RFP No. BSCDCL/14

January 2017

SMART CITY BHOPAL

BHOPAL SMART CITY
DEVELOPMENT CORPORATION LIMITED

REQUEST FOR PROPOSAL

Selection of Master System Integrator for Integrated Command and Control Centre (ICCC) for Smart City Bhopal

Volume II- Scope of Work

Bhopal Smart City Development Corporation Limited (BSCDCL)

Table of contents

1. Introduction		9
1.1	About BSCDCL	9
1.2	Objective of this RFP	9
1.3	Project Vision	9
1.4	Project Objectives:	11
1.3	***Phase wise envisaged activities of ICCC***	12
1.4	Regarding Bhopal City and need of ICCC	14
1.5	Integration Capabilities	22
1.6	Roles and Responsibilities	24
1.7	Current ICT based systems of Bhopal City	25
2	Scope of the Project	32
2.4	Scope of Services	32
2.5	Overview of Scope	32
2.6	Detailed Scope of Work	35
3	Compliance to Standards & Certifications	83
4	Project Management and Governance	85
4.1	Project Management Office (PMO)	85
4.2	Steering Committee	85
4.3	Project Monitoring and Reporting	86
4.4	Risk and Issue management	86
4.5	Staffing requirements	86
4.6	Governance procedures	87
4.7	Planning and Scheduling	87
5.	Change Management & Control	88
5.1	Change Orders / Alterations / Variations	88
5.2	Change Order	88
6.	Annexure I-Functional Requirements	90
6.1	Command and Control Centre Application	90
6.2	Backup / Achieved / Replication Software	114
6.3	EMS (Enterprise Monitoring System)	118
6.4	Software Defined Security (SDS) for Applications /Services	124
6.5	Virtualization Software	124
7.	Annexure II-Technical Specifications	127
7.1	Multi-Function Laser Printer	127

7.2	Laser Printer	127
7.3	Video Wall	128
7.4	Workstations (Desktop Computer)	128
7.5	Television Set (Meeting room)	129
7.6	Projector	129
7.7	IP PABX System	130
7.8	Civil Work, Safety Instrumentation and Furniture (at command center)	131
7.9	DG Set	140
7.10	Server (Application / Database or Other)	142
7.11	Blade Chassis	143
7.12	Storage Specification	144
7.13	Core Switch	146
7.14	Core Router	146
7.15	Internet Router	147
7.16	SAN Switch	147
7.17	Aggregation/ Data center Switches (L3 Manageable)	149
7.18	KVM Module	150
7.19	Purpose Built Backup Appliance (PBBA) Features	151
7.20	Rack with KVM over IP	152
7.21	Load Balancer	153
7.22	Firewall (Internal/ External)	157
7.23	Data Leakage Prevention	158
7.24	Integrated Building management system	162
8.	Annexure III: Common guidelines/ comments regarding the compliance of equipment/ systems	202
9.	Annexure IV: GIS Layers	206
10.	Annexure V- ICCC -Design Consideration	214
10.3	Key Design Considerations	214
10.4	Guiding Architecture Principle	216
10.5	Integration Architecture	223
10.6	Security	229
10.7	Software Development Lifecycle	238
10.8	Quality Assurance & Audit	239

Disclaimer

The information contained in this Request for Proposal document ("**RFP**") or subsequently provided to Applicants, whether verbally or in documentary or any other form by or on behalf of the Bhopal Smart City Development Corporation Limited (BSCDCL) or any of its employees or advisers, is provided to Applicants on the terms and conditions set out in this RFP and such other terms and conditions subject to which such information is provided.

This RFP is not an agreement and is neither an offer nor invitation by the BSCDCL to the prospective Applicants or any other person. The purpose of this RFP is to provide interested parties with information that may be useful to them in the formulation of their Proposals pursuant to this RFP. This RFP includes statements, which reflect various assumptions and assessments arrived at by the BSCDCL in relation to the System Integration. Such assumptions, assessments and statements do not purport to contain all the information that each Applicant may require. This RFP may not be appropriate for all persons, and it is not possible for the BSCDCL, its employees or advisers to consider the objectives, technical expertise and particular needs of each party who reads or uses this RFP. The assumptions, assessments, statements and information contained in this RFP, 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 and information contained in this RFP and obtain independent advice from appropriate sources.

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

The BSCDCL, its employees and advisers 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 or otherwise, including the accuracy, adequacy, correctness, reliability or completeness of the RFP and any assessment, assumption, statement or information contained therein or deemed to form part of this RFP or arising in any way in this Selection Process.

The BSCDCL 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.

The BSCDCL may in its absolute discretion, but without being under any obligation to do so, update, amend or supplement the information, assessment or assumption contained in this RFP.

The issue of this RFP does not imply that the BSCDCL is bound to select an Applicant or to appoint the Selected Applicant, as the case may be, for the BSCDCL reserves the right to reject all or any of the Proposals without assigning any reasons whatsoever.

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

Glossary of Terms

- **'Bhopal Smart City '-** Bhopal Smart City comprising of Smart Governance, City Surveillance, Intelligent Transport Management System, Utility Management System for Electricity and Water, Integrated Control and Command Centre, Smart Network, Building Management System and Data Centre.

- **'Master System Integrator (MSI)'-** Organization (Lead bidder in case of consortium) to be appointed by BSCDCL for implementation and maintenance of Integrated Control and Command Center (ICCC).

- **'Consortium Partner'-** Organization that will work with MSI in consortium for implementation and maintenance of ICCC.

- **'Bidder'-** The MSI and consortium partner (if any).

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.	**BCLL**	Bhopal Link Limited
7.	**BSCDCL**	Bhopal Smart City Development Corporation Limited
8.	**BMC**	Bhopal Municipal Corporation
9.	**CCC**	Command and Control Centre
10.	**ICCC**	Integrated Control and Command Center
11.	**CCTV**	Close Circuit Television
12.	**CERTIN**	Indian Computer Emergency Response Team
13.	**BEB**	Bhopal Electricity Board
14.	**DFMD**	Door Frame Metal Detector
15.	**DHCP**	Dynamic Host Configuration Protocol
16.	**DMS**	Distribution Management System
17.	**DNS**	Domain Name Server
18.	**EMS**	Employee Monitoring System
19.	**ERP**	Enterprise Resource Planning
20.	**ESS**	Employee Self Service
21.	**FMS**	Facility Management Service
22.	**FRS**	Functional Requirement Specification
23.	**GIS**	Geographical Information System
24.	**GOI**	Government of India
25.	**HVAC**	Heating, ventilation and air conditioning
26.	**IBMS**	Integrated Building Management System
27.	**ICT**	Information and Communication Technology
28.	**IED**	Intelligent Electronic Device
29.	**IEEE**	Institute of Electrical and Electronics Engineers
30.	**IT**	Information Technology
31.	**ITMS**	Intelligent Transport Management System
32.	**KPI**	Key Performance indicators
33.	**LDAP**	Lightweight Directory Access Protocol
34.	**LUN**	Logical Unit Number
35.	**MPLS**	Multiprotocol Label Switching
36.	**MSA**	Master Service Agreement
37.	**MSI**	Master System Integrator
38.	**MSI**	Master Service Integrator
39.	**MTBF**	Mean Time Between Failures
40.	**MW**	Mega Watt
41.	**NOC**	Network Operation Centre
42.	**BSCDCL**	Bhopal Smart City Development Corporation Limited
43.	**OEM**	Original Equipment Manufacturer

44.	**OFC**	Optical Fibre Cable
45.	**OWASP**	Open Web Application Security Project
46.	**PABX**	private automatic branch exchange
47.	**RAID**	Redundant Array of Inexpensive Disks
48.	**RTU**	Remote Terminal Unit
49.	**SAN**	Storage Area Network
50.	**SCADA**	Supervisory Control and Data Acquisition
51.	**SDC**	State Data Centre
52.	**SITC**	Supply Installation Testing and Commissioning
53.	**SLA**	Service Level Agreement
54.	**SNMP**	Simple Network Management Protocol
55.	**SRS**	Software Require Specification
56.	**SSL**	Secure Sockets Layer
57.	**STQC**	Standard, Testing and Quality Certification
58.	**UAT**	User Acceptance Testing
59.	**VLAN**	Virtual Local Area Network
60.	**VM**	Virtual Machine
61.	**DMZ**	De- Militarized Zone

1. Introduction

1.1 About BSCDCL

Bhopal is among the first 20 cities selected in first round of smart cities challenge under Government of India's (GoI) smart cities mission (SCM) to implement the smart city proposal (SCP). In this context, Bhopal has incorporated a special purpose vehicle (SPV) – Bhopal Smart City Development Corporation Limited (BSCDCL) (the **"Authority"**) to plan, design, implement, coordinate and monitor the smart city projects in Bhopal. BSCDCL is a company incorporated under Indian Companies Act 2013 with equal shareholding from Madhya Pradesh Urban Development Company Limited (MPUDCL) on behalf of Government of Madhya Pradesh (GoMP) and Bhopal Municipal Corporation (BMC).

1.2 Objective of this RFP

BSCDCL intends to select a Master System Integrator (MSI) 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 date on turnkey basis.

This document contains the following details:

a. Scope of work that will be assigned to the MSI as part of this project
b. Other terms and conditions of the envisaged Smart City by BSCDCL.

This document provides a high-level overview of the technology approach for ICCC and in-depth details of the functional roles of system components, and the interactions between roles, 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 Bhopal Smart City Operations and emergency response. The hosting of all applications and database will be done at in premise data centre and DR will be on cloud based Data Centre. Integrated Building management system will be implemented in the ICCC building for managing and monitoring building utilities, access, security etc.

1.3 Project Vision

To establish an Integrated Control and Command Centre (ICCC) for Bhopal city to run operations for city and citizens using ICT as backbone and seamless integration with all the required & existing ICT systems / Smart components.

Integrated Control and Command Center (ICCC) of Bhopal City 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 department command centers and applications will be collected and analyzed for better planning of the city. ICCC will have BI 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 have an Experience Center which will showcase the smart technologies used for making the command center and city smart. ICCC will also have a situation room, to manage incidents very effectively.

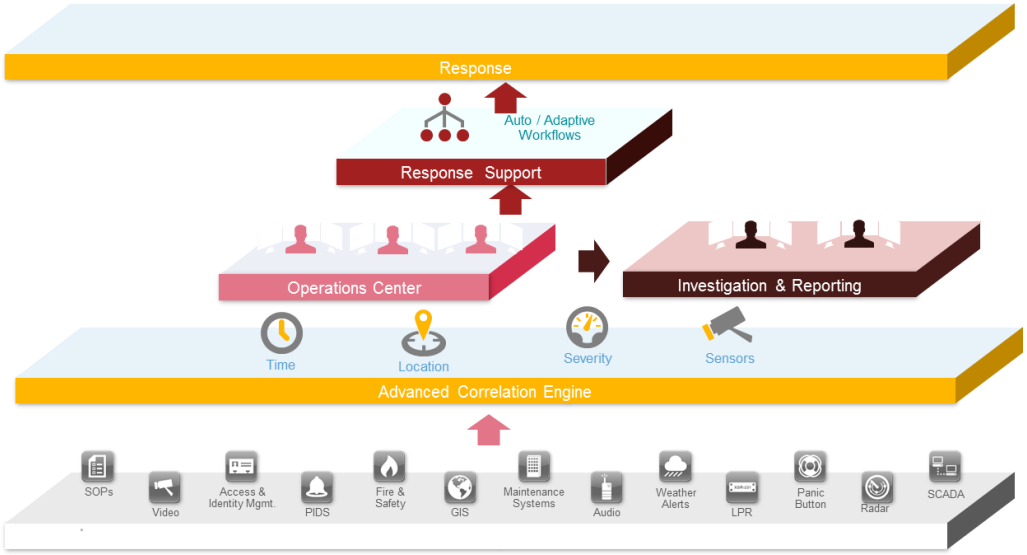
ICCC will have its own data center, co-located with command center and DR to be on cloud.

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 Bhopal City smart and livable for its citizens.

ICCC will manage utilities for ABD area, and in future capable of managing utilities of the entire city.

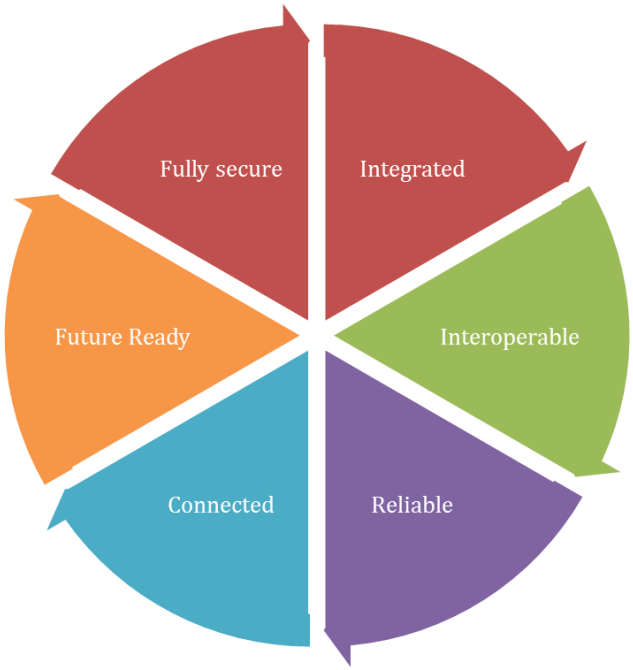


1.4 Project Objectives:

The primary objective of the establishing a command and control centre is to provide better services to citizens with a view to improve the quality of life. The objective of establishing an Integrated Command and Control Center (ICCC) is to implement holistic and integrated solution for multiple (existing and future) IT initiative for Bhopal Smart City Development Corporation Limited (BSCDCL). The IT initiative may of any department for example whether it is safe city (CCTV surveillance) and DIAL 100 of police department, DIAL 108 of health department or network of Municipal Corporation. The end objective of establishing ICCC is to drive the actions by BSCDCL on behalf of all the departments for city operations.

BSCDCL envision the planned ICCC to fulfil following objectives:

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



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

- To provide assistance to citizen at the time of emergencies
- To provide facilities of Ambulance, Police Van, Fire Brigade to the citizens
- To effectively manage Traffic and Roads and support police to maintain Law and Order

- Disaster Management
- Environmental Control/ Pollution Control
- Efficient user of public resources like electricity and water
- Efficient and timely delivery of public services
- Better health and education services

1.5 Phase wise envisaged activities of ICCC

The following activities to be undertaken by the Master System Integrator (MSI)

- 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) with approximately minimum area of 25,000 square feet of floor area. The floor area may be increased if required, but all the facilities and components of ICCC will remain as mentioned below. There will be no additional cost for layout design for more than 25000 square feet floor area. This layout must contain the following:
    - Control and Command Setup
    - Data Center Setup
    - Experience Center
    - Situation Room
    - Office Setup for BSCDCL and MSI
        - At least 5 cabins for BSCDCL officers (with seating capacity of 4 – 5 personal along with BSCDCL officer)
        - At least 3 meeting rooms (with furniture and fixtures)
        - One Conference Room with seating capacity of 20-30 personals (with video conferencing facility, furniture and fixtures)
    - Pantry / Common Area (with adequate capacity)
    - Restroom facilities (separate for Male & Female) with adequate capacity
    - Fire Escape & Evacuation Facilities (ISO 23601)
    - Other facilities which will be required for specially abled people as per guidelines defined by Govt. of India
- Assessment of physical security, housekeeping, waste management requirements for ICCC premises.
- Assessment of IT Infrastructure and Non IT Infrastructure requirements, assessment of business processes, assessment of software requirements, assessment of integration requirement, assessment of connectivity requirement all locations (including buildings).
- Formulation of solution architecture, detailed design of smart city solutions, development of test cases (Unit, System Integration and User Acceptance), SoP documentation.

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

Implementation Phase:

- Physical Setup of ICCC as per the layout agreed with BSCDCL. This includes activities like false flooring, false ceiling, partitions, network cabling, electric fitting, establishment of office spaces, ICCC facility, data center facility, meeting rooms, conference rooms (with video conferencing facility), Inline UPS, DG Set, Auto on-off lighting system 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 MSI
- Housekeeping facility for ICCC.
- 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
- Network connectivity establishment and configuration between ICCC and various other command centers / applications (which are to be integrated with ICCC).
- 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 Incident Management Support 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 BSCDCL or its authorized agency for doing various kinds of Audits as and when required.
- Preventive, repair maintenance and replacement of non ICT components as applicable under the warranty and AMC services during the contract period.
- Network connectivity maintenance between ICCC and various other command centers / applications (which are to be integrated with ICCC).
- Overall maintenance of the ICCC facility and continuity of operations as per SLAs.
- For continuity of operations all cost (Bills) pertaining to power, water, telephone and internet connectivity for ICCC will be paid by the MSI.
- Overall maintenance of housekeeping and physical security at ICCC.
- Provide necessary security to the ICCC premises and its setup during the period of contract.
- Submit Quarterly reports as defined in the RFP.

