ fighting system.

As per design panel shall comprise of micro perforation for making false ceiling acoustically sound with fire rated acoustic fleece.

Design:

The ceiling panels shall be made up of combination of perforated and non-perforated panels to achieve strength and acoustics. These tiles shall be bend through CNC, machine punched & laser Cut to achieve perfect accuracy.

Structure Shall be made from heavy duty powder coated modular steel frame (minimum sheet thickness 1 to 1.6mm). It Shall be securely grouted from roof with help of anchor fastener and GI self-threaded rods. It shall be formed with the help of slotted rolled W sections (stiffener) and M section (Master) with help of M6 cage nut and bolts.

Surface Finish:

For Panels: Powder coated GI sheet. (sheet thickness: 0.6mm with powder coating:)

For Structure: Powder coated sheet. (sheet thickness: 1.0mm to 1.6mm with powder coating)

The metal sheet shall have possibility of being formed mechanically per the specific needs of the project. It shall be able to undergo stretching up to 100% and therefor follow (adhere to) bend with the steel in all its deformation.

Fire rated acoustical fleece to be pasted on the perforated metal ceiling planks to achieve better acoustic levels. Metal modular false ceiling is having Sound absorption coefficient (NRC) value 0.30 per IS:8225-1987, ISO: 354-1985 and ASTM 423-90.

The master section shall have laser cut profile to enable fixing of perforated, Non-Perforated & diffused continuous LED section with acrylic sheet.

Material Selction-

Non- Perforated Tile: - Machine profiled GI sheet of 290mm (Wide)available in various length of 600mm to 1800mm in multiple of 300mm

Perforated Tile: - Machine profiled GI sheet with fleece of 146mm (Wide) in various length of 600mm to 1800mm in multiple of 300mm

Material Testing/Certification:

Core material (compressed polystyrene): Acoustic test: 9301/ ISO: 140/ASTM 413, ASTM C 578-08b type VI

Powder coating

Adhesion test: EN ISO 2409 (2 mm)

Impact resistance test: ASTM D 2794 (5/9' ball)

flexibility test: EN ISO 1519

Salt spry test: 600 hrs.

resistance to humid atmosphere test: DIN 50017.

Component Specification:

Master M Section:

1.2 mm thick GI section length 1200mm. the installation to be carried out with runner's spaces at 1200/1500/2100 mm center to center securely fixed to the hanging "c" section by means at M6Nut and bolts.

The end section shall be covered by 0.8mm thick powder coated MS sheet.

The master section shall have laser cut profile to enable clip on tiles viz. perforated, Non- Perforated & diffused continuous LED section with acrylic sheet.

Hanging W Section:

Specially machine profiled W section 65x15x0.8mm.the section should be 2400 mm long & shall run across the length at the room.

Center to center distance between W section shall be 1000mm.

These sections are securely fixed to the slab by means of Metal fastener and 8mm GI rod fully threaded (with hex nut for precision level adjustment.)

The two-master section shall be attached to each other by means at fixing pate 45x34mm & M6 cage nut & bolts

U Section:

Machine profiled ‘U’ Section 150x77x0.6mm section to accurate continues running light.

It shall have provision for fixing acrylic sheet.

This whole assembly shall be hang from roof slab with help of anchor fastener and full threaded GI rod.

Ceiling Plank:

Plank shall be made from 0.6mm thick GI powder coated sheet of approved shade and sizes.

Light fitting can be defined as per the LUX requirement.

It shall have Laser cut circular hole for light fixing as per defined lux requirement and approved layout.

Non-perforated tile slots to be punched to accommodate AC grills.

8.9 Lighting and Illumination of Control Room.

LED dynamic lights

Brief:-LED colour changing lights. The lights shall be available in flat panels and shall be dimmable. These shall be designed and developed with slim shape for stylish look. The product shall have better colour rendering index for interior illumination.

In LED color changing lights shall have three basic colours like cool white, warm white and neutral white. The user shall be able to tune to any colour temperature between 2700 to 6500 Kelvin. The master controller shall be able to control upto 32 luminaires. The system shall be expandable, flexible system and user friendly to change the color/dimming as per pre-decided schedule. The LED colour changing lights shall have uniform light distribution without any spots on surface of panel, to make it highly luminous.

8.10 WIRING FOR CEILING LIGHT

i. Wiring for ceiling lights: For ceiling wiring inter looping will be done and switches will be provided.

ii. The system of wiring shall consist of PVC insulated copper conductor stranded flexible FRLS wires of 1100 volts grade of insulation, in metallic conduits for all exposed wiring and PVC/ metallic conduits for all concealed wiring. Minimum size of copper conductor shall be 1.5 sq. mm for lighting and 2.5 sqmm for power. Color code shall be maintained for the entire wiring installation that is Red/Yellow/Blue (or as per Local Standards) for the all single phases, Black for neutral and Green for earthing.

iii. Appropriate ferrule will be used in both the side (LDB Side &Switch’s Side)

iv. Note – Each Light Fixture will have 3 Wires: Phase, Neutral & Earth individually & If there is a need of another wire for Dimming/Dynamic Lighting Purpose then it will add on.

v. **SWITCHES & SOCKETS**

a. Compliance to stringent quality norms, Dual shutter mechanism for easy & better fitment Wide & flat switch knob for easy operation. FR grade polycarbonate with high impact resistance, shock proof & UV rays stabilized.

vi. **MCBs**

a. For the control and protection of low voltage installations against overload and short circuits.

b. Ripping characteristic: C Curve – 5 to 10 x In

c. Rated at 25°C to -50°C

d. Isolation function

e. Double entry points, separate bus bar entry, open mouthed terminal and lift clamps.

8.11 Acoustic Laminate Flooring in other areas: -

Acoustic flooring (shall reduce impact sound by 14dB (ISO 717-2)). It shall be twinlayer linoleum built up from 2 mm Marmoleum and a 2 mm Corkment backing. Flooring shall be decorative type of approved shade, pattern, texture and design and of approved manufacturer. Dimensions shall be as per the final approved design and site requirement. Flooring shall be laid over concrete floor with laying compound strictly as per manufacturer’s specification.

For fixing details please refer the procedure mentioned below.

a) Areas to receive material should be clean, fully enclosed and weather tight with the permanent HVAC in operation. A minimum temperature 68º F (20ature 68anent HVAC in operation. A minimum cleaning prior to beginning the installation, maintained during the installation, and for at least seven days following the installation.

b) Installation should not begin until the work of all other trades has been completed, especially overhead trades.

c) Areas to receive material shall be adequately lighted to allow for proper inspection of the substrate, installation, seaming and for final inspection.

d) Concrete substrates shall be structurally sound, rigid, smooth, flat, clean, and permanently dry. The concrete surface must be free of all foreign materials including, but not limited to, dust, paint, grease, oils, and solvents, curing and hardening compounds, sealers, asphalt and old adhesive residue.

e) Concrete substrates shall have a minimum compressive strength of 3,000 psi and a dry density of at least 150 pounds per cubic foot.

f) Concrete substrates on or below grade are required to have an effective moisture vapor retarder installed directly below the slab. The vapor retarder shall be puncture and tear resistant with a minimum thickness of 0.010" and a presence of 0.1 y. (Refer to ASTM E 1745.).

g) Imperfections such as chips, spills, cracks, and joints must be repaired using suitable patching and leveling materials. Always follow the manufacturer's recommendations for the use and application of these products. Refer to the Substrate Preparation section of this guide for additional information.

h) Use material from the same batch/dye lot.

i) Install rolls in sequence by roll number and cuts from each individual roll in consecutive order.

j) Do Not Reverse sheets for seaming.

k) Install one sheet at a time, making sure to place the material into wet adhesive.

l) Remove fresh adhesive residue immediately with a clean white damp cloth. Dried adhesive can be removed with a clean white cloth and mineral spirits.

m) Linoleum will expand slightly in the width and shrink slightly in the length when placed into the adhesive. Proper installation procedures will compensate for this characteristic.

n) Measure the area to be installed and determine the direction in which the material will be installed and. seam placement. Seams must be a minimum of 6" away from underlayment and concrete joints, saw cuts, etc.

o) Cut the required length for the first sheet off the roll, adding approximately 3" - 6" for extra trimming.

p) The factory edge must be trimmed to produce a clean edge suitable for seaming.

q) Position the straight edge approximately 1/2" - 3/4" from the factory edge and score the material using the utility knife along the straight edge. After scoring, complete the cut using a hooked blade knife following the score line. Hold the blade at a slight angle to the surface of the material so the seam edge will have a slight undercut.

r) When ready to adhere the first sheet, lap the material back about halfway from one end.

s) Begin spreading adhesive at the lap point and work back toward the wall. Spread the adhesive from the side wall up to the pencil line at the seam edge. For longer sheets that have not yet been trimmed to fit at the top, stop spreading the adhesive approximately 4' - 6' from the wall to allow for final fitting at the ends after the center portion has been adhered.

Note: Not spreading adhesive approximately 4' - 6' at the end of each sheet allows any shrinkage of the material to occur within the center of the sheet, ensuring a tight fit and seam at the end of the sheet.

t) When installing acoustic laminate and linoleum with jute backing on porous substrates, no open time is necessary before placing the flooring material into the adhesive. For non-porous substrates, a short open time may be necessary in order to allow the adhesive to develop body before placing the flooring material into the adhesive, but DO NOT ALLOW THE ADHESIVE TO DRY. The flooring material MUST always be placed into wet adhesive and rolled immediately. Check for adhesive transfer frequently. There must be a wet transfer of adhesive to the material backing to achieve a secure bond.

u) After adhering, immediately roll the flooring in both directions using a 100-pound roller. Roll first across the width and then along the length so that any trapped air pockets will be removed.

v) The flooring material must also remain in contact with the adhesive while the adhesive is drying and curing.

w) Adequate relaxing should enable the material to remain in contact with the adhesive, but if necessary, weight should be applied after rolling to ensure that the flooring material remains in full contact with the adhesive while the adhesive is drying.

Note: To ensure proper transfer of adhesive to the material backing at walls and fixtures, roll the edges of the material with a steel steam roller.

GENERAL NOTES: -

1. **The Command and Control room paneling and partition to have minimum 15% thermo-fused printed tiles (with similar material of construction as that of paneling and partition tiles) to print local art of state and increase the association of the facility with the state. Design will be selected by the.**

8.12 Control Desk

The following specifications detail the minimum requirements of the Console System. Bidders must respond on the enclosed chart. This allows for a point-by-point technical response stating compliance, taking exception or providing requested information. Bids submitted without this chart will be considered non-responsive.

Vendor shall supply the following to obtain project level approval:

- Copy of ISO 9001:2008 Certification.
- Copy of Green guard certifications for full console. Certification for compliance with minimum indoor air quality standards.