Exclusions

- Development of basic civil infrastructure of the building for the control and communication center
- Provisioning of network bandwidth for connectivity at various locations to connect with ICCC.
- Provisioning of power and water connection at ICCC location.

1.3 Regarding Bhopal City and need of ICCC

Bhopal is the capital of the Indian state of Madhya Pradesh and the administrative headquarters of Bhopal district and Bhopal division. The city was the capital of the former Bhopal State. Following are the major challenges that are being faced by current capital city:

a. Rapid urbanization
b. Severe pressure on city resources
c. Severe Transportation and Traffic Issues
d. Lack of social inclusion
e. Livability challenges for citizens
f. Environmental sustainability
g. Inefficiency in city operations

Migration towards cities is putting lot of pressure on cities infrastructure resulting in unplanned urbanization. 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 city department makes investments independently, resulting in:

a. Isolation of infrastructure and IT resources
b. No sharing of intelligence and information such as video feeds, data from sensors, etc.
c. Duplication in investment and effort
d. 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:

1. 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.

2. 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.

3. 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.

4. 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, Bhopal Smart City Development Corporation Limited (BSCDCL) has decided to develop state-of-art Integrated Control and Command Centre in Bhopal city which will help to deliver below services as and when required:

i. Integration with Smart Parking
ii. Integration with Public Bike Sharing
iii. Integration with Smart Pole & Smart Lighting
iv. Integration with Solid Waste Mgmt. Services (Tracking of Solid Waste Vehicles)
v. Integration with Intelligent Traffic Management System (Police)
vi. Integration with BMC Call Centre & BMC Services
vii. Integration with Bhopal Smart MAP (GIS)
viii. Integration with Bhopal Plus
ix. Integration with DIAL 100
x. Integration with DIAL 108 & Jannani Express
xi. Integration with Transport Management System (BCLL)
xii. Integration with CCTV Surveillance (Police Dept.)
xiii. Integration with Dynamic Market Place (Mayor Express)
xiv. Integration with Emergency Response and Disaster Mgmt.
xv. Integration with Water Management System
xvi. Integration with Met Department (Local Weather Forecast)
xvii. Integration with Area Based Development (ABD) Services
- Utilities
- Lighting
- Metering
- Surveillance

xviii. Integration with Crowdsourcing Data
xix. Integration with Fire Brigade Control System
xx. Integration with Solar Roof Top
xxi. Any other services implemented in near future during the project period*

*These other services will be additional work and will be taken up as "Change request" following the process defined in Clause 37 and 43 of Vol III of this RFP.

Following is the service wise brief scope of integration for various initiative of Bhopal Smart City:

Sl. No	List of Services	Brief of Scope for Integration
1	Integration of Smart Parking	• ICCC will be required to integrate with the command center of the Smart Parking solution, which is a PAN City initiative. • ICCC will be required to receive feeds on the status of parking across the city which are managed by the Smart Parking command center (feeds received from all the edge devices of the Parking Solution). • These feeds will provide information of available, non-available parking slots, functional and non - functional parking slots. • ICCC will also be required get video feeds from the parking areas on real-time basis. • Such video feeds will only be saved for 7 days. • These video feeds will also help monitor assets of BMC, BSCDCL and BCLL. • All the information received will also be required to be mapped on the GIS map.

		• All the information received from the smart parking command center will also go into the Analytical layer which will help city in better planning and running of operations. • ICCC should also be able to trigger the commands / alerts (if required) to the respective command center. • This initiative is under BMC.
2	Integration of Public Bike Sharing	• ICCC will be required to integrate with the command center of the Public Bike Sharing solution, which is a PAN City initiative. • ICCC will be required to receive feeds on the status of utilization of public bike sharing docks across the city. • These feeds will provide information of available, non-available cycles in slots, functional and non - functional PBS stations. • ICCC will also be required get video feeds from the PBS stations on real-time basis. • Such video feeds will only be saved for 7 days. • These video feeds will also help monitor assets of BMC, BSCDCL and BCLL. • ICCC will also be required to get information regarding the position of the cycles deployed under the PBS project. • All the information received will also be required to be mapped on the GIS map. • All the information received from the PBS command center will also go into the Analytical layer which will help city in better planning and running of operations. • ICCC should also be able to trigger the commands / alerts (if required) to the respective command center. • This initiative is managed by BSCDCL.
3	Integration of Smart Pole & Smart Lighting	• ICCC will be required to integrate with command center of Smart Poles (Pan City Initiative) to receive all kinds of feeds such as environment sensor, lighting sensors. Video, etc. • ICCC will be required to get information on the status of working of the installed LED lights, as well as other sensors and other cameras. • ICCC will also get real-time video feed from the installed Smart Poles. • Such video feeds will only be saved for 7 days. • These video feeds will also help monitor assets of BMC, BSCDCL and BCLL. • All the information received will also be required to be mapped on the GIS map. • All the information received from the Smart Pole command center will also go into the Analytical layer which will help city in better planning and running of operations.

		• ICCC should also be able to trigger the commands / alerts (if required) to the respective command center. • This initiative is managed by BSCDCL.
4	Integration of Solid Waste Mgmt. Services (Tracking of Solid Waste Vehicles)	• ICCC will be required to integrate with the control room of Solid Waste Vehicle tracking project (Pan City Initiative) to receive feeds on the location of the solid waste vehicles. • ICCC will also get other information which is received in the control room like fuel utilization of Vehicles. • All the information received will also be required to be mapped on the GIS map. • All the information received from the command center will also go into the Analytical layer which will help city in better planning and running of operations. • ICCC should also be able to trigger the commands / alerts (if required) to the respective command center. • This initiative is managed by BMC.
5	Integration of Intelligent Traffic Management System (Police)	• ICCC will be required to integrate with Command Center of Traffic Management System, to receive real-time feeds of the camera installed by them. • These video feeds will not be saved, but will be utilized in Analytical layer to help administration monitor its assets and do a better urban planning. • ICCC will also be required to send video feeds received from Smart Parking, Smart Pole, PBS in real-time basis to the command center of Traffic (if required). • ICCC should also be able to trigger the commands / alerts (if required) to the respective command center.
6	Integration of BMC Call Centre & BMC Services	• ICCC will be required to integrate its helpdesk and system with BMC call center, in case if there is some information or notification is to be sent to BMC call center for doing some action in the field regarding Municipal Corporation work. • All the information received from the command center will also go into the Analytical layer which will help city in better planning and running of operations. • ICCC will be required to integrate with the backend system of Bhopal Municipal Corporation services which is SAP based system to monitor the performance of the application. • Along with this ICCC should be able to show the utilization by citizens of various sections of Bhopal Plus application in the form of a Dashboard. • ICCC should be able to integrate with the existing ICT systems and edge / end / mobile devices of various BMC departments such as Garden, General Administration Department, Water Supply, Sewerage, Assessment and Collection (Property Tax, Shops and establishment), Fire

		(Fire Brigade Section), Transport of Heavy Vehicles and Maintenance (Workshop), Audit and License Issue to receive and send information. • ICCC should be able to map the data received from various BMC departments on its GIS Platform. • ICCC will be required to send BMC field agents alerts and notifications for any emergency / incidents / disaster in the city for doing required action. ICCC system should also be able to get acknowledgement from the receivers.
7	Integration with Bhopal Smart MAP (GIS)	• ICCC will be required to use the GIS platform developed by BSCDCL for the city. • There will be a requirement for enhancing the existing platform and using it in the ICCC for doing all the necessary actions. • This is an ESCRI based platform with almost 96 layers. • Along with this ICCC should be able to show the utilization by citizens of various sections of Bhopal Plus application in the form of a Dashboard. • All the information received from the application will also go into the Analytical layer which will help city in better planning and running of operations.
8	Integration with Bhopal Plus	• ICCC will be required to integrate with the backend system of Bhopal Plus to monitor the performance of the application. • Along with this ICCC should be able to show the utilization by citizens of various sections of Bhopal Plus application in the form of a Dashboard. • All the information received from the application will also go into the Analytical layer which will help city in better planning and running of operations.
9	Integration with DIAL 100	• ICCC will be required to integrate with the command center of DIAL 100, which is a public safety initiative by Police Department. ICCC will be required to get information regarding the location and other details of DAIL 100 vehicles present in Bhopal area. • Such information will be useful in case of incident / disaster management for the city. • All the information received from the command center will also go into the Analytical layer which will help city in better planning and running of operations. • ICCC should also be able to trigger the commands / alerts (if required) to the respective command center. • ICCC will be required to integrate to send the alerts and notifications for any emergency / incidents / disaster in the city for doing required action.

10	Integration with DIAL 108 & Jannani Express	• ICCC will be required to integrate with the command center of DIAL 108 and Jannani Express, which is a public health initiative by Health Department. ICCC will be required to get information regarding the location and other details of DAIL 108 & Jannani Express vehicles present in Bhopal area. • Such information will be useful in case of emergency / incident / disaster management for the city. • All the information received from the command center will also go into the Analytical layer which will help city in better planning and running of operations. • ICCC should also be able to trigger the commands / alerts (if required) to the respective command center. • ICCC will be required to integrate to send the alerts and notifications for any emergency / incidents / disaster in the city for doing required action.
11	Integration with Transport Management System (BCLL)	• ICCC will be required to integrate with command center of BCLL to get all kinds of feeds from Transport Management System. • These feeds will be sensor based feeds on location of public transport vehicles, bus station information operations, etc. • All the information received from the command center will also go into the Analytical layer which will help city in better planning and running of operations. • ICCC should also be able to trigger the commands / alerts (if required) to the respective command center.
12	Integration with CCTV Surveillance (Police Dep't.)	• ICCC will be required to integrate with Command Center of CCTV System, to receive real-time feeds of the camera installed by them. • These video feeds will not be saved, but will be utilized in Analytical layer to help administration monitor its assets and do a better urban planning. • ICCC will also be required to send video feeds received from Smart Parking, Smart Pole, PBS in real-time basis to the command center of Police (if required). • ICCC should also be able to trigger the commands / alerts (if required) to the respective command center.
13	Integration with Dynamic Market Place (Mayor Express)	• ICCC will be required to integrate with the backend system of Dynamic Market Place (Mayor Express) to monitor the performance of the application. • Along with this ICCC should be able to show the utilization by citizens of various sections of Dynamic Market Place application in the form of a Dashboard. • All the information received from the application will also go into the Analytical layer which will help city in better planning and running of operations. • This is BMC initiative.
14	Integration with Emergency Response and Disaster Mgmt.	• ICCC will be required to integrate with existing ICT system of the Emergency Response and Disaster Management to send them alerts and notifications for any emergency / incidents / disaster in the city for doing required action. • ICCC system should also be able to get acknowledgement from the receivers.

		• All the information received from the application will also go into the Analytical layer which will help city in better planning and running of operations.
15	Integration with Water Management System	• ICCC will be required to integrate Water Management System control room to get all kinds of sensor and edge devices feeds. • ICCC should be able to map this information on the GIS layer and help authority monitor the water management of the city. • ICCC should also be able to trigger the commands / alerts (if required) to the respective command center. • All the information received from the application will also go into the Analytical layer which will help city in better planning and running of operations.
16	Integration with Met Department (Local Weather Forecast)	• ICCC should be able to receive real-time data on the weather forecast from Met Department and map the same on its platform as well as GIS layer. • All the information received from the application will also go into the Analytical layer which will help city in better planning and running of operations. • This information will also help in predictive analysis for urban planning based on weather forecast.
17	Integration with Area Based Development (ABD) Services: i. Utilities ii. Lighting iii. Metering iv. Surveillance	• ICCC will be required to integrate with control rooms / systems all the listed services of the Area Based development (ABD). • These services are planned for the near future. • ICCC will be required to get all kinds of feeds from all the sensors / edge devices installed for these services in the field. • In case of video feeds, feeds will only be saved for only 7 days. • ICCC will be required to monitor these services in real-time and manage the operations of these services. • All the information received from the application will also go into the Analytical layer which will help city in better planning and running of operations. • This information will also help in predictive analysis.
18	Integration of Crowdsourcing Data with ICCC	MSI has to make provision in the ICCC for receiving the data from crowdsourcing and perform standard operation at ICCC. It is planned to collect data as part of future IT initiative under which citizen of Bhopal would be sharing data. Received data would be part of existing data repository where data is received from various type of sensors owned by Bhopal smart City. All the operations like data analytics will be performed on the received data through crowdsourcing too. Connectivity between end devices and ICCC will be provided by BSCDCL. For example, in near future if any resident welfare society intends to share data with BSCDCL (ICCC) for surveillance purpose, this video feed would be received at ICCC and become part of other feeds coming from various CCTV camera installed in the city by BSCDCL.

19	Integration with Fire Brigade Control System	Fire brigade section is the part of Bhopal Municipal Corporation. There are 18 fire brigade vehicles and 15 motor bikes are available to cater to whole city. BMC has plans to strengthen and upgrade the fire brigade control system of the city. MSI has to integrate the city fire brigade control system with ICCC. This will help BMC in efficient usage of its resources and to achieve minimum response time in case of rescue operations. For example: If the ICCC receives information about fire in the city, the ICCC should able to trigger a command to appropriate fire station and its vehicle which can reach within minimum time with guidance about traffic conditions and shortest route.
20	Integration with Solar Roof Top Project	• ICCC will be required to integrate the energy management system of solar roof top project to get all kinds of sensor and edge devices feeds. • ICCC should be able to map this information on the GIS layer and help authority monitor the energy management system of the city. • ICCC should also be able to trigger the commands / alerts (if required) to the respective stakeholders. • All the information received from the application will also go into the Analytical layer which will help city in better planning and running of operations.

1.4 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) Sample Use Cases describing the need of integrated systems:

- *Urban Flooding Scenario:* The water level sensors (used for flood detection on streets) will send the ambient water levels accumulated on the street to the ICCC through the available connectivity. The ICCC shall baseline the existing water level and rainfall prediction with erstwhile flood levels to generate an alert for flooding. This alert will then be passed over to the citizens through the variable messaging displays and public address system to warn them of possible flooding in a locality.
- *Evacuating Hazardous places in event of fire:* As soon as the Command Center is intimated of a fire through any of the available channels, Fire tenders shall be dispatched to the location along with guidance for shortest path to the accident site. Event trigger shall be also sent to nearest Police Station & nearby hospitals. IP based public address system will be triggered to vacate the nearby fuel stations (if there is any) to reduce the extent of casualty. Information will be passed over to trauma centres in the vicinity to prepare for increased number of emergency care patients.

1.5 Roles and Responsibilities

Phase	MSI	BSCDCL	Other Departments
Pre – Implementation	• Adhere to defined SLAs and timelines • Define Project Implementation Plan • Conducting site survey, obtaining necessary permissions, developing system requirements, standard operating procedures etc. • Providing physical layout of the ICCC (with 3D simulation) • Assessment of IT Infrastructure and Non IT Infrastructure requirements, assessment of business processes, assessment of software requirements, assessment of integration requirement, assessment of connectivity requirement all locations (including buildings). • Formulation of solution architecture, detailed design of smart city solutions, development of test cases (Unit, System Integration and User Acceptance), SoP documentation • MSI will define the formats for data exchange between various services and systems in agreement with BSCDCL.	• Provide necessary information to MSI for doing surveys • Facilitate Interaction with other Departments for getting the required integration • Help MSI get necessary approvals for implementing ICCC. • Help MSI finalize the protocols for data exchange between ICCC and various other systems. • Review the documents submitted by MSI and provide feedback	• Provide necessary information to MSI for doing future integrations. • Provide necessary information to MSI for finalizing the data exchange between the systems.
Implementation	• Adhere to defined SLAs and timelines • Physical Setup of ICCC as per the layout agreed with BSCDCL. • Helpdesk setup, procurement of equipment, edge devices, COTS software (if any), licenses. • Physical Security and Housekeeping setup • IT and Non IT Infrastructure installation, development, testing and production environment setup • Safety and security of IT and Non IT Infrastructure • Establishment and configuration of Network Connectivity (provided by service provider) as per service level between ICCC and various other command centers / applications for integration. • Software Application customization (if any), development of bespoke solution (if any), data migration, integration with third party services/application (if any) • User Manuals , training curriculum and training materials • Role based training(s) • SoP implementation, Integration with	• Provide building structure for setting up ICCC (based on agreed plan) • Provide necessary Electricity and Water Connection to the ICCC facility. • Provide necessary network connectivity as per the desired requirements between ICCC and other systems for integration • Facilitate Interactions with other Departments for getting the required integration. • Help MSI get necessary approvals for implementing ICCC. • Review the documents submitted by MSI and provide feedback. • Provide manpower for getting trained on ICCC operations	• Provide necessary access to the current ICT setup for integration with ICCC.