- Copy of FSC certification (Forest Stewardship Council) for consoles. Certificate for compliance towards sustainable forest initiative ensuring wood used is from sustainable forest harvesting.
- Detailed CAD (PDF format) drawings of console and equipment layouts for coordination of site measurements, architectural, mechanical, and electrical project elements for each console type.
- Copy of test certification for the following ANSI/BIFMA test procedures performed by an independent testing laboratory or approved by a professional engineer:
    a. Concentrated Functional Load Test
    b. Distributed Functional Load Test
    c. Concentrated Proof Load Test
    d. Distributed Proof Load Test
    e. Leg Strength Test
    f. Stability under Vertical Load Test

The tests must be based on the ANSI/BIFMA X5.5-2008 Standard applied to the proposed product solution.

- Detailed CAD (PDF format) drawings of each console type with its specific equipment per application.
- Renderings of consoles and room upon request.

Pre-production review, to include a drawing submittal and component listing complete with samples of selected finish materials upon request.

Samples of the following material components, which demonstrate workmanship, shall be provided upon request:

a. Work surface sample with ergonomic nosing.
b. Sample panel construction and finish materials.

- The consoles shall be suitable for areas of Seismic zone, it should be Zone 4 or better.
- Control Desk shall be ROHS certified.

Work surfaces

- The work surface shall be designed to provide a smooth, level work area, while complying with accepted human factors criteria. All applicable ergonomic standards will be taken into consideration1, including view and reach distances, keyboard height, and knee-well space.
- The following custom options shall be available:

a. Work surface return with support panel. (Fixed work surfaces only)
b. Work surface return with painted metal support legs. (Fixed work surfaces only)

Technology Accommodation

Below Work surface Level (CPU storage). The console shall accommodate computer equipment* with a variety of optional processor shelves. Fixed shall be available with the hinged panels.

The desk should be capable of accommodating all the hardware component as per the requirements.

CPU Shelf Options Internal Components and Attachment:

1. Components shall have the following properties:
   a. Fixed processor shelf 16 Gauge Cold rolled steel, powder coated
2. Processor Shelf
   a. Fixed Shelf – 200 lbs. (90 Kg) load, 14 gauge CRS, Powder coated black
3. Maximum Equipment (Reduced Depth)
   a. Fixed Shelf – 21” (533 mm) x 8 ¾” (222 mm) x 19” (483 mm)
      - Termination board Options
      - Desktop Level (Under-counter and Rack-mount technology)

Above Work surface Level

- The console shall have the ability to have flat screen monitors and various desk accessories mounted on the rear slatwall. Standard slatwall heights include 150-180mm, and can be combination slatwall and partition structure. The slatwall design can be configured to accommodate equipment mounting on both sides and in aback-to-back configuration both modules share one set of slatwall.
- The following options shall be available:
  a. Articulating monitor arm, depending on console configuration.
- Cable Management
- Console System shall be designed to allow for unrestricted cable management and access.

Console Frame Structure

All sheet metal used for structural components shall be 14 Gauge cold rolled steel/ Extruded Aluminum Frame of min. 13 gauge or better. These components ensure square, rigid connection of the front portal to the rear frame assembly, module-tomodule connections at corner positions, and attachment of front, rear and end panels. Sheet metal parts to be produced on CNC machines to ensure precision.

The Console assembly should allow all applicable shapes (Convex, concave, straight) to complement the control room.

All sheet metal parts must be finished with a durable, black, electrostatic powder coating.

- Internal Components and Attachment

Components shall have the following properties:

a. Work surface support arm 12 Gauge Cold rolled steel, powder coated

b. Work surface support stiffener 14 Gauge Cold rolled steel, powder coated

c. Fixed processor shelf 16 Gauge Cold rolled steel, powder coated

- Work surfaces and Panels

Panels and work surfaces shall have the following properties:

a. Materials: 1” (25mm) particleboard/ 25mm thick Medium Density Fiber board (MDF), high-pressure laminate surface

b. Finish Horizontal grade laminate.

c. Static Load 50-lb./ linear ft.

d. Surface to Floor Distance Fixed 29”-29.5’’ (737- 750mm mm)27 ½”-28.15’’ (692-715mm) mm) clearance

- Panels shall have the following properties:

  a. The console must offer hinged clipped panels as an option for front and back. Hinged panels will hinge from the column. Standard is a low pressures laminate surface. Custom options include High-pressure laminate or Veneer.

  b. End Panels: 1 in Thermofused Melamine Laminate(LPL).

  c. Lower/Intermediate Panels ¾ in Thermofused Melamine Laminate (LPL).

- o The work surface shall be supplied with a nosing(waterfall edge). The nosing shall comply with the characteristics as follows: Should be manufactured from high impact polyurethane edging OR Moulded Polyurethane edging directly over the wooden top.

So that it cannot be removed from table. Comfortable and ergonomically sound. oAllows for curved sections with a min. 356mm radius. oNo T-Mold or flat edge banding will be accepted at the front edge for nosing.

- o Slatwall Component oSlatwall shall be 6063-T6 Extruded Aluminum, fully anodized, black in color.

Table 1. Space Planning and Configuration Design

- Applicant must submit a floor plan to scale, showing each item being proposed.

Elevation and section drawings will be required in the submittal with dimensions of height, width, and depth in order to determine compliance with the specifications.

Photo-realistic isometric color renderings of consoles and room upon request.

- All accessories being proposed need to be shown in drawings.
- Colors are to be selected from manufacturer’s standards. A Color Guide shall be submitted with the proposal.

Table 2. Comfort Air Conditioning at Command Centers

Cooling Capacity as per the requirements at each of the control rooms

Compressor– Hermetically Sealed Scroll Type

Refrigerant– R22 Type

Power Supply–Three Phase, 380-415V, 50 Hz

Air Flow Rate–minimum 19cum/min

Noise Level- < 50dB

Operation–Remote Control

Table 3. IBMS Solution for Control Room

8.13 Fire Alarm System

Fire can have disastrous consequences and affect operations of a Control Room. The early-detection of fire for effective functioning of the Control Room.

System Description

The Fire alarm system shall be a single loop address able fire detection and alarm system, and must be installed as per NFPA 72 guidelines.

Detection shall be by means of automatic heat and smoke detectors (multisensor) located throughout the Control Room (ceiling, false floor and other appropriate areas where fire can take place) with break glass units ones cape routes and exits.

Control and indicating component

The control panel shall be a microprocessor based single loop address able unit, designed and manufactured to the requirements of UL/EN54 Part 2 for the control and indicating component and UL/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 back lit 8linex 40-character alphanumeric liquid crystal display.

All system controls and programming will be accessed via an alphanumeric key pad. 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 upto 10 minutes to allow for investigation of the fire condition before activating alarm out puts. The operation of a manual call point shall override any verify command.

Manual Controls

Start sounders

Silence sounders

Reset system

Cancel fault buzzer

Display test

Delay sounder operation

Verify fire condition

Disable loop

Smoke detectors–Smoke detectors shall be of the optical or ionization type. Devices shall be compatible with the CIE conforming to the requirements of UL/EN54 Part 7. The detectors shall have twin LEDs to indicate the device has operated and shall fit a common addressable base.

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 UL/EN54 Part 5 the detectors shall have a single LED to indicate the device has operated and shall fit a common addressable base.

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 on to an industry standard conduit box.

Addressable Manual Call points must also be provided

Control & Monitor module must be provided for integration with 3rd party systems.

Audible Alarms–

Electronic sounders shall be colored red with adjustable sound outputs and at least 3 sound signals. The sounders should be suitable for operation with a 24 VDC supply providing a sound output of atleast 100 dBA at 1meter and 75dBA min, for a bed head or sounder base type device. The sounder frequency shall be in the range of 500Hz to 1000Hz.

Commissioning

The fire detection and alarm system will be programmable and configurable via an alphanumeric keypad on the control panel.

Aspirating Smoke Detection System

This specifications covers the requirements of design, supply of materials, installation, testing and commissioning of Aspirating Smoke Detection System. The system shall include all equipment's, appliances and labour necessary to install the system, complete with high sensitive LASER – based Smoke Detectors with aspirators connected to network of sampling pipes.

Codes and standards

The entire installation shall be installed to comply one or more of the following codes and standards:-

NFPA Standards, US

British Standards, BS5839 part:1

Approvals

All the equipment's shall be tested, approved by anyone or more:

LPCB (Loss Prevention Certification Board), UK

FM Approved for hazardous locations Class1, Div2

UL (Underwriters Laboratories Inc.),U

ULC (Underwriters Laboratories Canada), Canada

Vds (Verbandder Sachversicherere.V), Germany

Design Requirements

The System shall consist of a high sensitive LASER-based smoke detector, aspirator, and filter.

It shall have a display featuring LEDs and Reset/Isolate button. The system shall be configured by a programmer that is either integral to the system, portable or PC based.

The system shall allow programming of:

a) Multiple Smoke Threshold Alarm Levels.

b) Time Delays.

c) Faults including air flow, detector, power, filter block and network as well as an indication of the urgency of the fault.

d) Configurable relay out puts for remote indication of alarm and fault Conditions.

It shall consist of an air sampling pipe network to transport air to the detection system, supported by calculations from a computer-based design modeling tool.

Optional equipment may include intelligent remote displays and/or a high level interface with the building fire alarm system, or a dedicated System Management graphics package.

Shall provide very early smoke detection and provide multiple out put level scor responding to Alert, Action, and Fire 1 & 2. These levels shall be programmable and shall be able to set sensitivities ranging from 0.025–20% obscuration/meter.

Displays on the Detector Assembly

The detector will be provided with LED indicators.

Each Detector shall provide the following features: Alert, Alarm, Fire 1 and Fire 2 corresponding to the alarm thresholds of the detector/ Smoke Dial display represents the level of smoke present, Fault Indicator, Disabled indicator

Sampling Pipe

The pipe shall be identified as Aspirating Smoke Detector Pipe along its entire length at regular intervals not exceeding the manufacturer's recommendation or that of local codes and standards.

Installation

The Contractor shall install the system in accordance with the manufacturer's recommendation.

Where false ceilings are available ,the sampling pipe shall be installed above the ceiling, and Capillary Sampling Points shall be installed on the ceiling and connected by means of a capillary tube.

Air Sampling Piping network shall be laid as per the approved pipe layout. Pipe work calculations shall be submitted with the proposed pipe layout design for approval.

The bidder shall submit computer generated software calculations for design of aspirating pipe network, on a ward of the contract.

8.14 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 online access control system. Access control shall be provided for entry/exit 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 conditions pecially for stair case and main doors. Entry to the restricted area shall be by showing aproximity 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.

8.15 Rodent Repellent

The entry of Rodents and other unwanted pests shall be controlled using non-chemical, non-toxic devices. Ultrasonic pest repellents shall be provided in the false flooring and ceiling to repel the pests without killing them. However periodic pest control using Chemical spray can be done once in 3 months as a contingency measure to effectively fight the pest menace.