	GIS Platform, Integration of solutions with Command and Control Centre • Facilitating UAT 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		
Post – Implementation	• Deploying manpower • Security of ICCC premises • Annual technical support • Preventive, repair maintenance and replacement of hardware and software components • Provide a centralized Helpdesk and Incident Management Support 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 required access and information for Audits • Preventive, repair maintenance and replacement of non ICT components • Overall maintenance of the ICCC facility and continuity of operations as per SLAs. • Monitoring of Network Connectivity (provided by service provider) as per service level and report the non-compliance. • Submit Quarterly Reports • Adhere to defined SLAs • Payment of utilities bills during the operations period (like electricity, telephone, internet, water, etc.)	• Facilitate Interactions with other Departments for getting the required integration. • Help MSI get necessary feeds for ICCC. • Help MSI get necessary approvals (if any). • Review the documents submitted by MSI and provide feedback • In case of any incident or disaster facilitate communication from ICCC to field agents (in case of absence of ICT setup with field agents)	• Provide and receive (if applicable) data feeds to/ from ICCC to their current ICT setup in the predefined formats. • Perform needful action in case of any incident or disaster

1.6 Current ICT based systems of Bhopal City

There are various state of the art IT systems/initiatives already deployed in the city or being deployed. Following are the few important IT systems of the city and their features. BSCDCL envisages to integrate these IT systems with command and control center of smart city Bhopal.

1.6.1 Smart Parking

The objective of Smart Parking is to better manage the parking areas of the city and provide seamless information to users of parking slots. Smart Parking is a pan city initiative for all the parking areas which falls under purview of BMC and managed by BMC. Under this minimum 60 parking areas will be managed. Minimum 6500 two wheelers and 3500 four wheelers parking slots will be managed under smart parking project. There will be a sensor based smart parking solution, one sensor for each parking

slot which will help in better manage and knowing the status of parking slot and subsequently provide parking availability status to end users.

1.6.2 Public Bike Sharing

Public bike sharing system is a service in which bikes will be made available to the citizens of Bhopal city on shared basis. Public bike sharing project will allow citizens to borrow a bike from one point and return it at another point. Following are the main features of public bike sharing system:

a. There will be 50 Stations, 500 smart Bicycles across the city with onboard computer and GPS
b. Fare Collection device on each smart bicycle – using NFC, Smart Card and Pin Code
c. The central control system collects data from each station for efficient planning and operation of the system.
d. This data is used to make decisions on redistribution of cycles around stations during the hours of operations.
e. The Cycle sharing system is also being integrated with the fare collection system of the BRT system to aid the multimodal integration.

1.6.3 Smart Pole

The smart Pole or intelligent pole project envisage installation of 400 poles across the city. Each smart pole will be equipped with multiple utilities like CCTV cameras, environmental sensors, Wi-Fi services, Smart LED Lights. Following are the key features of this project:

a. Converting 20000 traditional street lights to LED based intelligent lights
b. 400 Smart poles with capability to accommodate multi operator telecom Base Stations for 2G/3G/LTE to reduce mobile call drops
c. 400 Surveillance cameras inbuilt into smart poles
d. Wi-Fi hotspots - 100
e. Interactive Digital Signage for traffic & business - 400
f. Environment sensors – 100
g. 48 core , 200 km of citywide Optical Fiber Cable network to enable connected communities
h. Network/cloud controlled EV Charging at 100 poles
i. State of the art control and command center (for smart poles) for the O&M of services for 15 years

1.6.4 Solid Waste Management Services

Principally Solid Waste Management refers to control of generation, storage, collection, transport or transfer, processing and disposal of solid waste materials in a way that best addresses the range of public health, conservation, economics, aesthetic, engineering and other environmental considerations. Under this project all the vehicles involved in collection of solid waste are being tracked. Following are the key attributes of this project:

a. Installation of GPS devices on all the vehicles, RFID Tags, RFID Readers.
b. GPS Based Application software (Vehicle Tracking System) integrated with GPS, RFID devices
c. GPS/GPRS System, RFID, fuel sensors for all vehicles. Minimum number of vehicles is 300 (232 current).

d. Cloud based data center
e. Infrastructure including Server and Control center (with video wall). Software with MIS reports.
f. Provision for alerts to the Central Command center on Scheduled Missed Trips, over speeding vehicles, unauthorized stoppage and /or non-stoppage of the vehicles at designated bins & route deviation by vehicles etc.

1.6.5 Intelligent Transport Management System

"Intelligent Traffic Management System (ITMS) includes setting up Automatic Number Plate Recognition (ANPR) system, Red Light Violation Detection (RLVD) Cameras with E-Challan System at specified locations of Bhopal City. Following are the key features of ITMS system.

a. All buses equipped with GPS based Automatic Vehicle Location System (AVLS) connected with Central Control and Command Center (of ITMS).
b. Real time tracking and monitoring of Bus Operations.
c. 16 Ft X 6 Ft Video Wall comprising of 08 Nos. of High Resolution LED Panels at Control room.
d. Bus Stops are connected with Command Center reflecting Expected Time of Arrival (ETA) on Passenger Information System (PIS)
e. All the buses are equipped with 04 Nos. of PIS in buses and PAS in buses. .
f. Signal Priority for BRTS buses
g. Automatic Fare Collection
h. Number of Bus Stops – 100
i. Number of Buses – 225 (in future 300)
j. Real time tracking and monitoring of bus operations
k. Bus stops are connected with command center

1.6.6 BMC Call Center

BMC call center is a public grievances redressal system related to municipal services. All the issues /complains related to municipal services are addressed by BMC call center. Citizen of Bhopal city residing in Bhopal municipal area can call the call center and register their complaints. In future BMC call center will also be used as one of the channels for taking request for dynamic market place.

1.6.7 Bhopal Smart Map (GIS)

Smart Map is a web-GIS portal developing as part of Bhopal Smart City Project, a web-based application addresses issues affecting urban areas, through GIS based plans adopting smart city concept. GIS provides an effective and efficient way to handle infrastructure and asset related data and its associated attribute information from multiple sources for better decision support, improved governance and to deliver better citizen services. It aims to facilitate the citizens of Bhopal with various services. The portal allows the public to easily discover and search for geospatial and textual data, though modules like know your ward. It enables users to view multiple data layers on a map and perform various functions for data analysis like search and

query. The advanced search and query tools enables users to search for specified features like Landmarks, Heritage sites, Museum etc., based on the map layers.

a. 96 layered GIS cutting across departments.
b. Citizen portal - Map visualization module, Query module, and location based information module, education, health services, public feedback, transport, cultural and community events.
c. Property and other taxes.
d. Heritage

1.6.8 Bhopal Plus (App)

Bhopal Plus is a mobile application. It is an integrated platform enabling and promoting "Collaborative Participatory Governance, Centralized Citizen Service Delivery, Live City Feeds, Citizen Grievance Redressal, etc. The goal of the platform is to make citizen engagement an integral part of policy planning and implementation.

Following are the key features of Bhopal Plus:

a. Citizen Collaboration platform
b. Citizen Services (G2C & B2C)
c. Smart city dashboard
d. Grievance Redressal
e. Integration with external apps (Dynamic market place, women safety application, etc.)

1.6.9 BMC Municipal Services

These are pan city citizen services, which are hosted using SAP based web application and they are also hosted on Bhopal plus mobile application, these services include:

a. Water Tax;
b. Property Tax;
c. Birth Registration;
d. Death Registration;
e. Marriage Registration; etc.

There are some more services of various BMC departments such as Water Supply, Sewerage, Assessment and Collection (Property Tax, Shops and establishment), Fire Protection (Fire Brigade Section.

1.6.10 Water Management System

BMC manages the water supply system of the city, which was previously dependent on two sources viz., the Kolar dam which supplies 155 MLD to southern, eastern and central parts of the city and the Upper Lake with 105.75 MLD supplies central and northern parts of the city. These two sources are rain fed and hence, were susceptible to seasonal variations. In addition to these there are 1104 tube-wells accounting to approximately 50 MLD supply supplemented through Ground water.

Under water management system of the city it is planned to use supervisory control and data acquisition system. Under this project approximately 3 lakh edge devices would be connected through data acquisitions system in whole city.

Advantages of SCADA System:

The entire water supply and distribution system shall be upgraded to control from the remote station. SCADA system will enable the authority to monitor the system on real time basis and will also help the authority to see the functioning of individual plant as well as to change / correct the working set points at the plant locations.

The SCADA shall transfer the water distribution network data in real time to the Water Supply Information Management System (WIMS) to enable real time analysis of the distribution system.

Following are the features of WIMS

a. Installation of measuring devices spread over the city for automatic data transfer, at a central location having network facility with main server of the administrative system of the utility.
b. The main role of WIMS will be to gather, analyze and present data from various software packages and will provide a data connectivity link that will enable the operations engineers to make informed decisions on improving the operating efficiently of the network.
c. Use of the software will enable authorities to make informed decisions on operating strategies, to improve the level of service and equability of supplies in all the areas.

d. A tool to compare billing information with actual flow in each zone.

e. Reliable information to improve the capacity and operating strategy of the network to distribute the available supplies. The basis or planning future capacity strengthening and modeling towards 24-hour continuity of supplies.

1.6.11 DIAL 100

DIAL 100 is an emergency response system of police department. Madhya Pradesh police has set up a state level centralized dial 100 control room cum command center in Bhopal for police related emergencies and other services to help people in distress. The proposed center is be equipped with latest technological tools like GIS MAP for whole state, CAD (Computer aided dispatch) and GPS enabled 1000 first response vehicles to attend to handle public distress calls for services. At present approximately 100 vehicles are deployed in Bhopal City. Police personnel are equipped with wireless Radios, CUG GSM connectivity and other model gadgets. As soon as a person makes a call on “100” number, it is received at the center by well trained staff who will take necessary person details, incident details, and location details. Besides computer systems will also validate at the same on the basis of CLI database, GIS MAP, Vehicle database, and other information available in public domain. The trained dispatcher immediately dispatches nearest available one or more well equipped first response vehicle. Each vehicle is monitored and tracked through the GPS based AVLS equipment fitted in the vehicle.

1.6.12 DIAL 108

It is and emergency medical services where citizens can call the ambulance during emergency. This medical ambulances are running across the State of M.P. and is also popularly known as "108 Ambulance Service". This Emergency Medical Ambulance Services, with a fleet of 554 Basic Life Support (BLS) Ambulances and 50 Advance Life Support (ALS) Ambulances deployed strategically across the State of Madhya Pradesh supported with a fully functional centralized call center situated near TB Hospital, Idgah Hills, Bhopal which is receiving more than 25000 calls per day and handling

approx. 2500 emergencies on daily basis. GPS with Biometric System has been installed in ambulances. There are around 200 ambulances are operational in Bhopal city.

Objectives:

To provide round the clock pre-hospital emergency transportation care (ambulance) services across the state. Improve the access to Medical & Health care, police and fire service, particularly attending emergency situations relating to pregnant women, neonates, parents of neonates, infant and children in situations of serious ill health and all other emergencies in the general population: and thereby assist the state to achieve the critical Millennium Development goals in the health sector, i.e. reduction of infant mortality rate, and maternal mortality rate, and in general reduce the vulnerability of the people by providing access to Emergency Response Services.

1.6.13 Traffic Management System

Traffic police of MP at present issues spot challans and court challans manually in the form of hand written hard copy format for violations of various traffic rules in force in Bhopal. The data of prosecution for traffic violations with various combinations for report generation and monitoring is fed manually and maintained in various formats for the purpose of traffic management.

With Traffic Management System MP Police intends to procure the RLVD and e-Challan system under this Project for management of traffic violations in near real time, data maintenance, generation of prosecution reports and to prosecute repeat violators for appropriate punishment as provided in Motor Vehicle Act. The purpose of this project is to ensure that all traffic violations are recorded in real time and stolen vehicles are tracked and legally prosecuted accordingly.

1.6.14 Safe City Cameras Feed

This project has an objective to implement holistic and integrated video surveillance system which includes Command and Control center, Video Management Software and Video Analytics for fifty cities of the state of Madhya Pradesh. Under this city at present 650 CCTV cameras are and 100 ANPR Cameras (Automatic Number Plate Recognition) installed at 135 locations (approximate) In Bhopal city. The key advantages of this project are:

- To provide assistance to citizen at the time of emergency
- To effectively manage Road Traffic
- To make use of technology for traffic challan
- Support police to maintain Law and Order
- To help in investigation of crime
- Help in preventing, detecting and dealing with criminal activities with minimum turnaround time
- Provide alerts and video analytics for counter terrorism
- Monitoring of suspicious people, vehicles, objects etc. with respect to protecting life and property and maintaining law and order in the city
- Continuous monitoring of some important locations/ public places in city area like area near to railway station, airport and other public places for keeping eye on regular activities & for emergency support

1.6.15 Dynamic Market Place (Mayor Express)

Dynamic Market Place is e-Market place providing various kinds of services to citizens. The services includes: Electrician, Plumber, Carpenter, Mason, Driver, Gardener, Painter, Accountant, Air Conditioner Servicing, Baby Sitter, Beautician, Car Cleaner, Cook, Dish Washer,

Domestic Maid, House Cleaning, Pest Control, Photographer, etc. The objective of this project is to provide an operational platform for the dynamic market place which will be integrated with BMC Call Center and Bhopal+ Application at the front end.

1.6.16 Crowdsourcing of Data

It is planned to collect data as part of future IT initiative under which citizen of Bhopal would be sharing data. Received data would be part of existing data repository where data is received from various type of sensors owned by Bhopal smart City. All the operations like data analytics will be performed on the received data through crowdsourcing too. Connectivity between end devices and ICCC will be provided by BSCDCL. For example, in near future if any resident welfare society intends to share data with BSCDCL (ICCC) for surveillance purpose, this video feed would be received at ICCC and become part of other feeds coming from various CCTV camera installed in the city by BSCDCL.

1.6.17 Fire Brigade Control System

Fire brigade section is the part of Bhopal Municipal Corporation. There are 18 fire brigade vehicles and 15 motor bikes are available to cater to whole city. BMC has plans to strengthen and upgrade the fire brigade control system of the city. MSI has to integrate the city fire brigade control system with ICCC. This will help BMC in efficient usage of its resources and to achieve minimum response time in case of rescue operations.
For example: If the ICCC receives information about fire in the city, the ICCC should able to trigger a command to appropriate fire station and its vehicle which can reach within minimum time with guidance about traffic conditions and shortest route.

1.6.18 Solar Roof Top

India is endowed with vast solar energy potential. From an energy security perspective, solar is the most secure of all sources, since it is abundantly available. Theoretically, a small fraction of the total incident solar energy (if captured effectively) can meet the entire country's power requirements. It is also clear that given the large proportion of poor and energy un-served population in the country, every effort needs to be made to exploit the relatively abundant sources of energy available to the country. While, today, domestic coal based power generation is the cheapest electricity source, future scenarios suggest that this could well change.
The broad aim of this project is to develop and deploy new and renewable energy for supplementing the energy requirements of the city. Remote monitoring systems of all the solar roof top installed on Govt. of Private buildings will be monitored through ICCC. This will result in better planning and running the operations from energy management perspective.

2 Scope of the Project

2.1 Scope of Services

MSI (along with its consortium partner) will be responsible to implement and maintain the Integrated Control and Command Centre (ICCC) for Bhopal 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 5 year period, the contract can be extended, at discretion of BSCDCL, for additional five years on yearly basis or part thereof on terms and conditions that may be mutually agreed to.

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

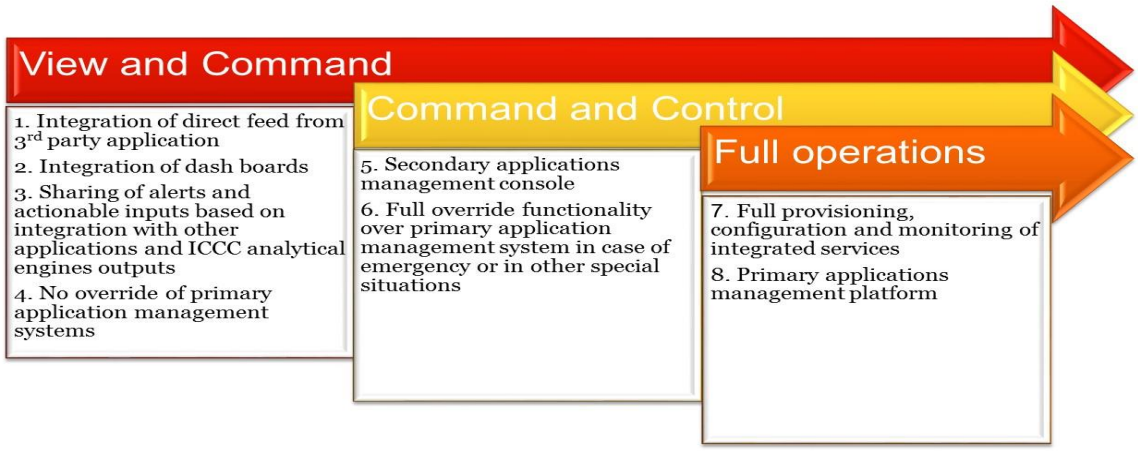
Integration of various services pertaining to IT projects (DIAL 100, Smart Parking etc.) of Bhopal city is a key component of scope of work of MSI. For all the services which belongs to other department (other than BMC) like DIAL 100- Police Department or DAIL 108- Health Department etc., providing the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

If the MSI has conceptualized and created an experience centre using latest technologies with respect to Smart City Applications perspective for demonstration of practical scenarios, officials of BSCDCL would like to visit the bidder's premises to understand and evaluate the technical capability of the bidder in respect to establishing a command and control system.

2.2 Overview of Scope

The snapshot of scope is as below:

1. The MSI will conduct a detailed assessment and design a comprehensive technical architecture and project plan including:
    a. 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. MSI will design, customize, supply, implement and maintain the ICCC software platform with integration with three types of smart city components. These components can be classified on the basis of their respective functions:



A. Command and View:

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

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

B. Command and Control:

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

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

i. Smart Parking
ii. Public Bike Sharing
iii. Smart Pole & Smart Lighting
iv. Solid Waste Management Services
v. Intelligent Transport Management System
vi. BMC Call Centre & BMC Services
vii. Bhopal Smart MAP (GIS)
viii. Bhopal Plus (App)
ix. Water Management System
x. Dynamic Market Place (Mayor Express)
xi. Crowdsourcing Data
xii. Fire Brigade Control System
xiii. Solar Roof Top

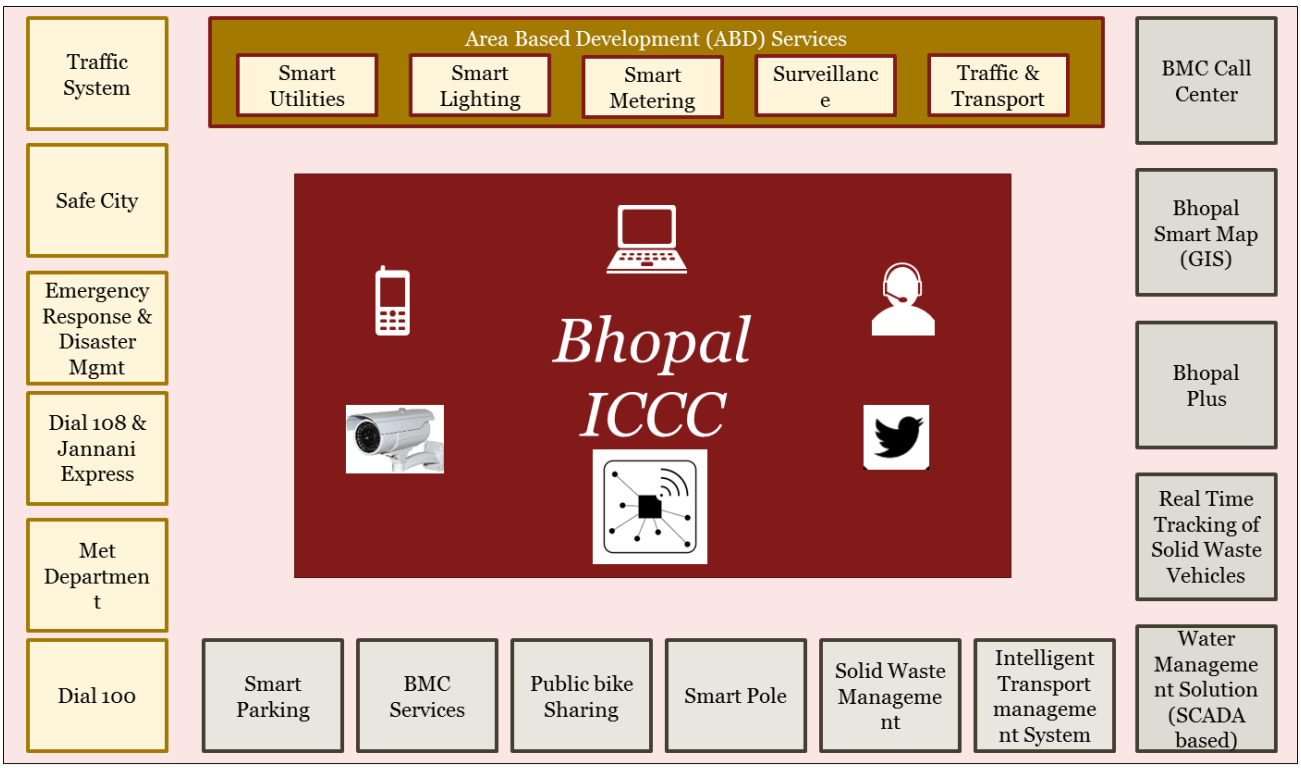
C. Full Operations:

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

i. Utilities
ii. Lighting

iii. Metering
iv. Surveillance

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



D. MSI 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.

E. MSI 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

F. MSI will design, supply, install and commission the network and backbone connectivity for ICCC.

G. MSI will supply, install and maintain Infrastructure including Hardware and Application Software at ICCC.

H. MSI will supply, install and maintain Infrastructure including ICT and non- ICT components at ICCC.

I. MSI 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.

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

   a. Technical and operational support of the system

   b. Maintenance of the IT and Non-IT Infrastructure

   c. Technical & Operational Manpower for smooth running of the system

   d. This help desk will also act as a functional call center to send instructions to various field agencies to do the needful.

K. MSI will provide the design and area specific requirement for the Physical building for the ICCC. MSI must appoint Civil Architect and Interior designer for doing a designing and defining the requirements for ICCC (with minimum area of 25,000 sq. feet).

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

M. MSI should present design of the ICCC using 3D modelling, which can be refined and present the final view of the actual ICCC (with minimum area of 25,000 sq. feet).

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

   a. Access control system

   b. Surveillance System

   c. Physical security system

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

2.3 Detailed Scope of Work

2.3.1 Preparation of detailed technical architecture and project plan

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

   a. Project Charter, Project concept understanding

   b. Names of the Project Team members, their roles & responsibilities

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

d. Co-Location plan for identified services in agreement with relevant stakeholders like BSCDCL, BMC, BCLL 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. Plan for the next week
   iv. Proposed revision to planned schedule provided such revision is necessitated by reasons beyond the control of MSI
   v. Support needed
   vi. Highlights/lowlights
   vii. Issues/Concerns
   viii. Risks/Show stoppers along with mitigation

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

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

2.3.1.1 Requirement Gathering Stage

The MSI 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, MSI shall develop & finalize the System Requirement Specifications

(SRS) in consultation with BSCDCL and its representatives. While doing so, MSI at least is expected to do following:

a. MSI shall study and revalidate the requirements given in the RFP with BSCDCL and submit as an exhaustive FRS document.
b. MSI shall translate all the requirements as captured in the FRS document into SRS.
c. MSI shall develop and follow standardized template for requirements capturing and system documentation.
d. MSI must maintain traceability matrix from SRS stage for the entire implementation.
e. MSI must get the sign off from user groups formed by BSCDCL.
f. For all the discussion with BSCDCL team, MSI shall be required to be present at BSCDCL office with the requisite team members.
g. BSCDCL 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. MSI will prepare interoperability traceability matrix with third party systems (existing legacy systems with ICCC) in consultation with BSCDCL 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 MSI shall design and build the solution for ICCC as per the Design Considerations detailed in **Annexure – V**. The solution proposed by MSI should comply with the design considerations requirements as mentioned therein.

2.3.1.3 Development Phase

The MSI 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 MSI 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 Bhopal city and explicitly mention the same in the technical proposal. The implementation of the application software will follow the procedure mentioned below:

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

i. MSI shall be responsible for supplying the application and licenses of related software products and installing the same so as to meet ICCC requirements.
ii. MSI shall have provision for procurement of licenses in a staggered manner as per the actual requirement of the project.
iii. The MSI shall perform periodic audits to measure license compliance against the number of valid End User software licenses consistent with the terms and conditions of license agreements, volume purchase agreements, and other mutually agreed upon licensed software terms and conditions. The MSI shall report any exceptions to license terms and conditions at the right time to BSCDCL. However, the responsibility of license compliance solely lies with the MSI. Any financial penalty

imposed on BSCDCL during the contract period due to license non-compliance shall be borne by MSI.

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

- Software & licenses.
- Supply tools, accessories, documentation and provide a list of the same. Tools and accessories shall be part of the solution.
- **System Documentation**: System Documentation both in hard copy and soft copy to be supplied along with licenses, document updates and shall include but not limited to following:
    - Functional Requirement Specification (FRS)
    - High level design of whole system
    - Low Level design for whole system / Module design level
    - System Requirements Specifications (SRS)
    - Any other explanatory notes about system
    - Traceability matrix
    - Technical and product related manuals
    - Installation guides
    - User manuals
    - System administrator manuals
    - Toolkit guides and troubleshooting guides
    - Other documents as prescribed by BSCDCL
    - Quality assurance procedures
    - Change management histories
    - Version control data
    - SOPs, procedures, policies, processes, etc. developed for BSCDCL
    - Programs:
        - Entire source codes
        - All programs must have explanatory notes for understanding
        - Version control mechanism
        - All old versions to be maintained
    - Test Environment:
        - Detailed Test methodology document
        - Module level testing
        - Interoperability Testing
        - Overall System Testing

- Acceptance test cases

- The above mentioned documents are required to be updated and to be maintained updated during entire project duration. The entire documentation will be the property of BSCDCL.

b. Bespoke (Custom Developments)

i. The successful MSI shall identify, design and develop the customization for components/functionalities that are required to address the requirements mentioned in this RFP.

ii. The MSI shall supply the following documents along with the developed components:

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

2.3.1.4 Integration & Testing Phase

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

i. Integration with Smart Parking
ii. Integration with Public Bike Sharing
iii. Integration with Smart Pole & Smart Lighting
iv. Integration with Solid Waste Mgmt. Services (Tracking of Solid Waste Vehicles)
v. Integration with Intelligent Traffic Management System (Police)
vi. Integration with BMC Call Centre & BMC Services
vii. Integration with Bhopal Smart MAP (GIS)
viii. Integration with Bhopal Plus
ix. Integration with DIAL 100
x. Integration with DIAL 108 & Jannani Express
xi. Integration with Transport Management System (BCLL)
xii. Integration with CCTV Surveillance (Police Deptt.)
xiii. Integration with Dynamic Market Place (Mayor Express)
xiv. Integration with Emergency Response and Disaster Mgmt.
xv. Integration with Water Management System
xvi. Integration with Met Department (Local Weather Forecast)
xvii. Integration with Area Based Development (ABD) Services
    - Utilities
    - Lighting
    - Metering

- Surveillance

xviii. Integration with Crowdsourcing Data
xix. Integration with Fire Brigade Control System
xx. Integration with Solar Roof Top System
xxi. Any other services implemented in near future during the project period*

*These other services will be additional work and will be taken up as "Change request" following the process defined in Clause 37 and 43 of Vol III of this RFP.

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

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

The MSI shall provide the testing strategy including traceability matrix, test cases and shall conduct the testing of various components of the software developed/customized and the solution as a whole. The testing should be comprehensive and should be done at each stage of development and implementation.

The detailed testing requirements are mentioned in subsequent section.

2.3.1.5 Integration of Future IT initiatives

The software solution should be scalable and modular in structure and should be able to integrate other future IT initiative of Bhopal 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.

2.3.1.6 Go-Live Preparedness and Go-Live

a. MSI shall prepare and agree with BSCDCL, the detailed plan for Go-Live which should be in-line with BSCDCL's implementation plan as mentioned in RFP.
b. As per clause 2.6.20 Go-Live for ICCC will be considered when the identified 10 services are integrated, tested, and operational from ICCC.
c. The MSI shall define and agree with BSCDCL, the criteria for Go-Live.
d. The MSI shall ensure that all the system integration is done with existing systems of agreed 10 services.
e. MSI shall submit signed-off UAT report (issue closure report) ensuring all issues raised during UAT are being resolved prior to Go-Live.

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

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

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

The MSI shall be responsible for procurement, supply and installation of entire ICT hardware and software infrastructure at the Command and Control Centre for successful operations of the systems. The Primary Data Centre will be in premise data centre and DR will be on cloud. 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. MSI will not procure Infrastructure including Hardware, COTS Software licenses and other system software etc. at the start of the project, but will procure after discussion and receipt of go ahead from BSCDCL.

d. MSI shall optimize procurement of ICT infrastructure i.e. the equipment shall not be procured earlier than its requirement.

e. Virtualization technologies to be used to reduce the physical space required for hosting

f. ICT infra deployed for ICCC should be dedicated for the project and MSI shall not use the same for any other purpose.

g. The ownership of ICT infrastructure shall get transferred to BSCDCL after "Acceptance and Go Live" of such items by BSCDCL/ appointed TPAs.

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

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

a. Design, Supply, Installation and Commissioning of IT Infrastructure including site preparation of ICCC.

b. Establishment of LAN and WAN connectivity at ICCC, and connectivity of individual Command 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

- Physical Access to the building hosting Command and Control Centre should be armed and it must be possible to even depute police personnel for physical security of the premises if felt necessary.
- Networking & Security Infrastructure and other associated IT Components.

d. 24 x 7 Helpdesk and other monitoring and management services.

e. Purchase of all the Non IT and IT Equipment for the ICCC Project.

f. Physical infrastructure components such as UPS, Diesel Generator Units, Power, and cabling for power and data connectivity, etc. The recurring charges of diesel consumption for DG set will be borne by MSI.

g. IT Infrastructure components such as Servers, Databases, System Software , Networking & Security components, Storage Solution, Software and other IT components required for the ICCC Project.

h. No Products supplied under the RFP should be nearing their date of "end of life".

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 BSCDCL.

m. Standard business process management framework should be followed for workflow management with capabilities of configurability at user level.

n. Acceptance of the source code is by installing and generating the object code on a test environment performing identically to that of the production environment.

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

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

a. The bill of material proposed by the MSI bidder will be approved by BSCDCL for its supply and installation. Indicative IT Infrastructure to be commissioned as part of the ICCC project at Command and Control Centers are as under:

i. Servers (inclusive of OS)

- Application Servers
- 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 in this

ii. Application & System Software

- Integrated Command and Control Centre Application
- Enterprise Management Software (EMS)
- GIS software
- RDBMS (if required)
- Anti-virus Software
- Backup Software
- Virtualization software
- Host Intrusion Prevention System (HIPS) software
- Security Information & Event Management (SIEM) software
- Customised Software to cater to requirements of Project Requirements

iii. Other systems

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

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

4. The MSI shall prepare the overall data centre establishment & their operational plan for this project. The plan shall comprise of deployment of all the equipment required under the project. The implementation roll-out plan for setting up the data centre shall be approved by BSCDCL.

The detailed plan shall be also comprise of the scalability, expandability and security that such data centre will implement under this project.

5. The MSI shall establish a state of the art Command Centre, the key components of the Command Centre will be as follows:

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

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

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

2.3.3 Open Data Platform

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

2.3.4 Document Management

a. System should support the storing of document (Image & Metadata)

b. Support for archiving a large number of file formats. The system should support all commonly used file formats as MSOffice, Acrobat, TIF, JPEG, GIF, BMP, etc.

c. Provision for an integrated scanning engine with capability for centralized and decentralized Scanning & Document Capturing. The scanning solution should directly upload documents in Document management system.

d. Association of the document with Workflow Management System

e. Movement of the document based on selected parameters

f. Provision to edit the document Metadata

g. Versioning of the document

h. Provision for marking comments

i. Archival of data on pre-defined parameters

j. Role based access to the documents

k. Final Decision by the Decision Authority

l. Should be platform independent and should support both Linux and Windows both with and without virtualization. It should support multiple databases i.e. MSSQL, Oracle and Postgre.

m. The inbuilt image viewer shall support comprehensive annotation features like highlighting, marking text, underlining putting sticky notes on documents, and support for text and image stamps etc.

n. Should include record management to manage lifecycle of documents through record retention, storage, retrieval and destruction policies and should be certified for record management standard like DoD 5015.02/ISO 15489.