9 Data Centre Infrastructure Requirement

9.1 IBMS Solution for Data Centre

It is aimed to meet the requirement of NDMC's high availability and maintain uptime of the IT services to keep its Operations safe, secure and operational. Scope of this work will also involve designing the Data Centre considering N+1 redundancy, remote manageability & scalability and setting up the infrastructure for high efficiency containing the following elements:

1. Server & Network racks with cooling, Monitoring and remote management system.
2. False ceiling for data center
3. Safety & security of Data Center
    - i. Fire alarm System & Fire Suppression System
    - ii. Access Control system
    - iii. Video surveillance system
    - iv. Rodent Replant System
    - v. Water leak detection system
4. Redundant and modular Power Distribution system
5. UPS with modular/hot swappable batteries.
6. Installation and configuration of Integrated Management Software for centralized monitoring and control of Safety and Security System.

The Data Center approach will be in two phases where 50% Capacity which will be 5 Racks Solution will be installed immediately and will augmented for another 50% 5 Racks in Future, if required, all low side work such as Civil Works, Interior Works, electrical Cabling, Lighting, Flooring and Electrical DB's to be designed for both the phases.

9.2 Server and Network racks with cooling & Monitoring system

1. **Network & server Racks specification:** Racks will be used to house all the servers/network/storage devices. Rack is designed as per safety standards to withstand the modern IT infra requirement. Both front & rear door should be designed to give active high performance liquid cooling system with handle lock system.

    Dimension of racks: for Server / Storage / Network – 600/800W X 2000H (42U) x 1200D

    Each Rack should include: Frame Of sturdy frame section construction, consisting of 16 x folded rolled hollow frame section punched in 25mm DIN pitch pattern, PU Gasket Side panel, 1.5 mm with PU Gasket ,Full Height 19" angle, Top and bottom cover. Vertical PDU, 32A, Single Phase, Digital Ammeter, C13X16, C19X4, 32A MCB & NEMA Socket as Input

    Specifications:

Sl No	**Parameter**	**Specification**	**Quantity**
1	Rack Height	42U	
2	Rack Width	19"	
3	Max Height	2000mm	

4	Max Width	800mm	
5	Max Depth	1200mm	
6	Color	Black / standard color	
7	Front Door	Glass with unique lock	
8	Rear Door	Steel	
9	Load bearing capacity	1400 kg	

- Covered top and bottom
- Rear space saving spilt door with 3-point secure locking
- Lockable & remove able side panels
- Front door with toughened glass
- Modular PDU socket strips: 3 phases 5 wire 440V, 50Hz, 32Amp PDU Each PDU should have 18 Nos. IEC C13 and 8 Nos. Of C19
- Stationary shelf-1 No/Rack
- Sliding Shelf – 2No/Rack
- Provision of fan mounting in top which does not occupy usable “U” space
- 24 port patch panel
- Surface finish: Nano ceramic coated, electro-dip coated primed to 20 microns and powder coated with texture polyester RAL 9005/7035 to 80 to 120 microns
- Optimized for high capacity cable management system
- Cable access openings with pre-installed brushes.
- Complaint to all security & stability standards and provided integrated electrical grounding

IP Based Automatic Rear door opening system

All 5 racks of data centre should be fitted with automatic rear door opening system; the door should open automatically in case of failure of the cooling system, high temperature and fire.

2. False Ceiling

The work should also involve provision of suitable ramps and steps for the movement of man and material to/from the Data center as per industry standard practices.

The Server room, communication room and staging area to be provided with suitable false ceiling for covering the various fittings on the ceiling. This should be fire resistant and able to support fittings like lights, various sensors of FAS, CCTV etc. It should be of removable type for any future maintenance.

9.3 Cooling units for server & Network Racks

High Performance Cooling Liquid Cooling Package

The Data center should be equipped with Liquid Cooling System; it is an air/water heat exchanger to remove high levels of waste heat from server enclosures and to provide uniform, effective, affordable cooling for Servers and similar IT equipment (switches etc) installed in server enclosures. Each liquid cooling system should be a closed unit consisting of a cooling system and cool either one or two server enclosures.

Rack Based In Rack DX Cooling System

The Data centre should be equipped with DX Gas Based In Rack Cooling System where Hot and cold aisle is maintained within the rack it has heat exchanger to remove high levels of waste heat from server enclosures and to provide uniform, effective, affordable cooling for Servers and similar IT equipment (switches etc) installed in server enclosures. Each DX Gas cooling system should be a closed unit consisting of a cooling system and cool either one or two server enclosures.

High Performance DX Gas Based Cooling System

The design of the unit should be optimised for use in data centres.

The integrated DX Gas Based heat exchanger should guarantees a cooling output of up to 12KW, combined with standard server enclosure dimensions, the lowest possible weight and comprehensive possibilities for monitoring.

The air/Gas Based heat exchanger is mounted on the side of the rack.

Cooling Rack DX Gas Based should offers enclosure-based cooling separate from the room air and is thus also able to reduce the noise level.

The unit should capable of providing cooling for either one or two server racks.

The hot server air is drawn off to the rear of the server rack. After cooling, it is expelled left and right in front of the 482.6 mm (19") level over the whole enclosure height and is thus made available to the IT equipment once more.

The use of an integrated EC fan module (cooling output 12 kW) achieves maximum efficiency and minimises the electrical energy consumption.

The unit is prepared for the incorporation of EC fan modules. A full fan configuration can thus also be realised to achieve redundancy or to minimise power consumption.

The standard integrated software/controller concept provides for automatic control of the specified server air intake temperature. The fan speed and cooling Gas Based flow rate are both infinitely variable, for precise matching to the power losses of the components installed in the IT rack.

The optimum operating point is thus achieved with minimum energy consumption and correspondingly reduced operating costs.

An intelligent sensor network monitors the air and Gas Based temperatures, as well as the Gas Based flow rate and leakage management.

The incorporation of three temperature sensors for the hot and cold air provides for redundancy.

An integrated fail-safe mode, furthermore, ensures reliable cooling, even in case of failure of the electronics.

The monitoring and alarm management for all physical parameters is realised via SNMP and Ethernet. A BAC net link is possible as an option. New control algorithms permit energy-efficient operation and take into account the demands of facility management.

Parameters	**Required Performance**	**Complied Y/N with Data Sheet cross reference Page No.**
Air throughput of fans	4800 m3/h	
Cooling output	12 kW	
Duty cycle %	100%	
Cooling medium	R410a	
Fan	EC	
Compressor	Speed Regulated	

9.4 Monitoring & Remote Management system for server & Network racks

Monitoring should be an intelligent monitoring system with an Ethernet 10BaseT network connection. The priorities of the various functions are monitoring, controlling and documenting physical parameters inside the Server and network racks.

These functions should be managed and controlled via different protocols.

The basis of the CMC should be the processing unit (PU unit). Several input/output units (I/O unit) should be connected to one processing unit via a patch cable. This/these function module(s) should connect to the sensors via a standard plug connector. The sensors should be coded so that the function blocks recognise automatically which sensors are connected.

Technical specifications:

Temperature Range	0^0C to 550^0C
Operating humidity range	5% to 95% relative humidity, non-condensing
Sensor / CAN - Bus connection units	4 or more
Interfaces	Network Interface :(RJ 45): Ethernet to IEEE 802.3 via 10/100 BaseT with PoE. Mini USB for system setting. Serial interface: 1 x for connecting Display unit or GSM Unit or ISDN UNIT User Interface: Integral WEB Server. Control room connection: Integral OPC Server. User administration: LDAP
Protocols	Ethernet :TCP/IPv4, TCP/IPv6, SNMPv3, Telnet , SSH, FTP, SFTP, HTTP, HTTPS , NTP, DHCP , DNS Server, smtp, xml , Syslog, LDAP

Redundant power supply	Input 24 V DC -1 X for connecting unit power pack. Power over Ethernet 1 x
Time Function	Real-time clock, energy -buffered (24 h) without battery/accumulator with NTP
Main sensors	NTC temperature Sensor for Access control infrared technology sensors.

9.5 Modular Redundant Power Distribution for Server room & Communication Room, Electrical cabling, power sockets & plugs.

Redundant & Modular Power Distribution:

The server and communication room will be provisioned with structured power distribution system. The 3 Phase commercial conditioned 440V/50Hz power supply will be made available by the user as the Distribution panel along with MCBs. The Vendor would install the UPS and would connect them with the 3 Phase supply available at the distribution panel. From the UPS power will be routed to a distribution panel to be installed by the Vendor. From the distribution panel, electrical cable will be drawn to the for distribution to the racks. The wiring will be carried out by the vendor by using fire retardant appropriate rating electrical cable.

Technical specifications

- SI will supply, install, test &commission, the main distribution panel.
- Complete Single Line Diagram should be made and certified by the user before starting the work.
- The wiring will be carried out by the vendor by using fire retardant appropriate rating electrical cable
- All power rating should be designed in consideration with all the devices involve inside server room.
- Complete distribution should not have any single point of failure,
- Complete distribution panel should be non-compartmentalized type, modular, totally shrouded
- Bus bars should be of Electrolytic Grade Copper as per EN 13601
- Bus bar support and cover systems are fire retardant as per UL 94 V0.

Power Socket & Plug

Power socket & Plug for Racks 3 Phase. Indoor type IP 65 (latched) , 35A, 5pin 4-pole + earth, Three phase 415volts, inter-locked Socket & Plug outlet similar to Lapp EPIC-Industrial connectors.

9.6 UPS with modular batteries(Adequate capacity with 30 minutes backup):

Uninterrupted Power supply: For entire set up, uninterrupted and efficient power supply is of primary concern. Hence, it is proposed to install a pair of modular   KVA (Max) UPS with N+1 redundancy. No single point of failure should be there in the complete uninterrupted power system.

Bidder should propose a solution that would help in right sizing the UPS System and avoid over sizing to keep system energy efficient.

Uninterrupted Power supply (UPS) specifications

Parameter	Specification
Qty	kVA N+1 Initial load
Modular	19" rack based
AC Power Supply Input	1. Input voltage(V) – 400 V(3Phase) 2. Frequency range – 40Hz-60Hz 3. Input current harmonic distortion – less than 5% for full load
Ac Power Supply Output	1. Output voltage(V) – 400V (3-phase) 2. Frequency 50 Hz 3. Power factor – 0.8 4. Voltage distortion <3%
Performance	1. Efficiency (at full load) > 95% 2. Paralleling should support up-to four units capacity or redundancy
Environmental	1. Operating Temperature 0°C to 40°C 2. Operating relative humidity – 0 to 95% 3. Storage temperature - 15°C to 45°C 4. Storage elevation – 0-15,000 meters
Communication & Management	1. Control panel with Multifunctional LCD status and control console 2. Audible alarm on battery On 3. Communication ports: RS232, SNMP, Mod Bus, remote panel 4. Emergency power off
Batteries & Runtime	1. Modular, user replaceable hot swappable battery 2. Battery efficiency >95% 3. Included Integrated Battery module. 4. 15 Min backup with suitable rating.