2.3.5 Workflow Management System

a. Movement of Proposals on various parameters

b. Facility to mark the application to pre-defined hierarchy

c. Inbox for officers (listing applications received)

d. FIFO principle for taking action on application

e. Creation of a Note Sheet for Scanned Documents

f. Alerts for delay in action

g. Compliance to workflow standards: BPMN, BPEL and WFMC

h. Shall support Inbuilt Graphical workflow designer for modelling complex Business Processes using drag and drop facilities.

i. Information/Alert to be sent to higher authority in case of delay in action by specific employee of the department

j. Pre-defined scrutiny for citizen applications

k. Display of all application data during scrutiny process

l. Check-list for rejection

m. Should have inbuilt Rule Engine for defining rules

n. Facility to mark the application to other officer

o. Facility to mark the application to other department for their NOC / Comments / Input

p. Final Decision by the Decision Authority

q. Shall provide graphical and tabular tools to create reports and view progress of each individual process.

2.3.6 File Tracking System

a. Scanning & Marking the inward to the respective department.

b. Capturing of DAKs using inbuilt scanning solution.

c. Incorporation of separate hierarchy for RTI letter movements & Commissioner Office.

d. Capturing of Fresh applications & Appeals

e. Tracking of the Inward and outward correspondence

f. File Closure to be carried out as per the final decision of respective authorities.

g. DAK and File Management system should build using robust Enterprise Document Management and Workflow Management and should comply with the Manual of Office Procedure (MOP), published by the Department of Administrative Reforms and Public Grievances (DARPG).

h. Shall have an In-built Web based Text Editor with basic functionalities such as bold, alignment, font, color etc. for writing the notes.

i. The system shall provide a facility to view correspondences (DAKs) on RHS and indexing fields on LHS.

j. Shall support the Whitehall view of the file. The system shall replicate the Present file handling in the same manner as followed i.e. electronic files shall give the same look and feel of Physical file with documents on the right hand side and green note sheet on the left hand side.

2.3.7 Data Analytics Capabilities

a. The ICCC software solutions should have inbuilt capability of data analytics/ business intelligence.

b. The Data Analytics/ BI Tool of software solution should work as single platform for analyzing data coming/input from all the IT components/initiative of Bhopal smart city like DIAL 100, DIAL 108 or Safe City project.

c. The system should be able to generate report in the user defined manner.

d. There should be a provision for a dash board which may take input from various system like individual sensors of multiple IT components (SCADA sensor, Environment sensors etc.)

e. Apart from basic analytics system should also have provision to perform Predictive Analysis.

f. User should be able to choose any permutation and combinations of data fields to perform predictive analysis.

g. System should be able to predict the events, make scenarios which helps in decision making to city authorities.

h. The Data analytics/BI tool should have ability to analyze the useful information and sharing it with general public. For example in case of water supply effected areas and traffic situation awareness etc.

i. System should have capabilities to suggest best response options on the basis of current and historic data sets.

j. Solution should enable the department to monitor activities and operations relating to the citizen (Municipal) service being provided, feedback and grievances received

k. Solution should help department understand the level of responsiveness of the officers concerned in terms of their response to the grievances.

l. The solution should also contain abilities for forecasting and scenario analysis, this will help the department understand the trends of different concern areas.

m. Forward looking decision making – BI and analytics tool provide the predictive and forecasting capabilities which can help department in forward looking policy and decision making.

n. Analysis of citizen sentiment across topics as represented through news and social media

o. Identification of recently emerging and trending topics of interest

p. Providing analytical platform for identification of misclassified events reported by citizens and inadequacies in action taken versus relief requested

q. System shall provide an Enterprise Reporting and Visualization solution to author, manage, and deliver all types of highly formatted reports

r. The solution should have mining, analytical and querying capabilities, and should be able to interoperate with other DBMS.

s. The BI Platform should have the capability to schedule reports on the basis of a time calendar i.e. by hour, day, week, month, etc.

t. The BI Platform should have the capability to schedule reports on the basis of a trigger or an occurrence such as an email, database refresh, etc.

u. Solution should provide capability to :

- Understand issues and concerns of citizens in a quick and effective manner
- Monitor progress of grievances and quality of grievance redressal
- Understand special / specific needs for different part of cities / subject areas affecting citizens (such as water, electricity etc.)

2.3.8 Helpdesk

a. MSI 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.

2.3.9 Disaster Management

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

2.3.10 Integration of GIS Platform

BSCDCL has prepared a GIS application for providing GIS MAP based services. GIS layers are already created under GIS application for BSCDCL. There are approximately 90 numbers of GIS layers created on GIS application. The MSI should be able to integrate these GIS layers on user interface of command and control software application.

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

2.3.11 Experience Centre

The bidder should conceptualize and provide a state of the art experience center. This experience center will be integral part of ICCC. Experience center would be used to practically showcase or demonstrate the latest technologies and innovative solutions with reference to smart city solutions. The bidder should plan for the experience center in the design of ICCC building. The experience center will be established within 6 months from the time of handing over physical building by BSCDCL to bidder. It will be managed by bidder for O&M period (5 years). The bidder should periodically update the technological solutions with the advancement of technology.

It is imperative that technology will drive the next wave of growth hence it is crucial to make technology more accessible for faster adoption. This experience center will help entrepreneurs, and institutions gain a first-hand experience of modern technologies. It will also help in understand the value of IT and make it easier for stakeholders to adopt IT solutions. This initiative is also well in line with the government's 'Digital India' campaign.

2.3.12 ICCC Data Centre

The MSI 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 Centre for 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 942 standards.

b. Ensure redundancy for all the key components to ensure that no single point of failure affects the performance of the overall system

c. Support peak loads

d. MSI will not procure Infrastructure including Hardware, COTS Software licenses and other system software etc. at the start of the project, but will procure after discussion and receipt of go ahead from BSCDCL.

e. MSI 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 MSI shall not use the same for any other purpose.

h. The ownership of Data Centre shall get transferred to BSCDCL after "Acceptance and Go Live" of such items by BSCDCL/ BSCDCL appointed TPAs.

i. MSI to ensure warranties/AMCs are procured for all the hardware components for entire duration of the project including O&M Phase (1+5 years). For software components the support from OEM to be obtained for prescribed components. There would be a mechanism to verify these details on annual basis.

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

k. In the Data Center MSI 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

2.3.13 Situation Room

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

b. MSI shall do the necessary civil work and furnishing for the Situation room.

c. This room will also be used to do the discussion on the analysis done by ICCC system based on the data feeds.

d. This room will provide privacy features like acoustic treatment and will have limited access (using access management system)

e. This room must have the following

i. Small Video wall (1 x 2) with 55inch screens

ii. Video Conferencing facility
iii. Sitting capacity for 20 personal on a round table (with table top touch screens/capacitive, 84")
iv. 2 workstations (same as provided in ICCC) – these system should be capable of triggering any command on the ICCC system.

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

2.3.14 Disaster Recovery

a. MSI shall propose to host Applications and storage on cloud for complete Data Recovery (DR) operations.

b. MSI should select the Cloud Service Provider from the empaneled vendors of Deity.

c. Below are the key factors to be considered for cloud hosting-

i. The MSI is required to prepare and submit along with their technical proposal, the details of methodologies and computations for sizing and capacity of storage, compute, backup, network and security.
ii. Government Community Cloud should only be used by CSP
iii. There should be physical and logical separation (of space, servers, storage, network infrastructure and networks) to protect data, applications and servers.
iv. The system will be hosted in the site identified by the MSI and as agreed by the BSCDCL for DR (backup only).
v. There should be sufficient capacity (compute, network and storage capacity offered) available for near real time provisioning (as per the SLA requirement of the BSCDCL) during any unanticipated spikes in the user load.
vi. DR site will be located in India only.
vii. Ensure redundancy at each level
viii. MSI shall provide interoperability support with regards to available APIs, data portability etc. for the BSCDCL to utilize in case of Change of cloud service provider, migration back to in-house infrastructure, burst to a different cloud service provider for a short duration or availing backup or DR services from a different service provider.
ix. The MSI is fully responsible for tech refreshes, patch management and other operations of infrastructure that is in the scope of the MSI.
x. BSCDCL retains ownership of all virtual machines, templates, clones, and scripts/applications created for the BSCDCL's application. BSCDCL retains the right to request (or should be able to retrieve) full copies of these virtual machines at any time
xi. Provide a robust, fault tolerant infrastructure with enterprise grade SLAs with an assured uptime of 99.5%, SLA measured at the VM Level & SLA measured at the Storage Levels
xii. Cloud services should be accessible via internet and MPLS.
xiii. Required Support to be provided to the BSCDCL in migration of the VMs, data, content and any other assets to the new environment created by the BSCDCL or any Agency (on behalf of the BSCDCL) on alternate cloud service provider's offerings to enable successful deployment and running of the BSCDCL's solution on the new infrastructure.
xiv. The MSI should configure, schedule and manage backups of all the data including but not limited to files, folders, images, system state, databases and enterprise applications

a) Perform and store data and file backups consisting of an initial full back up with daily incremental backups for files;

b) For the files, perform weekly backups;

c) For the databases, perform a twice weekly full database backup, with a three times daily backup of database log files

d) Encryption of all backup files and data and management of encryption keys as a service that can be enabled for Government Departments that require such a service.

e) Retain database backups for thirty (30) days

xv. The MSI should offer dashboard to provide visibility into service via dashboard.

xvi. MSI shall not delete any data at the end of the agreement (for a maximum of 45 days beyond the expiry of the Agreement) without the express approval of the BSCDCL.

Preparation of Disaster Recovery Operational Plan

The bidder should provide detailed operating procedures for each application during the following scenarios. These will be mutually agreed upon with Authority during the project kick off.

- Business as usual: the primary site is functioning as required, procedures for ensuring consistency of data availability at secondary site.
- Disaster: Declaration of disaster, making the DR site live for production, ensuring availability of users to the secondary site.
- Operations from DR site: Ensuring secondary site is addressing the functionality as desired

Configure proposed solution for usage

The service provider shall provide DR Management Solution to Authority meeting following specifications:

#	Features
1	The proposed solution must offer a workflow based management& monitoring and reporting capability for the real time monitoring of a DR solution parameters like RPO (at DB level), RTO, replication status and should provide alerts(including SMS and e-mail alerts) on any deviations. The proposed solution should be able to conduct DR Drills from a centralized location
2	The proposed solution should provide a single dashboard to track DR Readiness status of all the applications under DR
3	The proposed solution should be capable of reporting important health parameters like disk space, password changes, file addition/deletion etc. to ensure DR readiness
4	The proposed solution should have inbuilt ready to use library of recovery automation action for heterogeneous databases and replication environment. This must significantly reduce custom development of scripts and speedy deployment of DR solutions

5	The proposed solution should facilitate out-of-the-box, workflow based switchover and switchback for DR drills for standard applications based on industry best practices
6	The proposed solution should facilitate workflows for bringing up the applications and all the components it depends on at DR while it is up at primary site without pausing/stopping the replication
7	The proposed solution should be able to manage hosts by either deploying agents or without deploying any agent and should not require any change in the existing environment
8	The proposed solution must support all major platforms including Linux, Windows, Solaris, HP-UX, and AIX with native high availability options. It must support both physical and virtual platforms
9	The proposed solution should facilitate workflow based, single-click recovery mechanism for single or multiple applications
10	The proposed DRM solution should integrate seamlessly with the existing setup without the need to reconfigure or remove existing application setup including clusters
11	The proposed solution should cover all the functionalities mentioned in the specifications and all the required licenses should be provisioned

Periodic Disaster Recovery Plan Update

The service provider shall be responsible for –

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

2.3.15 Design, Supply, Installation and Commissioning of Network & Backbone Connectivity for ICCC

1. Network & Backbone Connectivity is one of the most important components of the project and needs very careful attention in assessment, planning and implementation. It is important not only to ensure that the required connectivity is provisioned within the required timelines but also ensure that it is reliable, secure and supports the required SLA parameters of Latency, Jitter, Packet Loss and Performance.
2. It is envisaged that the ICCC system shall leverage Network Backbone infrastructure that is being created by BSCDCL under other smart city initiatives.

3. It is proposed that the MSI should help BSCDCL procure bandwidth as a service for the entire duration of project period for the locations which are not covered by BSCDCL, based on the approval from BSCDCL.

4. MSI should provide the network backbone infrastructure requirements for connectivity between individual command centres and ICCC. The details of the same are listed below:

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

*These other services will be additional work and will be taken up as "Change request" following the process defined in Clause 37 and 43 of Vol III of this RFP.

5. MSI has to provide the last mile connectivity between all above command and control centres and ICCC. MSI has to coordinate with, BSCDCL and telecom service provider for setting up last mile connectivity and other connectivity.

6. MSI will be required to maintain the network backbone infrastructure for connectivity between the following Command Centres / Components and proposed ICCC.

7. BSCDCL shall be providing the network backbone infrastructure requirement for connectivity between the following Command Centres / Components and proposed ICCC. MSI will be required to propose the bandwidth and help BSCDCL in procurement.

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

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

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

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

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

    c. MSI will also provide internet connectivity at ICCC site.

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

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

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

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

10. The MSI shall prepare the overall network connectivity plan for this project. The plan shall comprise of deployment of required network equipment in the field to be connected over network, any clearances required from other government departments for setting up of the entire network. The network architecture proposed should be scalable and in adherence to network security standards. It is necessary that 100% of the proposed connectivity should be wired.

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

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

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

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

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

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

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

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

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

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

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

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

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

2.3.16 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 BSCDCL & its authorized committees. The Security policy needs to be submitted by the MSI within 1st quarter of the successful Final Acceptance Tests.

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

2.3.17 Training and Capacity Building

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

   a. BSCDCL's employees
   b. BMC's employees

c. Stakeholder departments
d. Command Center Operator

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

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

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

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

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

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

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

   b. Computer based training modules

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

   d. Presentations

   e. User manuals

   f. Operational and maintenance manuals for the ICCC modules

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

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

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

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

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

10. There are estimated 100 users who need to be trained. MSI may accordingly plan the training budget.

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

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

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

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

2.3.18 Acceptance Testing

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

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

Type of Testing	Responsibility	Scope of Work
System Testing	MSI	1. MSI to perform System testing 2. MSI to prepare test plan and test cases and maintain it. BSCDCL may request the MSI to share the test cases and results 3. Should be performed through manual as well as automated methods 4. Automation testing tools to be provided by MSI. BSCDCL doesn't intend to own these tools.
Integration Testing	MSI	1. MSI to perform Integration testing

		2. MSI to prepare and share with BSCDCL the Integration test plans and test cases 3. MSI to perform Integration testing as per the approved plan 4. Integration testing to be performed through manual as well as automated methods 5. Automation testing tools to be provided by MSI. BSCDCL doesn't intend to own these tools
Interoperability Testing	MSI	1. MSI will prepare interoperability traceability matrix with third party systems (existing legacy systems with ICCC) in consultation with BSCDCL and other relevant stakeholders (of external systems). Interoperability is an ability of one system to interact with another system. This matrix will cover all the use cases of system interaction and data movement. 2. MSI to perform Interoperability testing 3. MSI to prepare and share with BSCDCL the Interoperable test plans and test cases with scenarios 4. MSI to perform Interoperable testing as per the approved plan 5. In Interoperability testing all the functions / components will be tested of a particular third party system which is integrated with ICCC.
Performance and load Testing	• MSI • BSCDCL / Third Party Auditor (to monitor the	1. MSI to do performance and load testing. 2. Various performance parameters such as transaction response time, throughput, and

	performance testing)	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 BSCDCL. 5. Performance testing to be carried out in the exact same architecture that would be set up for production. 6. MSI need to use performance and load testing tool for testing. BSCDCL doesn't intend to own these tools. • BSCDCL if required, could involve third party auditors to monitor/validate the performance testing. Cost for such audits to be paid by BSCDCL.
Security Testing (including Penetration and Vulnerability testing)	• MSI • BSCDCL / Third Party Auditor (to monitor the security testing)	1. The solution should demonstrate the compliance with security requirements as mentioned in the RFP including but not limited to security controls in the application, at the network layer, network, data Centre(s), security monitoring system deployed by the MSI 2. The solution shall pass vulnerability and penetration testing. The solution should pass web application security testing for the portal, mobile app and other systems and security configuration review of the infrastructure if applicable. 3. MSI should carry out security and vulnerability testing on the developed solution. 4. Security testing to be carried out in the exact same environment/architecture that would be set up for production.

		5. Security test report and test cases should be shared with BSCDCL 6. Testing tools if required, to be provided by MSI. BSCDCL doesn't intend to own these tools 7. During O&M phase, penetration testing to be conducted on yearly basis and vulnerability assessment to be conducted on half-yearly basis. BSCDCL will also involve third party auditors to perform the audit/review/monitor the security testing carried out by MSI. Cost for such auditors to be paid by BSCDCL.
User Acceptance Testing of ICCC System	• BSCDCL appointed third party auditor	1. BSCDCL appointed third party auditor to perform User Acceptance Testing 2. MSI to prepare User Acceptance Testing test cases 3. UAT to be carried out in the exact same environment/architecture that would be set up for production 4. MSI should fix bugs and issues raised during UAT and get approval on the fixes from BSCDCL / third party auditor before production deployment 5. Changes in the application as an outcome of UAT shall not be considered as Change Request. MSI has to rectify the observations.

Note:

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

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

the requirements specified in the RFP. The MSI shall take remedial action based on outcome of the tests.

c. The MSI shall arrange for environments and tools for testing and for training as envisaged. Post Go-Live; the production environment should not be used for testing and training purpose. If any production data is used for testing, it should be masked and it should be protected. Detailed process in this regard including security requirement should be provided by the MSI in its technical proposal. The process will be finalized with the selected bidder.
d. All the Third Party Auditors (TPA) as mentioned above will be appointed and paid by BSCDCL directly. All tools/environment required for testing shall be provided by the MSI.

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

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

2.3.19 Operations and Maintenance for a period of 5 years

MSI will operate and maintain all the components of the ICCC for a period of five (5) years after Go-Live date. During O&M phase, MSI shall ensure that service levels are monitored on continuous basis; service levels are met and are reported to BSCDCL. After Go-Live, if any system/sub-system/appliance that is deployed during the O&M phase must be added in the ICCC only after proper induction procedures are followed including hardening and security testing. MSI needs to implement suitable Performance Improvement Process (PIP) in the project. PIP program applies to all the processes of ICCC project. MSI need to submit its detailed approach for PIP in its technical proposal. Every process and procedure implemented in ICCC project must be reviewed and updated by MSI at least on annual basis from the Go-Live Date. All the manpower engaged for O&M support of the project should be citizens of India.

MSI will ensure that at no time shall any data of ICCC be ported outside the geographical limits of the country.

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

2.3.19.1 Helpdesk and Facilities Management Services

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

The MSI shall setup a central helpdesk dedicated (i.e. on premise) for the Project, which shall be supported by individual smart city command centres, implemented and proposed to be setup under Bhopal 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.

Functional requirements of the helpdesk management system, fully integrated with the enterprise monitoring and network management system, are provided in **Annexure III**. The system will be accessed by the stakeholder department officials for raising their incidents and logging calls for support. The detailed service levels and response time, which the MSI is required to maintain for provisioning of the FMS services are described in the Service Level Agreement of this Tender.

MSI shall deploy Manpower during implementation and O&M phases. The deployed resource shall report to BSCDCL's Project In-charge for Smart City Project and work closely with Program Management Office of the project. Following are the minimum resources required to be deployed in the Project, however MSI may deploy additional resources based on the need of the Project and to meet the defined SLAs in this RFP:

#	Type of Resource	Minimum Quantity	Minimum Deployment during Operation and Maintenance phase
1.	Project Manager	1	100%
2.	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 (24*7 – 1 in each shift)	3	100%
11.	Command Center Operators (24*7 – 10 in each shift)	30	100%

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

2.3.19.2 Applications Support and Maintenance

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

comprehensive ticketing solution. Key activities to be performed by MSI in the application support phase are as follows:

a. Compliance to SLA

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

b. Annual Technology Support

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

c. Application Software Maintenance

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

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

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

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

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

vi. MSI, at least on a monthly basis, will inform BSCDCL about any new updates/upgrades available for all software components of the solution along with a detailed action report. In case of critical security patches/alerts, the MSI shall inform about the same immediately along with his recommendations. The report shall contain MSI's recommendations on update/upgrade, benefits, impact analysis etc. The MSI shall need to execute updates/upgrades though formal change management process and update all documentations and Knowledge databases etc. For updates and upgrades, MSI will carry it out free of cost by following defined process.

d. Problem Identification and Resolution

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

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

e. Change and Version Control

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

i. Detailed impact analysis

ii. Change plan with Roll back plans

iii. Appropriate communication on change required has taken place

iv. Proper approvals have been received

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

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

vii. Version control maintained for software changes

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

f. Maintain configuration information

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

g. Training

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

h. Maintain System documentation

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

i. High level design of whole system

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

iii. System requirements Specifications (SRS)

iv. Any other explanatory notes about system

v. Traceability matrix

vi. Compilation environment

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

i. Source code is documented

ii. Functional specifications are documented

iii. Application documentation is updated to reflect on-going maintenance and enhancements including FRS and SRS, in accordance with the defined standards

iv. User manuals and training manuals are updated to reflect on-going changes/enhancements

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

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

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

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

l. Any additional changes required would follow the Change Control Procedure. BSCDCL may engage an independent agency to validate the estimates submitted by the MSI. The inputs of such an agency would be taken as the final estimate for efforts required. MSI to propose the cost of such changes in terms of man month rate basis and in terms of Function point/Work Breakdown Structure (WBS) basis in the proposal.

2.3.19.3 ICT Infrastructure Support and Maintenance

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

2.3.19.4 Technology Refresh

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

Key Drivers for technology refresh:

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

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

2.3.19.5 Warranty support

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

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

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

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

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

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

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

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

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

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

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

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

2.3.19.6 *Maintenance of ICT Infrastructure of Command and Control Centre (ICCC)*

a. Management of ICT Infrastructure of ICCC

MSI 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 MSI and be Indian citizens. All the L1 and L2 resources proposed for the project need to be dedicated for the ICCC project. Any change in the team once deployed will require approval from BSCDCL. It is expected that the majority of resources have worked with MSI for at least preceding 1 year and have proven track record and reliability. Considering the criticality of the project, BSCDCL may ask for security verification (Police verification) of every resource deployed on the project and MSI need to comply the same before deployment of the resource at the project. At all times, the MSI need to maintain the details of resources deployed for the project to BSCDCL and keep the same updated. A detailed process in this regard will be finalized between BSCDCL and MSI. The MSI shall maintain an attendance register for the resources deployed Attendance details of the resources deployed also need to be shared with BSCDCL on monthly basis. BSCDCL reserves the right to interview resources deployed for Operations and maintenance and assess the suitability of the resource for the role. In case a resource is not found suitable, MSI will change the resource on request of BSCDCL. MSI shall comply with this.

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

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

ii. Ensure compliance to relevant SLA's

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

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

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

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

vii. Preventive maintenance plan for every quarter

viii. Performance tuning of system as required

ix. Design and maintain Policies and Standard Operating Procedures

x. User access management

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

xii. Updation of all Documentation.

During operations phase the MSI needs to submit proof of renewal of support for all IT infrastructure products and other system software's for whom it is mandated to have OEM support. This needs to be submitted on an annual basis and needs to be verified before release of 2nd quarter payment of each year.

b. System Maintenance and Management

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

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

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

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

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

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

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

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

c. System Administration

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

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

iii. MSI shall be responsible for operating system administration, including but not limited to management of users, processes, preventive maintenance and management of upgrades including updates, upgrades and patches to ensure that the system is properly updated.

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

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

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

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

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

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

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

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

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

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

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

d. Storage Administration

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

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

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

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

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

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

vii. To facilitate scalability of solution wherever required.

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

e. Database Administration

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

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

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

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

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

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

f. Backup/Restore/Archival

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

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

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

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

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

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

g. Network monitoring

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

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

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

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

h. Security Management

i. Regular hardening and patch management of components of the ICCC system as agreed with BSCDCL

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

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

iv. Reporting security incidents and resolution of the same

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

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

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

viii. Reporting security incidents and co-ordinate resolution

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

x. Maintaining secure domain policies

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

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

xiii. Resolution of calls for security notifications, system alerts, vulnerabilities in hardware/software and alerting BSCDCL as appropriate

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

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

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

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

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

xix. Performing periodic review of security policy and suggest improvements

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

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

xxii. Modifying security policy, routing table and protocols

xxiii. Performing zone management (DMZ)

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

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

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

xxvii. Testing and implementation of patches and upgrades

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

xxix. Implementing and maintaining security rules

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

i. Other Activities

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

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

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

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

v. Updates/Upgrades/New releases/new versions: The MSI shall provide from time to time the Updates/Upgrades/new releases/new versions of the software and operating systems as required. The MSI should provide free upgrades, updates & patches of the software and tools to BSCDCL as and when released by OEM.

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

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

viii. Disaster Recovery management services

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

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

2.3.19.7 Compliance to SLA

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

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

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

2.3.20 Project Implementation Timelines

Sl No.	Activity / Deliverables	Timelines
1	Project Inception Report (must include 10 services to be implemented as part of Go-Live, implementation plan, resource deployment plan and co-location plan for services)	T1+ 30 Days
2	Requirement Analysis and Report	T1+45 Days
3	Complete System Design and submission of Design Report along with engineering drawings Including ICCC building design (using 3D Simulation along with physical report)	T1+ 90 Days
4	Installation of Hardware and S/W Infrastructure and acceptance testing + Submission of Installation Report	T2+120 Days
5	Integration with various service components (T= Readiness/Service Availability for integration) T will be different for each service and will be based on agreed project plan	T+ 90 Days
6	Go Live and Go Live Report	T2 + 240 Days
7	Operation and Maintenance (Submission of Quarterly SLA Report)	G+5 Years

T1 = Date of signing contract Agreement

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

G = Go Live Date

Go – Live Report: Go – Live report will consists of all testing reports of identified services, along with all the As-build drawing with marking of field devices, controllers and sensors, As-implemented configurations, As-implemented architecture and topology diagrams, Standard operating procedures for administration of the installed devices, Each Site specific user manual and standard operating procedures for end users, Hardware-devices warranty details and License details.

List of service to be integrated with ICCC

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

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

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

#	Name of Service	Integration timelines	Co-location	Advanced analytics
1	Dial 100	At launch	X	√
2	Dial 108	At launch	X	√
3	Traffic Management System	3 months	X	√
4	Safe City Cameras feed	At launch	X	√
5	Met Department (Weather Forecast)	At launch	X	√
6	Emergency Response and Disaster Management	6 months	X	√
7	Smart Parking	At launch	√	√
8	Public Bike Sharing	At launch	√	√
9	Smart Pole & Smart Lighting	3 months	√	√
10	Solid Waste Management services	6 months	√	√
11	Intelligent Transport Management System	12 months	√	√
12	BMC Call Centre & BMC Services	At launch	√	√
13	Bhopal Smart Map (GIS)	At launch	√	√
14	Bhopal Plus	At launch	√	√
15	Water management System	6 months	√	√
16	Dynamic Market Place (Mayor Express)	6 Months	√	√
17	Crowdsourcing Data	12 months	√	√
18	Fire Brigade Control System	12 months	√	√

19	Solar Roof Top	At launch	√	√
20	ABD services Utilities • Lighting • Metering • Surveillance	2 years	√√	√√

2.3.21 Exit Management

a. This sets out the provisions, which will apply on expiry or termination of the Master Service Agreement, the Project Implementation, Operation and Management SLA.

b. In the case of termination of the Project Implementation and/or Operation and Management, the Parties shall agree at that time whether, and if so during what period, the provisions of this Schedule shall apply.

c. The Parties shall ensure that their respective associated entities carry out their respective obligations set out in this Exit Management Schedule.

d. The MSI shall provide the following documentation at the stage of exit management:
   i) 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

2.3.21.1 Cooperation and Provision of Information

During the exit management period:

a. The MSI will allow the BSCDCL or its nominated agency access to information reasonably required to define the then current mode of operation associated with the provision of the services to enable the BSCDCL to assess the existing services being delivered

b. Promptly on reasonable request by the BSCDCL, the MSI shall provide access to and copies of all information held or controlled by them which they have prepared or maintained in accordance with this agreement relating to any material aspect of the services (whether provided by the MSI or sub-contractors appointed by the MSI). The BSCDCL shall be entitled to copy of all such information. Such information shall include details pertaining to the services rendered and other performance data. The MSI shall permit the BSCDCL or its nominated agencies to have reasonable access to its employees and facilities, to understand the methods of delivery of the services employed by the MSI and to assist appropriate knowledge transfer.

2.3.21.2 Confidential Information, Security and Data

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

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

   ii. documentation relating to Intellectual Property Rights;

   iii. documentation relating to sub-contractors;

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

   v. all other information (including but not limited to documents, records and agreements) relating to the services reasonably necessary to enable BSCDCL or its nominated agencies, or its Replacement MSI to carry out due diligence in order to transition the provision of the Services to BSCDCL or its nominated agencies, or its Replacement System integrator (as the case may be).

b. Before the expiry of the exit management period, the MSI shall deliver to the BSCDCL or its nominated agency all new or up-dated materials from the categories set out in Schedule above and shall not retain any copies thereof, except that the MSI shall be permitted to retain one copy of such materials for archival purposes only.

2.3.21.3 Employees

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

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

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

2.3.21.4 Transfer of Certain Agreements

On request by the BSCDCL or its nominated agency the MSI shall effect such assignments, transfers, licenses and sub-licenses BSCDCL, or its Replacement MSI in relation to any equipment lease, maintenance or service provision agreement between MSI and third party lessors, vendors, and which are related to the services and reasonably necessary for the

carrying out of replacement services by the BSCDCL or its nominated agency or its Replacement MSI.

2.3.21.5 General Obligations of the MSI

a. The MSI shall provide all such information as may reasonably be necessary to effect as seamless a handover as practicable in the circumstances to the BSCDCL or its nominated agency or its Replacement MSI and which the MSI has in its possession or control at any time during the exit management period.

b. For the purposes of this Schedule, anything in the possession or control of any MSI, associated entity, or sub-contractor is deemed to be in the possession or control of the MSI.

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

2.3.21.6 Exit Management Plan

a. The MSI shall provide the BSCDCL or its nominated agency with a recommended exit management plan ("Exit Management Plan") which shall deal with at least the following aspects of exit management in relation to the MSA as a whole and in relation to the Project Implementation, and the Operation and Management SLA.

   i. A detailed program of the transfer process that could be used in conjunction with a Replacement MSI including details of the means to be used to ensure continuing provision of the services throughout the transfer process or until the cessation of the services and of the management structure to be used during the transfer;

   ii. plans for the communication with such of the MSI's sub-contractors, staff, suppliers, customers and any related third party as are necessary to avoid any material detrimental impact on the BSCDCL's operations as a result of undertaking the transfer;

   iii. (if applicable) proposed arrangements for the segregation of the MSI's networks from the networks employed by BSCDCL and identification of specific security tasks necessary at termination;

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

b. The MSI shall re-draft the Exit Management Plan annually thereafter to ensure that it is kept relevant and up to date.

c. Each Exit Management Plan shall be presented by the MSI to and approved by the BSCDCL or its nominated agencies.

d. The terms of payment as stated in the Terms of Payment Schedule include the costs of the MSI complying with its obligations under this Schedule.

e. In the event of termination or expiry of MSA, and Project Implementation, each Party shall comply with the Exit Management Plan.

f. During the exit management period, the MSI shall use its best efforts to deliver the services.

g. Payments during the Exit Management period shall be made in accordance with the Terms of Payment Schedule.

h. This Exit Management plan shall be furnished in writing to the BSCDCL 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 MSI will ensure that the entire ICCC solution is developed in compliance with the applicable standards.

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

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

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

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

   b. Guidelines and advisories for information security published by Cert-In/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 MSI should ensure high-quality documentation standards to improve the readability of the software module. An illustrative list of comments that each module contained within the source file should be preceded by is outlined below:

   a. The name of the module

   b. The date when module was created

   c. A description of what the module does

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

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

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

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

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

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

a. Proper and consistent indentation

b. Inline comments

c. Structured programming

d. Meaningful variable names

e. Appropriate spacing

f. Declaration of variable names

g. Meaningful error messages

6. Quality Audits

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

4 Project Management and Governance

4.1 Project Management Office (PMO)

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

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

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

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

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

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

4.2 Steering Committee

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

The MSI shall participate in monthly Steering Committee meetings and update Steering Committee on Project progress, Risk parameters (if any), Resource deployment and plan, immediate tasks, and any obstacles in project. The Steering committee meeting will be a forum for seeking and getting approval for project decisions on major changes etc.

All relevant records of proceedings of Steering Committee should be maintained, updated, tracked and shared with the Steering Committee and Project Management Office by MSI.

During the development and implementation phase of the project, it is expected that there will be at least fortnightly Steering Committee meetings. During the O&M phase, the meetings will be held at least once a quarter.

Other than the planned meetings, in exceptional cases, BSCDCL may call for a Steering Committee meeting with prior notice to the MSI.

4.3 Project Monitoring and Reporting

The MSI shall circulate written progress reports at agreed intervals to BSCDCL and other stakeholders. Project status report shall include Progress against the Project Management Plan, status of all risks and issues, exceptions and issues along with recommended resolution etc.

Other than the planned meetings, in exceptional cases, project status meeting may be called with prior notice to the Bidder. BSCDCL 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 MSI shall develop a Risk Management Plan and shall identify, analyze and evaluate the project risks, and shall develop cost effective strategies and action plans to mitigate those risks.

The MSI shall carry out a Risk Assessment and document the Risk profile of BSCDCL based on the risk appetite and shall prepare and share the BSCDCL Enterprise Risk Register. The MSI shall develop an issues management procedure to identify, track, and resolve all issues confronting the project. The risk management plan and issue management procedure shall be done in consultation with BSCDCL.