Desired Features:

- **Dual Main Input** – Allow the UPS to be connected to two separate power sources.
- **Parallel-capacity capable** – Allow usable of multiple UPS's simultaneously

- **Parallel-redundant capable** – Power the connected equipment with multiple UPS’s simultaneously
- **Cold start capable** – Provide temporary battery power when utility power is out
- **Automatic self test** – periodically battery self tests which ensure early detection of battery that need to be replaced
- **Power Module connected in parallel** – Allow immediate, seamless recovery from isolated module failures.
- **Scalable runtime** – Allowed additional run time to be added when needed.
- **Audible alarm** – Provide notification on changing utility power and UPS conditions.
- **Front Access services** – Should allow front access servicing to simplify installation and maintenance while minimizing space.

9.7 Safety & Security Systems:

Early Fire Detection and Extinguishing Systems:

Delivery of an active extinguishing system that detects and extinguishes fires in closed server and network cabinets.

High-performance fan must extract air samples for smoke analysis into the system's measuring chamber. The integrated extinguishing system must trigger if the concentration of smoke exceeds the limits. The extinguishing process must not be electrically conducting and must be fast and residue-free.

NOVEC 1230 must be employed as the extinguishing gas. The installation frame for the active extinguishing system must be designed as a 19" component group carrier. The system's installation depth must be specified such that it may be fitted into all 19" switch, server and network cabinets that possess an inside depth of > 1000 mm.

The installation and removal of the pre-assembled equipment must be carried out without interruption to the protected system's operations.

Technical features:

The following features must be provided:

Housing dimensions:	width: 483 mm - 19“ front plate (remaining width 445 mm) height: 1 RU (44.45 mm), depth: maximum 853 mm
Weight:	incl. extinguishing agent and propellant cartridge < 26 kg
Rated voltage:	100/240V AC, 50/60 Hz
Emergency power supply:	must be guaranteed for at least four hours
Ambient temperature	must be specified for +10°C to +35°C (operations) must be specified for -10°C to +60°C (storage)

Humidity: up to 95%, non-condensing

Protection type: at least IP 20

Connections: 1 potential-free change-over contact "advance alarm"
1 potential-free change-over contact "fire"
1 potential-free change-over contact "extinguish"
1 potential-free change-over contact "multiple malfunction"
24 V -3/+5 V rated voltage / 0.5A, ohm resistive load

Displays: 1 LCD with clear-text display for status reports

4 LEDs for "operation", "alarm", "multiple malfunction" and "mains/charger malfunction"

Sensors:
(Diffused light sensors) ST visual smoke alarm, approx. 2.0 – 3.9 %/m
HS visual smoke alarm, approx. 0.25 – 0.5 %/m

Air-flow monitor: approx. +/-10% flow rate

Protection volume: max. 3.0 m^3 (at air-change rate max. 10% / 20 min)

External devices: connection for manual trigger connector for door contact connector for external
signal equipment

Permits: CE conformity for the extinguisher unit in accordance with EC Directive 97/23/EC

Extinguisher container: must be integrated into one RU housing
Volume when empty: at least 2.2 l
Contents: at least two litres (=3.2 kg) Novec™ 1230

Extinguisher discharge through pressure charge produced by propellant gas cartridge. Integrated electrical trigger unit and integrated extinguisher-loss / filling-level monitoring (displays > 15% loss)

Connect rechargeable batteries, create electrical connections, insert active extinguishing system, create basic settings, carry out response test.

Accessory – intake pipe system

The intake pipe system is part of the fire-detection system. The pipe must be installed in an air-flow-facilitating manner in the flow of cooling air, air samples are taken in above the intake openings and analysed in the measuring chamber.

The intake pipe must be attached to the cabinet frame with pipe clips, pipe connectors, brackets and T-pieces must designed as push fit connections and it must be possible to disconnect them without tools.

Technical data:

Intake pipe system:	1 intake pipe with intake openings (2120 mm – to be shortened as required) 1 intake pipe (1100 mm – ditto)
Material / colour	polyamide / black
Ambient temperature [°C]	-25...+75
Outer/inner diameter [mm]	22/18
Weight [kg/m]	0.130

9.8 Access Control System:

Complete solution for restricting the movement inside the server room premises for authorized persons only. The access control system based on the finger printing based biometric system for providing physical security. Records are maintained in biometric system and report file can be generated from system based on date, time and authorized id.

Hardware Specifications

- **Intelligent Field Panel (IFP)**

The panels should be with UL 294, FCC and CE regulations:

IFP Architecture:

IFP shall utilize a fully distributed intelligence controller architecture whereby access decisions are made locally at the controller.

IFP shall utilize flash firmware for easy upgrades.

IFP shall support two access points.

IFP should be capable of expanding the functionality of the two access points to two access points IN/OUT, making the IFP a 4 reader controller.

IFP shall support local means of control through system and panel links as well as reader and reader/keypad input.

IFP shall support field interface to access control readers of various types.

IFP shall support field interface to eight variously configured alarm inputs.

IFP shall control four relay and four voltage outputs.

The Server software package (host computer) shall download panel specific data, including up to 3,000 cardholders & expandable up to 8000, to the IFP on the network. This data shall be stored within each panel and contain all pertinent information relating to the panel's functionality.

Host computer shall communicate global links and anti-pass back messages between panels.

Should communication with the Server software package (host computer) be lost, up to 1500 time-stamped events shall be stored in panel’s buffer, until communication is restored. Upon restoration of communications all event data shall be automatically uploaded to the host computer including the actual time of occurrence.

This functionality shall enable any off-line controller to maintain full access control processing capability. A card user shall not be aware of the off line condition.

A system that does not buffer event information when communications are lost will not be acceptable.

Controller will have 8 Input & 8 Output.

- **<u>Biometric Reader with Keypad & card</u>**

Templates :	9,500	
Integrated Proximity Reader :	125KHz Multi-technology	
PC to Reader / Panel to Reader :	Ethernet (CAT5) / Wiegand (6 Cond. Shielded 18 AWG)	
Dimensions / Weight :	5.7” (145 mm) Wide X 4.92” (125 mm) High X 1.3” (33 mm) Deep / 12 oz. (340 g.)	
Operating temperature / Humidity :	32° F to +131° F (0° C to +55° C) / 0 - 95% RH	
Power Requirements :	DC 9~24V, 1A	
Sensor (Resolution) / Template size :	Optical (500 DPI) / 352 bytes	
Authentication time Speed :	≤ 4 sec	
False Rejection / Acceptance Rate	0.01% / 0.001%	
Features :	LCD Display : 128 X 64 pixels; 2 LEDs; 10 number keys; 6 function keys; 1 bell button	

- Fail safe operation in case of no-power condition and abnormal condition such as fire, theft, intrusion and loss of access control etc.
- Inbuilt card reader
- Day, Date, Time and duration based access rights for user
- Adequate number of smart cards should be provided
- Interface with EM locks to manage the access to Server room

9.9 Video Surveillance System:

The bidder should propose a solution for IP enabled Closed Circuit Television System (CCTV) which will provide on-line display of video images on monitor. Cameras should be used to view specific areas of interest and create a record for post event analysis.

The system must be supplied with suitable number of cameras and Management Software to cover the server room. The system should have the facility of remote viewing over IP network and recording for at least 1 week.

Detailed specification of

The system should be fitted with an Hemispheric IP indoor camera for ceiling mounting, surveillance system for monitoring of activity outside the IT Server room. The system must be supplied with 3nos of Hemispheric

A	Hemispheric Camera	IP indoor camera for ceiling mounting (one on the front side & another on the rear side), The system should have Image sensor: 1/2.5" CMOS, 5 megapixel, color (day), Internal DVR: 4-GB Micro SD • Integrated microphone • Temperature sensor, illumination sensor, movement sensor, Activity Sensor, Analytics • 0.5-m Ethernet patch cable • Interfaces: Ethernet 10/100 (RJ45), remote viewing over IP network and recording.	3nos

9.10 Water Leak detection System

Bidder should propose a water leak detection solution which should be used in the sub floors of the area to be protected. It should have tape/Cable sensors, detection module and control panel as its major components. The leak sensor should able to detect electrically conductive fluids such as freshwater, salt water, glycol solutions etc and should be fitted underneath water pipelines. It should be capable of

- Detection of leaks in the sub floor
- Detection of leaks from air conditioners or support piping

System specification

- Supply Voltage : 230V 50Hz/60Hz
- LED Indications: Power, Alarm, Fault & Isolate
- Event recording facility: > 100
- Standard metal enclosure, wall mounting holes
- 80 character alphanumeric LCD
- Soft touch membrane keypad
- Configurable site name/location
- Dedicated outputs for all zones, hooter & Fire
- Configurable sensitivity adjustment
- Date and Time display
- Password protected event log clear facility
- Configurable baud rate selection
- Support network connectivity for SNMP monitoring
- Should cover the complete DC area

- From each network rack in the server room using Cat 6A & Multi Mode Fibre
- Along with LAN cabling, the bidder should also design and lay cable- trays for Storage System up to the racks in the Data Centre.
- Bidder should ensure that all the cable raceways are adequately grounded and fully concealed with covers. The cables should be appropriately marked and labelled.
- The data centre should come equipped with separate ducts for power supply distribution and NOC cable. The duct should be designed in such a way that it is possible to do the retro fitment in future. The ducts should be positioned in accordance with the racks for structured and snarl free wiring. The size of the power cable duct and NOC cable duct should be such that it must be possible to accommodate Wiring needs for Servers.

9.11 Integrated Management software:

Integrated management software for monitoring and, where required, controlling the physical infrastructure of the data centre in the fields of cooling, power supply and distribution, as well as security.

The following functions and features must include:

- All infrastructure sensor values, bus bar value and cooling values must be readable by SNMP
- Recording of warnings and alarms by SNMP traps
- Storage of all the data in a SQL database (MSSQL or Oracle)
- Quick and easy project planning of the data centre by means of location trees, views, charts and diagrams
- Lines, pie and Gantt charts/diagrams
- Graphics for standard devices must be already stored
- Integration of existing data centre floor plans (jpg format)
- Provision of standard charts
- Calculation engine to calculate values within the software (e.g. PUE)
- Dashboard functions
- Monitoring the status of all the components via a graphical view
- Simple creation of charts and graphs based on all the available data
- Simple creation of automated processes (“what should be done if...”)
- Controlling the infrastructure by writing values via SNMP
- Connection to higher-level management systems using Management Pack (SCOM) or SNMP
- Easy configuration of the software, in the ideal case with delivery as an appliance (software or hardware). Software appliance as a VM for VMware.
- Client/server architecture, clients must be able to run on Windows XP, Vista or Windows 7

- Report function
- User management with roles/rights. Accurately determining “who may do what”, right down to a single sensor
- Scalability from the single-rack data centre through to large-scale data centres
- Modular licensing, simple subsequent re-licensing for expanding data centre.

9.12 Seating Consoles & display:

- Bidder should also have to create cubicles/ workstation (2 nos.) in the network group work area and network operating centre
- LCD Screens: 50 inch of 2 LED Screens should also be provisioned in each NOC room of reputed brand.

9.13 Other Requirements:

Aesthetics:

The bidder also has to carryout changes as per aesthetics requirement of site with a concern of user designated site, to look the overall infrastructure looks aesthetically correct.

Civil and Interiors (Aesthetic)

Grid Based False Ceiling:

The top false ceiling should have sufficient space form the bottom of the beam in the server room. The lay in type grid ceilings should be made of naturally strong light-weight aluminium, zinc coated steel or stainless steel, pre-painted and treated for long life, rust free performance, and fire and moisture resistance. All grid ceilings must be designed for simple and economical installation on standard exposed systems or purpose designed grids which are easy to install and remove with minimum tools.

The salient features for the false ceiling should be as under: -

- Fully demountable - Easy to replace - Easy access to plenum grid tile and grid construction should enable frequent access to plenum without damage.
- The flexibility of the grid system should be such that it enables easy integration of services such as lighting, smoke detectors, speakers, Nozzles and air grilles.
- The grid ceilings shall be supplied with a range of acoustic treatments depending on the balance between intelligibility and confidentiality is to be achieved and quiet support for access floor panels.
- Mineral Fibre Acoustical Suspended Ceiling System Micro
- Look edge tiles with SUPRAFINE 15 mm EXPOSED GRID.
- Humidity Resistance (RH) of 95%
- NRC 0.75
- Light Reflectance >90%

- Thermal Conductivity k = 0.052- 0.057 w/m K, Colour White
- Fire Performance A2-s1.d0 in module size of 600 X 600 X 19 mm with Bio Block coating on the face of the tile, suitable for Green Building application, with Recycled content of 70-80%.
- Section flanges colour white having rotary stitching on all T sections i.e. the Main Runner, 1200 mm & 600 mm Cross Tees with a web height of 43mm and a load carrying capacity of 23.71 Kgs/M2. The T Sections have a Galvanizing of 120 grams.

Fire Rated Glass:

Fire rated glass has been provisioned to give a visibility to the NOC staff into the server farm area (wherever required). The technical specifications are given below.

- Fully glazed fire rated non-load bearing partition system for 120 minutes (E 120) fire rating. The glass should be SGG Pyro swiss Extra 6mm clear 120 minute fire rated (E-120) Non Wired Toughened glass having a light transmission of 89% and sound reduction of 32 db and compliant to class 1C1 category of Impact Resistance as per EN 12600
- The glass should be held in its place with the help of minimum 1.25mm GI beading which can be clamped or bolted to the fro file by 4 x 35mm steel screws at every 250m c/c and an intumescing type of the cross section of 5 x 20mm as per the test evidence. The glass panes are to be supported on non-combustible 5mm Calcium Silicate setting blocks. The maximum glazing size cannot be more than 1200 x 3000 mm

Fire Rated Gypsum Partition:

Gypsum partitions are required to divide the DC complex into different zones, as per the layout design, to server specific functions. Fire rated partitions are to be made slab to slab so as to provide an isolated, fire retardant area able to withstand fire and to prevent spread of fire to other areas.

The technical specifications are given below.

- The Gypsum board partition shall be provide to ensure their alignment by the method laid down by manufacturers, i.e. by fixing G.I. L & C section on the floor and ceiling and fixing gyp board onto them and fastening them to the walls/columns with the help of screws by the standard prescribed method, complete with sections from India.
- Gypsum finishing with tape and gypsum compound as specified by manufacturers. In double sided partition the above specification is valid with use of glass wool as insulation fill in between the gypsum boards for making the partition fire proof, acoustic and provides better degree of insulation.

Fire Rated Door:

Fire rated doors are provisioned for server farm area to provide a completely sealed fire retardant space. It will prevent fire from other areas to travel to server farm area and vice versa.

The technical specifications are given below.

- Providing & Fixing of thick steel fire rated door of 120 minutes fire rating fabricated.

- 1mm thick galvanized sheet with infill of fire rated proprietary insulation filler both faces of sheet with lock seam joints at stile edges and internal reinforcement at top, bottom and stile edges for fire rating.

- The door frames are manufactured from thick galvanized steel sheet pressed form to double rebate profile of size 100 x 50 mm (nominal). The door frames and door shutters are primed with etch primer. The shutter would be mounted with SS Ball Bearing Hinges of size 125mm x 75 x 3.0 mm of appropriate openings for view panel glass, if required.

Furniture and fixtures:

Room and Monitoring Room Console System:

The following specifications detail the minimum requirements of the Console System. This allows for a point-by-point technical response stating compliance, taking exception or providing requested information. Bids submitted without this stands cancel.

- The Console System shall be designed specifically for 7x24 mission critical environments such as System Control centers, Network Operation Centers, etc. Standard office grade, post and panel furniture will not be acceptable.

- Console System must be of modular design, facilitating future equipment retrofits and full reconfigurations without requiring any major modification to the structure or exterior elements.

Documentation:

The Bidder needs to Supply, Install, Test & Commission all the products specified in above data Centre specification & also provide complete single manual to run all the processes on satisfactory level. The Bidder needs to provide training to all the designated staff of user and provide sufficient amount of manuals.

All solutions offered should be IPv6 compliant.

Requirement

S. NO	ITEM	QUANTITY
1.	**Data Centre set Up – IT Security Solution** **For security and functionality of IT equipment's.**	**1 Set**
2.	Server and Network Racks , 600W /800 Wx2000Hx1200D, Front Glass Door with door stiffeners, Rear Sheet Steel Door with door stiffeners, Top cover plain, Bottom cover with cut-out of 400Wx150D with wire brush insert at back side for cable entry, 2 pairs of 42 U 19" L Type angles Front & Rear on 6nos of punched sections with "U" Marking Stickers. IP Based Automatic Rear door opening system	5 no
3.	**In rack Cooling units DX based for server and network racks**. 12,kW, 300x2000x1200 (WHD), Condenser, 12kW.	4 no

4.	**PDU for Server / network Racks**. Vertical PDU, 32A, Single Phase, Digital Ammeter, C13X16, C19X4, 32A MCB & NEMA Socket as Input.	10 no
5.	**Monitoring & Remote Management** system for server & Network racks.	1no
6.	Modular Redundant Power Distribution for Server room & NOC Room, Electrical cabling, power sockets, plugs, Earthling and raised floor.	1 set
7.	**UPS of required KVA (N+1) with batteries for 30 Min backup.**	1 no
8.	**Safety & Security Systems**:	
8.1	Early fire detection system with extinguishing system.	1 no
8.2	Access Control System	3 no
8.3	Video Surveillance system	3 no
8.4	Rodent Repellent System	1 no
8.5	Water Leakage Detection System	1 no
9.	Integrated Management software	1 no
10.	Seating Consoles & display.	1 set
11.	Other requirement : Aesthetic and Documentation	1 job

10. Annexure IV- ICCC –Design Consideration

Common guidelines/ comments regarding the compliance of equipment/ systems

1. The specifications mentioned for various IT / Non-IT components are minimum requirements. Bidders may propose higher specifications that are better suited to the requirements.

2. 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 8 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 NDMC.

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. SI 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).

16. All licenses should be in the name of the NDMC and should be Perpetual.

17. The proposed solution of SI 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, SI will be responsible to change the same with equivalent/better product without any additional cost to NDMC.

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 SI‘s responsibility to proactively take care of system obsolescence planning. The systems should not become obsolescent before 7 years. For proposed hardware and software systems, support from OEMs should be available for at-least 7 years. Failing which it will be SI‘s responsibility to provide support free of cost for initial 7 years of O&M.

22. Servers should be based on x86 platform in high density form factor to ensure optimal power and space usage.

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. SI shall deploy IPv4 and IPV6 dual stack supported network from day-1. The proposed solution and all appliances should meet this requirement. The SI 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.

Note: Bidder need to submit a copy of relevant section of the Gartner report along with technical proposal.

10.1 Key Design Considerations

Key design considerations taken into account are as follows –

- Designed for 24x7 online availability of application.
- Scalable solution on open protocols
- No propriety devices/ applications
- API based architecture for Integration with other web applications and Mobile applications

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

10.2 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.

NDMC system will be built on the following core principles:

10.2.1 Platform Approach

It is critical that a platform based approach is taken for any large scale application development, to ensure adequate focus and resources on issues related to scalability, security and data management. Building an application platform with reusable components or frameworks across the application suite provides a mechanism to abstract all necessary common features into a single layer. Hence the NDMC system is envisaged as a faceless system with 100% API driven architecture at the core of it. NDMC 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.

10.2.2 Openness

Adoption of open API, open standards and wherever prudent open source products are of paramount importance for the system. This will ensure the system to be lightweight, scalable and secure. Openness comes from use of open standards and creating vendor neutral APIs and interfaces for all components. All the APIs will be stateless. Data access must be always through APIs, no application will access data directly from the storage layer or data access layer. For every internal data access also (access between various modules) there will be APIs and no direct access will be there. System shall use open standards and protocols like BPMN, BPEL, OWASP, WSDL, SOAP, etc.

10.2.3 Data as an enterprise asset

Information is a high value asset to be leveraged across the organization to improve performance and decision making. Accurate information would ensure effective decision making and improved performance

Effective and careful data management is of high importance and top priority should be placed on ensuring where data resides, that its accuracy can be relied upon, and it can obtained when and where needed.

10.2.4 Performance

A best of breed solution using the leading technologies of the domain should be proposed in the solution ensuring the highest levels of performance. It will also ensure that the performance of various modules should be independent of each other to enhance the overall performance and also in case of disaster, performance of one module should not impact the performance other modules.

The solution should be designed in a manner that the following can be achieved:

- Modular design to distribute the appropriate system functions on web and app server
- Increase in-memory Operations (use static operations)
- Reduce number of I/O operations and N/w calls using selective caching
- Dedicated schemas for each function making them independent and avoiding delays due to other function accessing the same schema.
- Solution should provide measurable and acceptable performance requirements for users, for different connectivity bandwidths.
- The solution should provide optimal and high performance Portal Solution satisfying response time for slow Internet connections and different browsers.

10.2.5 Scalability

The component in the architecture will be capable of being scaled up to more user requests or handling more no. of input resources in various modules. Even inclusion of additional application functionalities can be catered to by upgrading the software editions with minimal effort.

The design of the system to consider future proofing the systems for volume handling requirements

- The application functions to be divided logically and developed as Modular solution.
- The system should be able to scale horizontally & vertically.
- ***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.

10.2.6 No Vendor lock-in and Replace-ability

Specific OEM products may only be used when necessary to achieve scale, performance and reliability. Every such OEM component/service/product/framework/SI pre-existing product or work must be wrapped in a vendor neutral API so that at any time the OEM product can be replaced without affecting rest of the system. In addition, there must be at least 2 independent OEM products available using same standard before it can be used to ensure system is not locked in to single vendor implementation.