The MSI shall monitor, report, and update the project risk profile. The risks should be discussed with BSCDCL 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 Staffing requirements

BSCDCL has identified certain key positions that should be part of MSI's team during execution. MSI shall provide resource deployment schedule including these key positions and other team members as mentioned in RFP Vol 1 and 2.

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

Please note that BSCDCL shall require that all project related discussion should happen in BSCDCL office. While the identified key personnel will operate out of BSCDCL's office,

other key members of the development/Data Centre team may need to travel to BSCDCL office for critical Project/Steering Committee meetings at their own expenses.

4.6 Governance procedures

MSI shall document the agreed structures in a procedures manual.

4.7 Planning and Scheduling

The MSI will prepare a detailed schedule and plan for the entire project covering all tasks and sub tasks required for successful execution of the project. The MSI has to get the plan approved from BSCDCL at the start of the project and it should be updated every week to ensure tracking of the progress of the project.

The project plan should include the following:

1. The project break up into logical phases and sub-phases;
2. Activities making up the sub-phases and phases;
3. Components in each phase with milestones;
4. The milestone dates are decided by BSCDCL in this RFP. MSI cannot change any of the milestone completion dates. MSI can only propose the internal task deadlines while keeping the overall end dates the same. MSI may suggest improvement in project dates without changing the end dates of each activity.
5. Key milestones and deliverables along with their dates including those related to delivery and installation of hardware and software;
6. Start date and end date for each activity;
7. The dependencies among activities;
8. Resources to be assigned to each activity;
9. Dependency on BSCDCL

5. Change Management & Control

5.1 Change Orders / Alterations / Variations

a. The MSI agrees that the requirements given in the Bidding Documents are minimum requirements and are only indicative. The vendor would need to etch out the details at the time of preparing the design document prior to actual implementation. It shall be the responsibility of the MSI to meet all the requirements of technical specifications contained in the RFP and any upward revisions and/or additions of quantities, specifications sizes given in the Bidding Documents required to be made during execution of the works, shall not constitute a change order and shall be carried out without a change order and shall be carried out without any time and cost effect to Purchaser.

b. Further upward revisions and or additions required to make MSI's selected equipment and installation procedures to meet Bidding Documents requirements expressed and to make entire facilities safe, operable and as per specified codes and standards shall not constitute a change order and shall be carried out without any time and cost effect to Purchaser.

c. Any upward revision and/or additions consequent to errors, omissions, ambiguities, discrepancies in the Bidding Documents which the MSI had not brought out to the Purchaser's notice in his bid shall not constitute a change order and such upward revisions and/or addition shall be carried out by MSI without any time and cost effect to Purchaser.

5.2 Change Order

a. The Change Order will be initiated only in case (i) the Purchaser directs in writing the MSI to include any addition to the scope of work covered under this Contract or delete any part of the scope of the work under the Contract, (ii) MSI requests to delete any part of the work which will not adversely affect the operational capabilities of the facilities and if the deletions proposed are agreed to by the Purchaser and for which cost and time benefits shall be passed on to the Purchaser, (iii) the Purchaser directs in writing the MSI to incorporate changes or additions to the technical specifications already covered in the Contract.

b. Any changes required by the Purchaser over and above the minimum requirements given in the specifications and drawings etc. included in the Bidding Documents before giving its approval to detailed design or Engineering requirements for complying with technical specifications and changes required to ensure systems compatibility and reliability for safe operation (As per codes, standards and

recommended practices referred in the Bidding Documents) and trouble free operation shall not be construed to be change in the Scope of work under the Contract.

c. Any change order as stated in Clause 2 a. comprising an alteration which involves change in the cost of the works (which sort of alteration is hereinafter called a "Variation") shall be the Subject of an amendment to the Contract by way of an increase or decrease in the schedule of Contract Prices and adjustment of the implementation schedule if any.

d. If parties agree that the Contract does not contain applicable rates or that the said rates are inappropriate or the said rates are not precisely applicable to the variation in question, then the parties shall negotiate a revision of the Contract Price which shall represent the change in cost of the works caused by the Variations. Any change order shall be duly approved by the Purchaser in writing.

e. Within ten (10) working days of receiving the comments from the Purchaser or the drawings, specification, purchase requisitions and other documents submitted by the MSI for approval, the MSI shall respond in writing, which item(s) of the Comments is/are potential changes(s) in the Scope of work of the RFP document covered in the Contract and shall advise a date by which change order (if applicable) will be submitted to the Purchaser.

6. Annexure I-Functional 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. Standard Operating Procedures (SoPs) must adhere with the Governance structure of BSCDCL and BMC, as in case of any incident or disaster decision making ability lies with the Authority.

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.

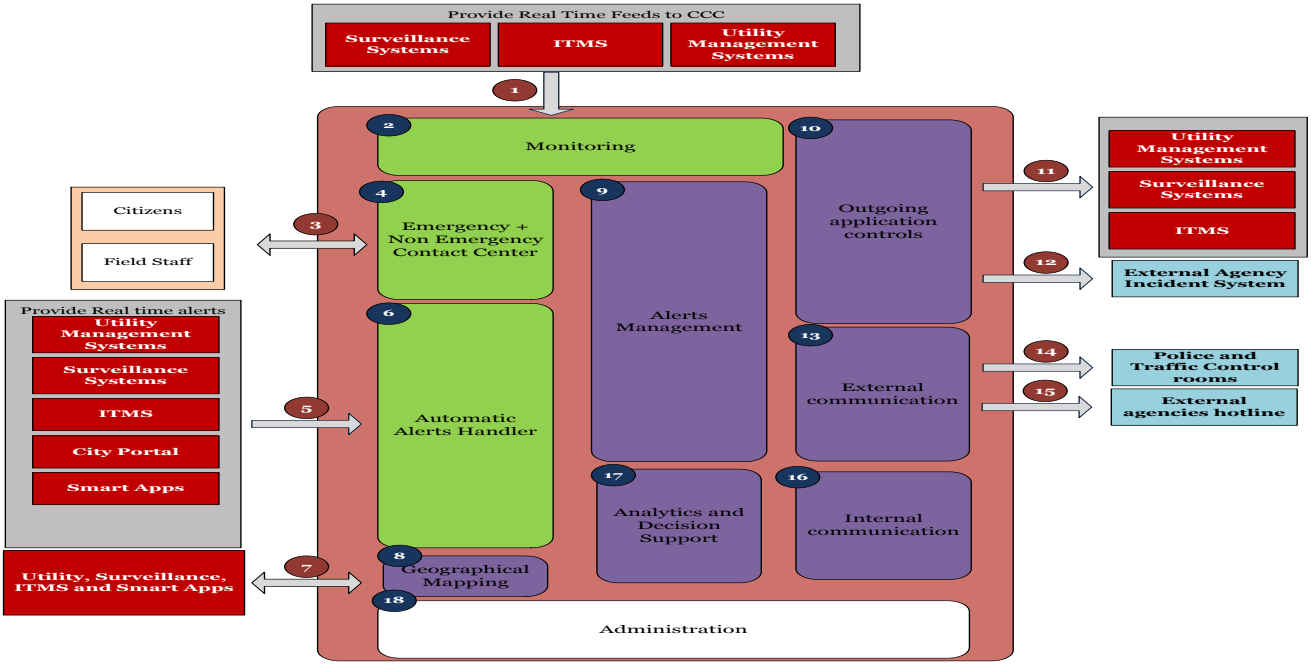
The ICCC shall have a very tight integration between GIS, Common Operating Picture and event/resource/response management functions – ideally at the software level.

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 CCCA:



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 CCCA.
2.	CCCA Function	Feeds received from systems mentioned in 1 above shall enable CCCA 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 center 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 CCC through audio call, SMS, mobile interface and web interface. This will be a two way interface enabling citizens to pass information to CCC and receive updates from CCC on the actions taken by CCC.
4.	CCC Function	The contact center function will enable CCC to record and update both day to day incidents such as electricity break down and emergency situations such as accidents. The contact center will receive the information from citizen and record in the database which will trigger the workflow for resolution of the incident.
5.	Interface	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 CCC via this automated interface. This will enable CCC to create a centralized repository of all 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 • 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.	CCC Function	This function within the CCC will enable it to receive the alerts, 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.	CCC Function	This block refers to the centralized GIS layer that would be created at CCC for access by other systems.

9.	CCC Function	The incidents reported manually through contact center as well as automatically received through alerts handler shall be handled by functional this block. It will execute the workflow for managing the incident life cycle as per pre-defined business rules and SOPs. This will ensure consistency of response to incidents.
10.	CCC Function	The CCC 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 CCC to pass data to be used by various systems e.g. view triggers into various systems such as viewing a specific camera view into CCC, sending SMS through a SMS gateway etc.
12.	Interface	This interface will enable CCC to pass data to intimate the respective agency about incident reported in CCC e.g. creating incident in incident management system of electricity department about power failure
13.	CCC Function	This function will enable CCC 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.	CCC Function	The internal communication within CCC shall be managed through video conferencing and IP telephony systems
17.	CCC Function	This block will enable CCC 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.	CCC Function	This block will enable CCC to define the security access rights, Standard Operating Procedures, Business Rules, and Workflows etc to enable the CCC to function in the desired manner.

The technical components of the CCC 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.	CCC application	1, 2, 5, 6, 9, 10, 11, 12, 17, 18
2.	GIS application with high resolution satellite image (base map) of Bhopal	7, 8
3.	Video wall display system	2
4.	Video Conferencing System	13, 14, 16
5.	IP Telephony	13, 15, 16
6.	Contact center 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 CCC shall be equipped with following facilities:

- Operating facilities for following personnel:
  - CCC operators
  - Contact Center/helpdesk
  - Technical Support
  - NoC
  - Security
- Meeting / conference rooms

MSI has to do required civil work (except structural work) for setting up the ICCC (after handing over of the basic building structure from BSCDCL) and install required furniture and fittings. MSI has to provision for necessary power backup for the ICCC.

Sr #	Requirements
Command and Control Application (CCA)	
1.	The CCA should be commercial-off-the-shelf applications that are customizable to meet the requirements of the RFP.
2.	The CCA should have the capability to integrate with existing GIS. If certain layers are not available then the MSI should give the details to the owner for creation of the layers.
3.	The system shall provide CCA operators and managers with a management dashboard that provides a regular status and is automatically updated when certain actions, incidents and resources have been assigned, pending, acknowledged, dispatched, implemented, and completed. The above attributes shall be colour coded.
4.	The CCA shall provide the “day to day operation”, “Common Operating Picture” and situational awareness to the centre and participating agencies during these

	modes of operation
5.	It shall improve scalability for large and geographically distributed environments.
6.	It shall provide complete view of facilities, sensors, and alarms in an easy-to-use and intuitive GIS-enabled graphical interface with a powerful workflow and business logic engine.
7.	It shall provide a uniform, coherent, user-friendly and standardized interface
8.	It shall provide possibility to connect to workstations in order to be displayed in one or more video wall with one or more module/application/solution being independently and/or simultaneously being displayed and functional.
9.	The dashboard content and layout shall be configurable and information displayed on these dashboards shall be filtered by the role of the person viewing dashboard.
10.	CCA should allow creation of hierarchy of incidents and be able to present the same in the form of a tree structure for analysis purposes
11.	The system shall integrate with GIS and map information and be able to dynamically update information on the GIS maps to show status of resources.
12.	The system shall also provide an integrated user interface to other Bhopal Smart City systems such as City Surveillance System, Utility Management System and Intelligent Transport as well as other third party information systems.
13.	The CCA shall be available via a VPN as a web-based interface or a thin-client interface.
14.	It shall be possible to combine the different views onto a single screen or a multi-monitor workstation.
15.	CCA should maintain a comprehensive and easy to understand audit trail of read and write actions performed on the system.
16.	System should provide ability to extract data in desired formats for publishing and interfacing purposes.
17.	System should provide ability to attach documents and other artefacts to incidents and other entities.
18.	CCA is required to issue, log, track, manage and report on all activities underway during these modes of operation: • anticipation of incident • incident or crisis • recovery • incident simulation
19.	**Core Components** • **Business Rules and SOP Definitions** – should enable users to define the business rules around incidents handling as per agreed SOPs for Bhopal Smart City • **System Platform** – The platform should provide a common data integration layer which can collect and contextualize information from disparate data sources regardless of protocol. The platform should support templatization to allow “build once-deploy everywhere” functionality.

	• **Workflow and Incidents Lifecycle engine** – This function should allow users to define and modify new 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. Workflow approvals should have facility to approve from any device with e-signature. This function should provide facility to trigger a corrective action workflow and define the stakeholders for the same. Should manage the life cycle of incidents and related entities via pre-define workflows. The workflow could cut across multiple systems via the interfacing modules. Workflow for operational alerts and escalations should be triggered automatically without human intervention. • **Incidents Planning** – should manage the planning preparations of an incident including resource allocation, tasks management etc. • **Analytics and MIS** – should provide users with business analytics reporting and tools to organize, evaluate and efficiently perform day to day operations • **Incidents and KPI Dashboards** – should present role filtered critical information pertaining to incidents and KPIs collated in a single view which can be drilled down further for more detailed information • **Security & Roles –** should manage roles definition for internal as well as external access • **Centralized data archiving for operational data :** Should provide facility for centralized storage of operational data (time-series or transactional) with high granularity and data compression capability • **Mobility:** should enable app-based access to monitor alerts, KPI ,KOPs, SOPs and reports to mobile users. Should support popularly user's smartphone /tablets. App content should be presented in context to the user role.
20.	**Planning** • The CCA software should have a planning, workflow and business rules engine to define the Standard Operating Procedures (SOPs) into the system. • The organization of BSCDCL and participating agencies should be configured into the CCA solution. The CCA should be able to create the BSCDCL City Management Centre organization structure together with roles and responsibilities within the system. Access to system functions and data shall be as per define roles and organization structure. • The SOPS shall be capable of being converted into editable but administrator protected workflow and tasks. • The CCA shall present the workflow and task information in a clear and logical manner on the incidents screen.

	• CCA system shall include a section that will contain the Policy and standard operation procedures with easy to search functions to support the Operators during a crisis.
21.	**Situational Awareness COP (Common Operational Picture)** • The CCA should be able to combine data from various sources and present it as different views tailored to different operator's needs. • The CCA should automatically update the information based on alarms and incidents that are presented to it via the business rules engine. The polling and CCA database refresh cycle shall be configurable to match the status of the situation (whether there is an emergency or crisis or just monitoring only). • Common Operational Picture should comprise of a comprehensive view of the incident or a group of related incidents as on a specific date and time which should include but not be limited to the following: o Tasks assignment and their status o Agencies involved o Resources deployed o Incident status across relevant parameters of the incident e.g. household affected by a transformer shut down o Timeline view of the situation o Suggested actions from the system with their status
22.	**Warning and Mitigation** • The CCA should use analytics to create a view of hazards and priorities based on a severity and risk profile. • The CCA shall be able to import data into its analytical tool. • CCA should be capable of easily interfacing with any other external analytical tool that might be required in future to provide warning inputs to Bhopal Smart City. • The CCA shall present a prioritized list of key anticipated incidents, actual incidents, and tasks requiring action. • CCA should be capable of performing multi-dimensional analysis on incidents data. This should provide capability to do: o Trends Analysis o Predictive Capability o "What-if" analysis
23.	**Resource Management** • The system shall provide an object based as well as visual representation of the multi-agency command structure at an incident. This visual representation is to be in the form of an organizational structure diagram. The management of

	resources, (who is doing what and answering to whom) is a critical part of this system and shall be configured into a particular actors attributes. • The system shall provide the following configuration functions around roles: o Allocation of roles o Creation, Editing and renaming of roles o Color coded role definition o Symbolic representation of roles o Notes and comments against roles • The system should provide a mechanism to define roles that are consistent with Organization Structure defined in CCA as part of requirements defined Planning section earlier. • The system should provide the following configuration functions around resources: o Building up the resourcing information on the organization structure o Creation of resources as different types of assets, (Human, physical, financial, equipment, vehicles, machinery etc.) o Assignment of individuals to locations, agencies, tasks, or other resources o Creation of call signs and symbols relating to resources. o Maintaining relationships between resources. o Tracking of availability and movement of resources • The system should provide ability to define attributes of above mentioned resources and their relationships in order to capture the resource definition in a structured manner. • The system should provide ability to create organization structures that could be assigned to a specific operation, incident or a task. Thus assigned organization structure take precedence over the default organization structure
24.	**Task Management** • The system should be able to create, assign, track and report on the lifecycle of tasks during a particular incident. • The system should allow a particular task to be decomposed into sub-tasks. • The system should provide an easy to interpret management dashboard view of the progress of all tasks during an incident. • The system should be able to organise the visual representation of tasks into prioritized list, filtered list, as well as colour coded representation for ease of understanding. • The system should be able to perform the following functions around task management: o Create a task with unique ID. (Subtasks shall follow parent ID with second level numbering).