10.2.7 Security

The security services will cover the user profile management, authentication and authorization aspects of security control. This service run across all the layers since service components from different layers will interact with the security components. All public contents should be made available to all users without authentication. The service will authenticate users and allows access to other features of the envisaged application for which the user is entitled to.

The system should be designed to provide the appropriate security levels commiserate with the domain of operation. Also the system will ensure data confidentiality and data integrity.

The application system should have the following

- A secure solution should be provided at the hardware infrastructure level, software level, and access level.
- Authentication, Authorization & Access Control: 3 factors (User ID & Password, Biometric, and Digital Signature) security mechanisms should be implemented to enable secure login and authorized access to portal information and services.
- Encryption Confidentiality of sensitive information and data of users and portal information should be ensured.
- Appropriate mechanisms, protocols, and algorithms necessary to protect sensitive and confirmation data and information both during communication and storage should be implemented.
- Data security policies and standards to be developed and adopted across the Smart City departments and systems
- In order to adequately provide access to secured information, security needs must be identified and developed at the data level. Database design must consider and incorporate data integrity requirements.
- Role based access for all the stake holders envisaged to access and use the system
- Appropriate authentication mechanism adhering to industry good practice of Password Policies etc.
- Ability to adopt other authentication mechanism such as Electronic Signature Certificates
- Authorization validity to be ensured for the users providing the Data to the system. Data should be accepted only from the entity authorized
- Data should be visible only to the authorized entity
- Audit trails and Audit logging mechanism to be built in the system to ensure that user action can be established and can investigated if any can be aided(e.g. Logging of IP Address etc.)
- Data alterations etc. through unauthorized channel should be prevented.
- Industry good practice for coding of application so as to ensure sustenance to the Application Vulnerability Assessment

System must implement various measures to achieve this including mechanisms to ensure security of procurement data, spanning from strong end-to-end encryption of sensitive data, use of strong PKI national standards encryption, use of HSM (Hardware Security

Module) appliances, physical security, access control, network security, stringent audit mechanism, 24x7 monitoring, and measures such as data partitioning and data encryption.

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

10.2.8 User Interface

The architecture and application solutions to be designed should promote simplicity and ease of use to the end users while still meeting business requirements. It should provide a simpler and more cost-effective solution. Reduces development time and makes the solution easier to maintain when changes in requirements occur.

This will be accomplished by the implementation of rich User Interfaces along with its integration with the DMS, Relational Data Store, Messaging and other external applications.

- Efficient and layout design are the key considerations that enhance usability which should be factored in while designing the application. Standard and consistent usability criteria must be defined. An intuitive, user friendly, well-articulated navigation method for the applications greatly enhances the usability of the application.
- Effective information dissemination
- Enhanced functionalities including personalized delivery of content, collaboration and enriching GUI features
- The load time for all web page user interfaces must satisfy both the following response time targets on 1 mbps connection:
    - 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

- o Support integration with native device API
- o Support utilization of all native device features
- o Support development of applications in a common programing language
- o Support integration with mobile vendor SDKs for app development and testing
- o Support HTML5, CSS3, JS features for smartphone devices
- o Support common protocol adapters for connection to back office systems (i.e. HTTP, HTTPS, SOAP, XML for format)
- o Support JSON to XML or provide XHTML message transformations
- o Support multi-lingual and language internalization
- o Support encrypted messaging between server and client components

10.2.9 Reliability

This is a very crucial system and data are of high sensitivity, the data transfer and data management should be reliable to keep the confidence of the stakeholders. The system should have appropriate measures to ensure processing reliability for the data received or accessed through the application.

It may be necessary to mainly ensure the following

- Prevent processing of duplicate incoming files/data
- Unauthorized alteration to the Data uploaded in the NDMC system should be prevented
- Ensure minimum data loss(expected zero data loss)

10.2.10 Manageability

It is essential that the application architecture handles different failures properly; be it a hardware failure, network outage, or software crashes. The system must be resilient to failures and have the ability to restart, and make human intervention minimal.

All layers of the system such as application, infrastructure must be managed through automation and proactive alerting rather than using 100‘s of people manually managing.

The entire application must be architected in such a way that every component of the system is monitored in a non-intrusive fashion (without affecting the performance or functionality of that component) and business metrics are published in a near real-time fashion. This allows data centre operators to be alerted proactively in the event of system issues and highlight these issues on a Network Operations Centre (NoC) at a granular level. The solution should be envisaged to utilize various tools and technologies for management and monitoring services. There should be management and monitoring tools to maintain the SLAs.

10.2.11 Availability

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

The solution should meet the following availability requirements

- Load Balanced across two or more Web Server avoiding single point of failure
- Deployment of multiple application instances should be possible
- Distributed or load balanced implementation of application to ensure that availability of services is not compromised at any failure instance.
- Network, DC, DR should be available 99.99 % time.

10.2.12 SLA driven solution

Data from connected smart devices to be readily available (real-time), aggregated, classified and stored, so as not to delay the business processes of monitoring and decision making, and will enable appropriate timely sharing across the Smart City organization.

Readily available and consumed device data will facilitate timely access of analytics reports at every level and department of the Smart City and provide timely analysis of data as well as monitoring of KPIs through SLAs resulting in effective service delivery and improved decision making.

10.2.13 Reconstruction of truth

System should not allow database/system administrators to make any changes to data. It should ensure that the data and file (data at rest) that is kept in the systems has tamper resistance capacity and source of truth (original data of invoices and final returns) could be used to reconstruct derived data such as ledgers and system generated returns. System should be able to detect any data tampering through matching of hash value and should be able to reconstruct the truth.

- Services/solutions should be flexible and extensible to respond to, accommodate and adapt to changing business needs and unanticipated requirements easily. Consolidate and simplify technology applications wherever possible to minimize complexity.
- Ongoing application, database and server consolidation may be required.
- Software should use meta-data to configure itself (using declarations rather than coding).
- Avoid proprietary solutions and technologies if possible. Consider adhering to latest industry best practices and technical standards.
- The infrastructure should support an environment that allows applications to start small, grow quickly, and operate inexpensively. An adaptable infrastructure provides the capability to add to the current infrastructure with minimum inconvenience to the user.
- The IT architecture should be designed to support the overall SLA requirements around scalability, availability and performance.

- Each application should be performance tested to identify performance issues. The potential performance bottlenecks need to be identified and cost-effective paths for performance improvements should be provided for these identified problem areas.
- The system infrastructure should be architected considering failover requirements and should ensure that a single server or network link failure does not bring down the entire system.
- The system should be reliable handling every request and yield a response. It should handle error and exception conditions effectively

10.2.14 Integration Architecture

This section recommends the proposed integration architecture aligning with the overarching architectural principles.

The following are the integration specifications for the various integration scenarios -

Real-time integration

All the Smart City applications will be deployed in the Data Centre while any external application of the Smart City ecosystem will reside in outside premises.

The need for a Service Oriented Architecture (SOA) and API Governance architecture is felt that will facilitate NDMC 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.

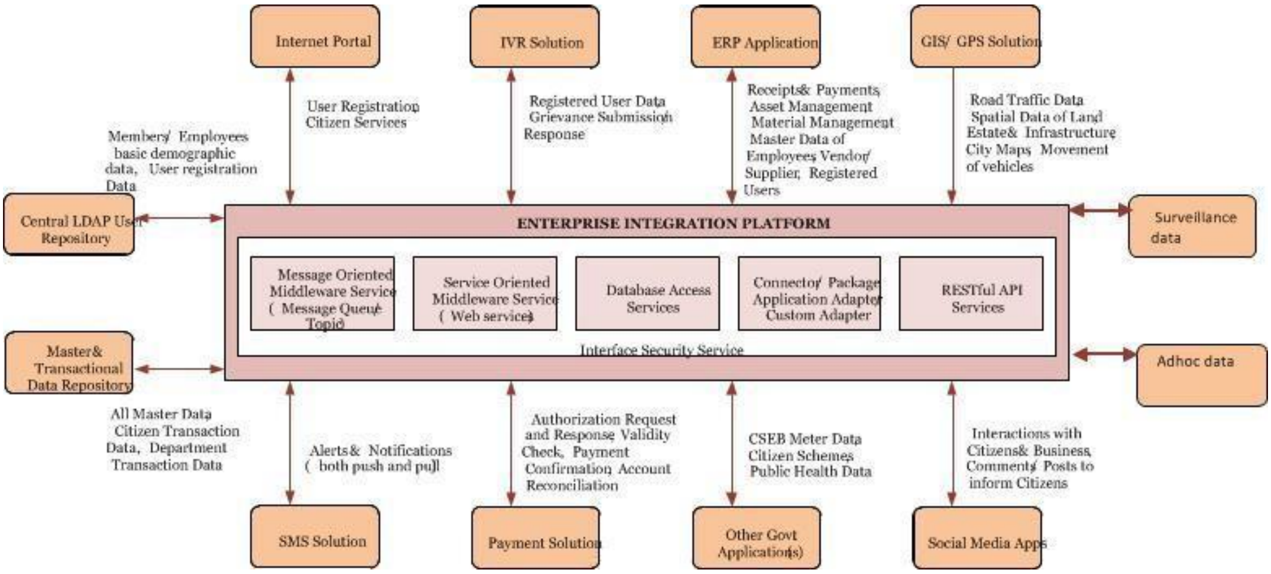

Internet Portal
IVR Solution
ERP Application
GIS/ GPS Solution
User Registration Citizen Services
Registered User Data Grievance Submission Response
Receipts& Payments Asset Management Material Management Master Data of Employees Vendor/ Supplier, Registered Users
Road Traffic Data Spatial Data of Land Estate& Infrastructure City Maps Movement of vehicles
Members/ Employees basic demographic data, User registration Data
Central LDAP User Repository
ENTERPRISE INTEGRATION PLATFORM
Surveillance data
Message Oriented Middleware Service (Message Queue/ Topic)
Service Oriented Middleware Service (Web services)
Database Access Services
Connector/ Package Application Adapter Custom Adapter
RESTful API Services
Interface Security Service
Master& Transactional Data Repository
Adhoc data
All Master Data Citizen Transaction Data, Department Transaction Data
Alerts& Notifications (both push and pull)
Authorization Request and Response Validity Check, Payment Confirmation Account Reconciliation
CSEB Meter Data Citizen Schemes Public Health Data
Interactions with Citizens& Business, Comments/ Posts to inform Citizens
SMS Solution
Payment Solution
Other Govt Application(s)
Social Media Apps

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 NDMC 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 NDMC 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 to NDMC, but it is a mandatory requirement that all the SMS based services (alerts and notifications) should be available as part of the solution. Following are some of the key requirements for the SMS services through the solution:

- Should contain required details/information and targeted to the applicant or designated officers of tax departments and other stakeholders and users as per prevailing TRAI norms
- Facilitate access through access codes for different types of services
- Support automated alerts that allows to set up triggers that will automatically send out reminders
- Provide provision for International SMS
- Provide provision to receive messages directly from users

- Provide provision for personalized priority messages
- Resend the SMS in case of failure of the message
- Provide messaging templates

Email Services: Email services are envisaged to be made available as part of the solution design to send alerts/intimations/automated messages to registered email ids, based on preferences set up/opted by individual users. An authenticated SMTP mail service (also known as a SMTP relay or smart host) is envisaged to be integrated with the solution for sending mail from the solution, and delivered to intended inbox. Support anti-spam features.

Payment Gateway: The solution is envisaged to have integration with payment gateways, to enable authorized Users make financial transactions, as per rights and privileges provided to him/her. The service provider is required to make the provisions for integration with such third party gateways and provide payment services, as per requirement of the NDMC. 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 Mark-up Language (Voice XML)
- 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:

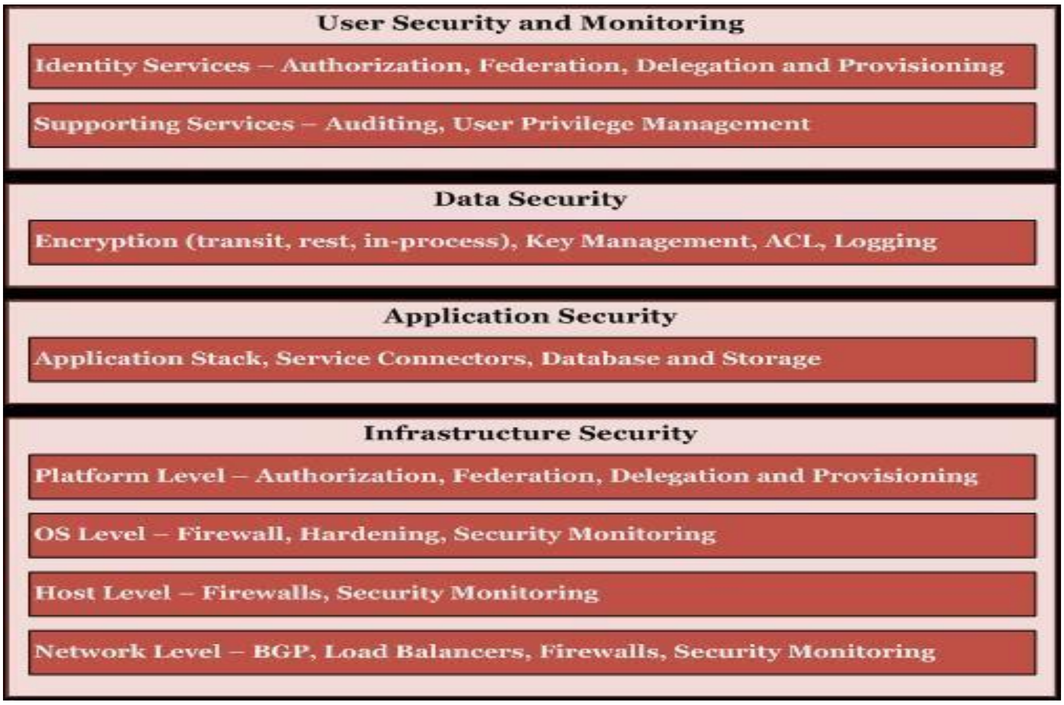
  - Interface Definition
  - Interface Owner
  - Interface Type
  - Interface Format
  - Frequency
  - Source System
  - API/Service/Store Procedure
  - Entitlement Service
  - Consuming System
  - Interface Layout (or) Schema

- 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
- Data exchange should be auditable

10.3 Security

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.



User Security and Monitoring

Identity Services – Authorization, Federation, Delegation and Provisioning

Supporting Services – Auditing, User Privilege Management

Data Security

Encryption (transit, rest, in-process), Key Management, ACL, Logging

Application Security

Application Stack, Service Connectors, Database and Storage

Infrastructure Security

Platform Level – Authorization, Federation, Delegation and Provisioning

OS Level – Firewall, Hardening, Security Monitoring

Host Level – Firewalls, Security Monitoring

Network Level – BGP, Load Balancers, Firewalls, Security Monitoring

Some of the key security principles are explained below.

SI 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 Centre.

10.3.1 User Security and Monitoring

Authentication & Authorization

A strong authentication mechanism should be considered to protect unauthorized access to the Smart City applications. Consider use of at least two of the following forms of authentication mechanism:

- Something you know, such as a password, PIN etc
- Something you have, such as a smart card, hardware / software security token etc
- Something you are, such as a fingerprint, a retinal scan, or other biometric methods

Levels of Authentication

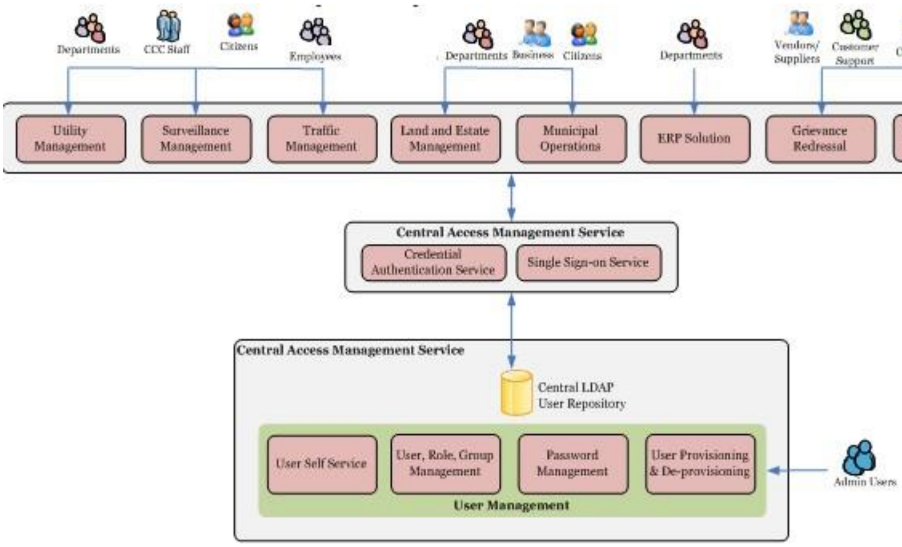
Based on the security requirements the following levels of authentication should be evaluated.

- 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 NDMC 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

10.3.2 Data Security

Traditional Structured Enterprise Data

NDMC 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 NDMC Smart City applications and stakeholders
- Data security controls to be put in place to restrict access to enterprise data based on roles and access privileges. Data audit logs should be maintained for audit trail purposes.
- Security controls will be able to be reviewed or audited through some qualitative or quantitative means for traceability and to ensure that risk is being maintained at acceptable levels.
- In order to adequately provide access to secured information, security needs must be identified and developed at the data level, not the application level. Database design must consider and incorporate data integrity requirements.
- Procedures for data sharing need to be established. Data integrity during data synchronization needs to be ensured across the enterprise.
- *Audit Capabilities:* The system provides for a system-wide audit control mechanism that works in conjunction with the RDBMS.
- *Maintaining Date/Time Stamp and User Id:* Every transaction, with a date and time and User ID, is captured. The system allows generating various audit reports for verification.
- *Access Log:* The NDMC Smart City System 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
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 behavior.

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, and 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 NDMC 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.

10.3.3 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
- o For effective prevention of SQL injection vulnerabilities, SI 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.

10.3.4 Infrastructure Security

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

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, and 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.

10.4 Software Development Lifecycle

Continuous Build and Deployment

The NDMC 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 SI 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.

10.5 Quality Assurance & Audit

A thorough quality check is proposed for the NDMC Smart City system and its modules, as per standard Software Development Life Cycle (SDLC). SI 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 NDMC. SI is required to incorporate all suggestions / feedback provided after the elaborate testing of the system, within a pre-defined, mutually agreed timeline. SI 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 NDMC that all applications installed in the system have been tested.

10.5.1 Automated Testing

SI 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, and 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.

10.5.2 Performance and Load Testing

SI 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.
- SI should perform the load testing of NDMC 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 custo 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.

10.5.3 Audits & Inspections

SI is expected to perform the following activities for overall ICCC Audits & Inspections organized by NDMC or its authorized agency:

SL. No.	Activities
1.	Should provide necessary information at the time of such activities
2.	Should provide necessary environment and access to the authorized personal for conducting such activities
3.	Should provide necessary evidences for Audits (if asked by the auditor / inspector) at the time of such activities. Data Leak Prevention (DLP)Solution should be able to support white listing of websites - No other website except listed should be allowed
4.	Solution should be able to separate history of successful and unsuccessful web visits
5.	Solution should be able to list all default 'In streaming' or ad pages should be denied to enter End-point
6.	Solution should be able to support list of successful only web visit for a given End Point
7.	Solution should be able to list top 10, 20,100 users of Internet - Report
8.	Solution should be able to list top 10, 20, 50 sites visited by all users - Report
9.	Solution should be able to list of all visitors of a given website
10.	Solution should be able to support view identity information on the sender (such as full name, manager name, business unit) and destination of the transmission (e.g., data sent to a blog, chat board, spyware site)
11.	Solution should be able to throw alert in case any bypass/Proxy is used.
12.	Solution should be able to support ability to whitelist email addresses
13.	Solution should be able to support ability to whitelist email domains
14.	Solution should be able monitor all mails sent out of corporate domain to be monitored
15.	Solution should be able to support filtering of mail content for specified words (content filtering), signature/ fingerprint
16.	Solution should be able to support attachment content to be filtered for specified words (content filtering) , signature/fingerprint
17.	Solution should be able to support violation of policy to be alerted to specified emails based on content filtering,
18.	Solution should be able to support Go Ahead or Abort (User should have option to send mail even on violation after reconfirmation) On violation, pop up warning
19.	Solution should be able to support alert to be sent to named HoD and IT In case of Go Ahead.

20.	Solution should be able to support saving in draft mail to be monitored
21.	Solution should be able to support Workflow for approval by named individual in case of 'violation' attempt
22.	Solution should be able to support coverage of Webmail or Mail agent (Outlook etc)
23.	Solution should be able to support set rules for each channel - Allow/Deny for external media (MTP devices/ CD-DVD/ USB Devices)
24.	Solution should be able to support capturing of document transfer to USB devices with specification weather data transferred can be monitored/blocked.
25.	Solution should be able to support pop 'Violation' message to user as well as log transfer files to each channel in case of End Point where it is denied
26.	Solution should be able to support user to have 'Go Ahead' or 'Abort' option in case of popped 'Violation' message
27.	Solution should be able to support alert to be sent to named HoD and IT
28.	Solution should support whitelisting of USB based removable devices
29.	Solution should be able to support allowing to set rules for allowed USB Ports -- option to capture all documents or just document name - based on category of user.
30.	Solution should be able to support choice to retain few documents for investigation for longer duration
31.	(No delete option)
32.	Solution should be able to support activities of Remote support software (such as Team Viewer) can be monitored and logged.
33.	Solution should be able to support printing facility monitor/Blocking per user wise/group wise/policy wise.
34.	Solution should be able to provide shadow copy of sensitive documents submitted for printing.
35.	Solution should be able to provide Real time notification for any sensitive documents submitted for printing.
36.	Solution should be able to support IM Channels (skype/ Gtalk) monitored/Blocked as per user/profile wise.
37.	Solution should be able to support blocking of all IM Channels
38.	Solution should ensure data is not copied from official LAN to third party LAN
39.	Solution should be able to enforce policy and generate logs even when system is not connected to corporate network
40.	Solution should be able to grant exception even if system is offline
41.	Solution should be able to detect and inspect image files
42.	Solution should be able to detect and report presence of : audio, video, graphic , designing files
43.	Solution should be able to allow Username/password of applications should travel in encrypted form
44.	Solution should be capable to Encrypt Data when copying in external media.
45.	Solution should be able to generate alert of violation if an encrypted document is transmitted, which can't be checked for content/fingerprint violation
46.	Solution should be able to recursively inspect the contents of compressed (e.g. ZIP, TAR, RAR) archives
47.	Solution should be capable in automatically notifying senders or their managers when a policy has been violated
48.	Solution should be capable in providing on-screen notifications to users
49.	Solution should be capable in providing automatic workflow functionality for tracking the remediation of an incident (e.g. status codes, attributes, assignment queues, severity
50.	Solution should be capable in generating granular Report User Wise / Policy Wise / Category Wise /Violation Wise
51.	Solution should be capable in providing summary Report Weekly / Monthly /for a given period
52.	Solution must ensure compatibility with existing Firewall/UTM and Web Proxies that might be present in the organization network

53.	Solution should be able to control unauthorized activity even if the user boots the operating system in safe mode
54.	Solution should be capable in reporting user activity through Screenshots of activities for user under surveillance
55.	Solution should be capable in providing a daily report of those clients who did not talk to server in last 'n' number of days to investigate the reason (travel/agent corruption)
56.	Solution should be capable in providing options for creating custom reports. (e.g. Provide custom report filtering across different variables and attributes; provide custom report summarization and grouping across different variables and attributes)
57.	Solution should be able to provide reports for all historical events
58.	Solution should be capable in providing comprehensive report covering summarized snapshot of unauthorized and suspicious activities occurring in the network listing top violators which can be leveraged for the purpose of compliance audits.
59.	Solution should be capable in providing search Based on specific time periods
60.	Solution should be capable in providing search for content based on Keywords, content , document type (Word, excel, CAD)
61.	Solution should be capable in providing search by alert ID , by client (Username / hostname)
62.	Solution should be capable in providing Email and Email Attachment based on specified sender / recipient
63.	Solution should be capable in providing Search by URL visited
64.	Solution should be capable in providing Search by groups like Audio Video, Images , attachments
65.	Solution should be capable in providing Search By Policy
66.	Solution should be capable in providing Search By Violation type (High/Medium/Low)
67.	Solution should be capable in providing facility to create new query and save it for future execution
68.	Solution should be capable in securing agent from administrative users tampering
69.	Solution should be capable in providing centrally controlled Installation and Removal facility.
70.	Solution should be capable in providing log of any tampering with the agent
71.	Solution should be capable in detection of tampering by end user and restart itself if it's stopped
72.	Solution should be capable in ensuring communications between agents and server are authenticated and secure
73.	Solution should be capable in providing Client - server log/document transmission should be in highly compressed mode
74.	Solution should be able to handle Client - server log/document transmission and should not choke the bandwidth
75.	Solution should be capable in providing Report of Bandwidth usage for client-server transmission for each site
76.	Solution should be capable in providing application level High Availability
77.	Solution should be capable in capturing Content of documents/mail and its attachment sent out
78.	Solution should be capable in providing facility to retain Data inside DLP system for any no of days (Choice to retain data for specific period in case of investigation/evidence requirement)
79.	Solution should be capable in providing facility to overwrite data If not chosen to retain for specific period or on DB space reaching its capacity
80.	Solution should be capable in providing multiple forensic repositories
81.	Solution should be capable in providing Software Whitelisting
82.	Solution should be capable in providing facility for Exception to SW While listing should be configurable user wise/group wise.
83.	Solution should be capable in providing software whitelisting to cover bypass proxy software too.
84.	Solution should be capable in providing facility to NW Whitelisting
85.	Solution should be capable in providing Exception to NW While listing which can be configurable user wise/group wise.

86.	Solution should be capable in providing facility for easy installation of agent, standard rule set for different class of users
87.	Solution should be capable in providing Remote configuration of agent to amend rule set for temporary/permanent exemption
88.	Solution should be capable in providing Report on active, passive and corrupted clients
89.	Solution should be capable in providing End Point should be identified by login name (AD) - for End Point on Active Directory
90.	Solution should be capable in providing identification of EP by login name or host name : For EP that are isolated or in workgroup
91.	Solution should be capable in providing Search of EP activities based on host-name or user name
92.	Solution should be capable in prevention of Disabling/removing of agent by end user
93.	Solution should be capable in providing facility for configuration of server should be saved in a named folder as backup (for restoration in case required).
94.	Solution should be capable in enabling incident work flow through email notifications.
95.	Solution should be capable in providing facility to Integration with directory services for multiple domains (eg, solar.xxx.in; epc.xxx.in etc.)
96.	Solution should be capable in providing Facility of Scheduling of AD Synchronization with DLP Server (to avoid synchronization in peak hours)
97.	Solution should be capable in providing synchronization with AD server, new clients added in AD should get highlighted in DLP Server (This will prompt in installing agent on such client)
98.	Solution should be able in providing Synchronization with AD server should capture all the details of users/device (Name, dept., phone etc, if available)
99.	Solution should be capable in providing facility to Admin that in the event of Any application is not working, Admin should be able to allow it.
100.	Solution should be capable in providing White-listing of URL
101.	Solution should be capable in providing facility to Any user/group or Any device or any site can be kept in exception.
102.	Solution should be capable in providing facility to Any service incase not working due to DLP client it can be put to exception.
103.	Solution should be capable in providing facility for Version up-gradation can be done without any downtime./ single console
104.	Solution should be capable in providing facility for Client up-gradation can be done remotely by pushing upgrade package.
105.	Solution should be capable in providing facility for providing user SI package; user should do it without feeding anything in it.
106.	Solution should require password protection for Uninstall of Agent
107.	Solution should be capable in providing facility for stealth mode deployment; user should not able to make out new service getting installed
108.	Solution should be capable in providing facility for silent installation
109.	Solution should be capable in providing facility for creating separate roles for technical administration of servers, user administration, policy creation and editing, incident remediation, and incident viewing
110.	Solution should be capable in providing facility for Admin activity audit logging
111.	Solution should be capable in providing facility for Dashboard Alert mechanism for system health as well as all type of violation.
112.	Solution should be capable in providing Bandwidth constraint alert during client-server transmission/synchronization. Solution should be Able to generate error logs for support team investigation
113.	Solution should be capable in providing facility for alert if Client is not working for a number of days
114.	Solution should have facility for Professional services for training, installation, configuration
115.	Solution should be capable in providing facility for Software upgrade policy (maintenance only, maintenance and major releases)

116.	On premises support should be available.
117.	Solution should be capable in providing facility for 24X7 support
118.	Solution should be capable in providing facility for logs to be saved off the system
119.	Solution should be capable in providing facility for Log report to be generated
120.	Solution should be capable in providing facility for Read only Auditor account can be created for audit purpose.
121.	Solution should be capable in providing agents for various OS (Windows- from XP to windows 10)
122.	Solution should be capable in providing facility for the case when up-gradation of OS, DLP patch should be available so that its functioning is not affected.
123.	Solution should be capable in providing analytical framework which can be used for reducing false positives for types of data that incorrectly match a pattern
124.	Solution should be capable in providing facility for architecture support for remote sites and network users distributed across many different locations
125.	Solution should be capable in providing facility for agent to be connected via vpn/ data card or any third party network
126.	Solution should be able in providing network activity monitoring via all major browsers
127.	Solution should be capable in providing facility for Data at rest scanning on End Points
128.	Solution should be capable in providing facility for time based productivity monitoring
129.	Solution should be capable in providing facility for Gmail monitoring (including Draft)
130.	Solution should have Web based monitoring system, in a format usable by non-IT business level users
131.	Solution should support data at rest scanning and detection of confidential data on endpoint computers (desktops and laptops)
132.	Solution should allow administrators to create custom policies based on keywords and patterns for sensitive data
133.	Solution should be able to report the list of files that contain sensitive data, along with details of sensitive data found.
134.	Solution should be able to report all applied policy violations inside a file.
135.	Solution should support Agent-Based Discovery.
136.	Solution should be able to scan common document and compressed file types on the basis of their file extensions.
137.	Solution should provide options to set scan specific or group of file types to speed up the scan process.
138.	Solution should perform reporting of events via the central monitoring console with appropriate metadata (date/time, user, file name, file path etc.)
139.	Solution should support storing and indexing of captured event data for inspection at a later date
140.	Solution should provide a report for each sensitive file activity per agent.
141.	Solution provided should not interfere with the day-to-day functioning of users on that agent.
142.	Solution should have agent that would run in background and would not interfere with normal resources where it is installed.
143.	Solution should provide an ability to search sensitive files based on specified time period of performed scans.
144.	Solution must be able to generate shadow logs of all outgoing emails, email attachments, files uploaded via Web that are found to be sensitive
145.	Solution must provide capability to provide real-time SMS alerts to the security administrator
146.	Solution must be capable to perform content analysis of online web searches performed by the end user
147.	Solution must be capable to perform content analysis of chats performed by the end user (Google Hangouts, Skype Chat, Google Talk)
148.	Solution must able to support internal access restriction, namely files copied to removable media in encrypted form should not be accessible from any third party computer
149.	Solution must be able to generate automatic cyber intelligence reports for risk analysis and highlighting to the key management personnel of the organization

CCTV Locations

S.NO.	NDMC Facilities	No of Location	Type 1	Type 2	Type 3	Type 4	Total No. of Cameras/Location	Total No. of Cameras
			Panoramic Camera	Fixed IR Camera	Fixed Box Camera	Camera-High Definition		
1	NDMC School	25	1	1	-	-	2	50
2	Major traffic junctions	75	-	-	-	1	1	75
3	Major Public Utilities Centres	75	-	-	1	-	1	75
4	Health Institutions	50	-	-	1	-	1	50
5	Bus Q-shelter	200	-	1	-	-	1	200
6	NDMC Market Area	Lump sum	50	-	-		5	50
	Total		**50**	**225**	**125**	**75**		**500**

END OF THE DOCUMENT