	○ Assign a target completion date and time for the task, either directly or as a time-span from the task's creation. ○ Date and time stamp of the creation of the task. ○ Log and track status of tasks. System should provide capability to define status of tasks during its lifecycle. These status definitions could be mapped to other task attributes such as the task type. ○ Key-word search against task list. • The above attributes shall be colour coded. • The system shall allow the tasks to be filtered on the real-time dashboard by agency then by task status. This filtering should allow an operator to filter for all tasks of a particular state or a combination of state; and by the time remaining until (or time elapsed since) the target completion time. • The system should allow multiple individual workstations to select specific agencies of interest on each workstation simultaneously. • The system should allow the BSCDCL to display all agencies' tasks simultaneously as well. • The tasks should be displayed on a real-time timeline. • The criticality of tasks should be dynamically changed depending on the performance of the incident response.
25.	**Timeline and Charting** • The system should provide a facility to see incidents and actions (tasks) added to the CCA in a tabular list form as well as GANTT chart format filtered by day, week, month, year or any specific date range. • The system should provide a facility to see incidents, actions and interdependencies between actions in a clear visual graphical manner. • The system should be able to filter the information based on at least the following parameters: ○ Incident information ○ Resources information ○ Agency type ○ Tasks ○ Criticality or priority
26.	**Business Rules Engine** • The CCA system should have a built-in alarm handling facility based on configurable cause and effect rules.

	• The CCA system should receive inputs (referred to as "incidents") from various sources. These incidents when passed through the business rules engine shall trigger an automated response as defined using the business rules engine. • The business rules engine should be able to send and receive messages to other applications running within the CCA suite as well as external systems like the surveillance system. • The business rules engine shall be able to co-relate between different types of incidents or frequency of similar types of incidents. • The business rules engine shall be able to distinguish between "early warning or anticipation" type mode of operation and an "emergency or crisis" mode of operation. • The CCA shall provide capability for users with appropriate rights to define business rules. • Any update to the Business Rules (Add/Edit/Delete) shall go through an approval workflow before the rule gets activated. Workflow approvals should have facility to approve from any device with e-signature. • The CCA shall provide capability to do a simulation run of a newly created/added business rule before it is activated.
27.	**CCA Graphical User Interface (GUI)** • The CCA should present information on standard Windows based workstations and terminals. • The CCA GUI should have the following capabilities as standard: o The CCA GUI shall be able to present management data such as dashboards, alarm and alerts, resource management information, incident information in colour coded, clear, simple and unambiguous, logical format. o The colour coding on the CCA GUI shall represent the different status of a task or incident / alert. o The GUI layout and arrangement of windows shall be user customizable. o Be able to present information and distinguish between an "early warning or anticipation" type set of data and "emergency or crisis" operating mode. • The CCA should be capable of presenting information in a browser based format such that it is accessible from any terminal with a web-browser. The supported browser should include, but not limited to, Internet Explorer, Chrome, Firefox and Safari • The CCA should be capable of showing still as well as video imagery.

	• The CCA shall also be able to present information on mobile devices such as tablets, smart-phones and tablet type devices while maintaining the basic UI features such as user friendliness, colour coding etc. • The CCA information shall be capable of pushing onto other display devices such as the video wall of the City Management Centre. • The CCA should be capable of providing the following features for still imagery: o The system shall have a thumbnail gallery to display all imported images o The system shall be able to import pictures from still imagery cameras o The system shall be able to import pictures from local hard drives o The system shall be able to share the imported images with other users o The system shall time and date stamp any imported images o The system shall have the ability to view each still image full screen o The system shall have the ability to zoom in an out of a still image when viewed full screen o The system shall allow the image to be imported to the planning whiteboard module o The system shall enable users to add tags to images for easy search and retrieval later on o The system shall enable users to group and title images together for easy retrieval • The CCA should be capable of providing the following features for video imagery: o The system shall be able to display video imagery o The system shall have a thumbnail gallery to display all video images o The system shall allow the video streams to be grouped and titled as per defined requirements. • The CCA presentation server shall have the capability of only refreshing those elements of the GUI that have changed state.
28.	**Recovery and Reporting** • The CCA should have a background function to collect and store the centre's performance data during an incident. The performance data shall be user configurable. Typical fields for performance shall be: o Actions-planned versus actual o Resources involved o Decisions executed o Schedule / incident duration performance o Incident information, e.g. no. of fatalities, persons recovered o Post-incident recovery information

	• The analytics tool should be able to produce performance analysis and produce dashboard reports on performance.
	• The CCA should be capable of providing a clear reporting function following an incident for:
	  ○ Management and dashboard reporting
	  ○ Analysis of what went well and "lessons learnt"
	• The CCA should allow users to define benchmarks against performance parameters. Performance reports shall have the option to generate reports with or without benchmark comparison
	• The CCA should provide facility to trigger a corrective action workflow and define the stakeholders for the same.

29.	**General System Display Functionality** • Shall have the facility to view and handle multiple alarms at one time • Shall have the facility to view multiple video windows at one time. Operators shall be able to resize and move video windows. • Shall have the facility to view windows in a single monitor or across multiple monitors • Shall have the facility to access, display and manage incidents/alarms and related sensors data and information from subsystem based on priority and authority level. • Shall view and manage detailed response procedures and tasks • Shall enable a single operator or multiple operators to monitor and control commands from connected subsystems, including all operational capabilities for detection, assessment, notification, entry control, and communications • Shall provide the rapid annunciation and display of alarms to facilitate evaluation and assessment
30.	**GIS Display** • Shall view the environment through geospatial or fixed composite computer-generated (JPEG, BMP, AutoCAD, etc.) map • Should allow user to view sensor and related name from the displayed map • Should allow all resources, objects, sensors and elements on the map to be geo-referenced such that they have a real world coordinate. • Should visually display a camera sensor with related camera orientation, camera range and camera field of view angle.

	• Should visually display an alarming sensor on map • Should visually differentiate sensor alarm severities on map through different color and icon identifiers • Should immediately view alarm details (including description, video, etc.) and investigate the alarm from the map • Should allow user to choose camera and other sensors from map to view live video and the data • Should allow user to choose camera and take live video image snapshot and save to file from any camera • Should allow user to choose camera from map to move PTZ cameras • Should allow user to choose camera to play, pause, stop, fast-forward, rewind, and play recorded video from preset time • Should allow user to choose camera and take recorded video image snapshot and save to file or print from any live or recorded video • Should allow user to jump from one map to the next with a single click of a mouse with map links • Should allow map information "layers" to be displayed/hidden on items such as – o Sensor names o Sensors o Sensor range (e,g. camera – orientation, range, field of view angle) o Locations and zones o Perimeter ranges o Resource tracks o Allow user to zoom in/out on different regions of map graphic
31.	**Video Display** • Shall view live or recorded video from resizable and movable windows • Should have an ability to perform video controls for video systems from workstation • Shall play, fast-forward, rewind, pause, and specify time to play recorded video • Shall take a video still image (snapshot) from live or recorded video • Shall export video for user specified time and duration • Shall have the capability to move PTZ cameras • Shall view Video in Video Matrix

	• Shall display in 1x1, 2x2, 3x3 and 4x4 window formats • Shall enable operator to specify video windows to be displayed in matrix • Shall enable matrix settings to be saved per user • Shall view either live or recorded video can be displayed in the video matrix window. • Shall enable video snapshot to be taken and saved from any window pane in the matrix view • Shall rotate video in "virtual" video guard tour • Shall rotate through multiple video views based on predefined video camera sequence and duration. • Shall enable the user to pause the rotation of video and resume the video rotation again • Shall enable times between new video to be adjusted • Shall enable both live video and recorded video to be played through the video guard tour. • Shall enable alarms to be generated from any video pane • Shall enable user to only view and control video for which they have been assigned permissions by the administrator • Shall manually create an alarm from the live or recorded video with specified severity and description
32.	**Summary Dashboard** • Shall provide alarm summary of each monitoring zone or monitoring area in graphical chart format • Shall display the following charts per global area, monitoring zone or monitoring area • Shall Open Alert Count by Monitoring Zone/Monitoring Area • Shall have the capability of New vs. Viewed (Opened Alerts) • Shall Open Alert Count by Alert Severity • Should have Highest Severity Alert • Shall enable Monitoring Zone or Monitoring area default to Summary view dashboard or to a map when the zone or area is selected.

	• Shall provide a tabular list of sensors in each monitoring are
33.	**Alarm Display** • Shall display real time, dynamic, iconic status of alarm point indications, overlaid onto a computer generated or GIS graphic map of the detection area and zone • Shall display textual alarm description alarm status, severity, activity, operator actions, tasks and procedures, and time/date status. • Shall allow users to view digital video scenes, automatically or manually, related to alarm for both live and recorded video • Shall allow users to handle alarms based on priority • Shall allow users to handle and view multiple alarms in individual windows or in a list • Shall allow users to view alarm notification in system tray • Shall allow users to view alarm notification and alarm summary in alert list window pane • Shall allow users to view alarm notification in the hierarchical tree view • Shall allow users to view alarm in a specific zone and associated with specific sensor on the map • Shall allow users to view a list of alarms associated to a sensor on the map • Shall sort alarms list by o time/date o severity (i.e. highest severity on top) o alarm type o location o alarm source
34.	**Alarm Handling** • Should have an ability to display alarm condition through visual display and audible tone • Should have an ability to simultaneously handle multiple alarms from multiple workstations • Should have an ability to automatically prioritize and display multiple alarms and status conditions according to pre-defined parameters such as alarm type, location, sensor, severity, etc.

	• Should display the highest priority alarm and associated data / video in the queue as default, regardless of the arrival sequence
35.	**Historical Alarm Handling** • Should have an ability to view historical alarms details even after the alarm has been acknowledged or closed. • Should have an ability to sort alarms according to date/time, severity, type, and sensor ID or location.
36.	**Alarm Reporting** • Should have an ability to generate a full incident report of the alarm being generated. • Should have an ability to display report on monitor and print report • Should have details of alarm including o severity, time/date, description and location o Captured video image snapshots o Relevant sensor data such as SCADA sensors o Response instructions o Alarm activities (audit trail) • Should have an ability to export alarm report in various formats including pdf, jpeg, html, txt, and mht formats • Should have an ability to generate an alarm incident package including the full incident report and exported sensor data from the incident in a specific folder location.
37.	**Alarm Policies and Business Logic Administration** • The CCA solution should have the following ability to handle the workflow alarms through graphical user interface. • Should have an ability to match keywords or text from the alarming subsystem's incident description to raise an alarm using criteria including exact match, exact NOT match, contains match, wildcard match and regularly expression match (such as forced door alarm, denied access, door open too long, etc.) • Should have an ability to optionally match alarming subsystem's incident status, incident severity, and sensor type • Should have an ability to apply any alarm policy to one or more monitoring area(s) or zone(s) without having to reapplying the policy multiple times. • Should have an ability to apply any alarm policy to one or more sensors without having to reapply the policy multiple times.

	• Should have an ability to assign specific actions for each alarm • Should have an ability to activate or deactivate alarms as required • Should have an ability to create exceptions • Should Create batch-wise rules and process them • Should Check and rectify logical errors and contradictory rules • Should have an ability to schedule execution of rules • Should Suspend or Terminate the application of rule • Should archive unused or deactivated rules
38.	**Availability, Scalability, Performance and Usability** • The CCA shall be highly available platform.. • The system shall be very tolerant to losses or reduction of communication such that the system shall recover gracefully from such incidents, with no human interaction required. • Should have a high performance and high availability architecture. • Shall be flexible, modular and tolerant to failures/errors and able to exchange information with other systems • The system must have an open architecture such that additional systems when added can be integrated with CCA without upgrades or disruption to other interfaces. • The communications use standard components that are widely available. • Should allow scalability and flexibility to include more applications / solutions in the future • The CCA server shall refresh CCA GUI within 1 second of an incident trigger requiring a change of state in the information in the database. • The CCA server hardware shall be based on high availability, fault tolerant design and capable of operating in mirrored server configuration. • The CCA shall have a resilient processing architecture such that failure of a single component does not affect entire CCA application. • The system shall be able to operate at network bandwidth down to a minimum of 250 kbps. • The system shall be able to operate at network latencies as long as 2 seconds.

Video Wall Cubes	
1.	It should be able to pre-configure and save various display layouts to be accessed at any given point of time with a simple mouse click.
2.	The large screen should provide real-time clear luminous view to share information between operators and decision makers. The operators whose systems are on the same Ethernet should be able to work on the large screen sitting at their own position with their own workstation.
3.	The large screen should be able to show the images of the monitor, which is connected on the LAN with various OS and the windows should be freely resizable, scalable and repositionable on any part of the large video screen.
4.	The large graphics wall shall be consisting of multiple rear projection modules in multiple rows and columns behaving as a single logical screen.
5.	The large screen should be able to show the various applications in the City Management Centre.
6.	The display wall should be rugged and industrial nature and should be able to work in 24/7 environments.
7.	Should have the scalability and upgradeability to be made up of multiple rear projection modules stacked up in rows and columns to achieve a display wall for better viewing ability in linear or curved configuration.
8.	During the useful lifetime of the illumination unit, it should be possible for color and brightness alignment of different projectors to a common target, resulting in a uniform display wall.
9.	The Projector should support Dual link DVI in and Dual link DVI out to have a flicker free image on the Large Screen Graphics Wall.
10.	Each cube shall have its own IP address and on board web server to have the access from a standard web page with status, health and configuration information.
11.	Power consumption for each Visual Display Unit / Rear Projection Modules should be less than 220 watts.
Video wall controller with wall management software	
1.	The software should be able to pre configure various display layouts and access them at any time with a simple mouse click or based on the timer.
2.	The software should enable the users to see the desktop of the graphics display wall remotely on the any WIN 7 PC or above connected with the Display Controller over the Ethernet and change the size and position of the various windows being shown.

3.	The software should enable various operators to access the display wall from the local keyboard and mouse of their WIN 7 or above workstation connected with the Display Controller on the Ethernet.
4.	The software should copy the screen content of the WIN 7 PC / workstation or above connected on the Ethernet with the Display Controller to be shown on the Display wall in scalable and moveable windows in real time environment.
5.	The wall management software should support open APIs to enable system integrators to integrate it with their Software.
6.	Video Wall Control Software should be server client Architecture and have following specifications: a. The Wall Control software should perform health monitoring that allows timely detection of faults. • Wall health • Cube health • Cube IP-address • Brightness b. Wall Control Software should allow commands on wall level or cube level or a selection of cubes : • Switching the entire display wall on or off. • Setting all projection modules to a common brightness target, which can be either static (fixed) or dynamic to always achieve maximum (or minimum) common brightness between projection modules. • Fine-tune color of each cube c. The integrated view should provide a database that • records all incidents • can record full status at given time intervals • can be exported to excel/html • Show internal patterns d. Log file functions (full Audit trail capabilities) should have the following information • Logs are not automatically overwritten • Client logs • Central server logs **e.** Logs should contain the following information • Individual User ID that has control of the video wall at any given time • Name of PC that has control of video wall at any given time. • Time control was taken.

	• Time control was released • Time stamps in log shall be at the one (1) second interval, or less
Video Conferencing software and solution	
7.	Video conferencing systems should be based on ITU's standards and guidelines.
8.	Should be simple user interface with command capabilities.
9.	Should be easy to use, on demand conferencing with always-on virtual meeting rooms Video
10.	One operator should be able to easily manage multiple simultaneous Conferences or several operators can manage one large Conference.
11.	Operators should be able to move participants between Conferences or create sub Conferences for private conversation
12.	The systems should be programmable to facilitate conference set-ups with pre-defined parties using only a few keystrokes.
13.	The systems should support document sharing (PC images, etc.)
14.	The systems should be supplied with a common operational support system that includes browser based system diagnostics.
15.	The systems should support central video server integration for streaming and/or storing sessions.
16.	Should support for various WAN interfaces for ISDN
17.	Should support for IP backplane about 70Gps or higher
18.	Shall have the ability for fast deployment with web-based wizard, tiered administration levels, and automated hardware systems management.
19.	Must offer an option of integration with external media application server for Automatic failover, full redundancy and high scalability.
20.	It should have seamless integration with any Telephony Platforms (Avaya/Cisco/Alcatel-Lucent/or similar/equivalent) for Video Telephony Integration using SIP (Session Initiation Protocol). This includes seamlessly add video to a voice call by simply dialling a voice extension when both endpoints are video-enabled and permits use of unified voice and video dial plan for convenient calling.
21.	The system's WAN ports should be configurable for different speeds depending on applications.
22.	It must be capable to support symmetric 1080p & 720p HD Calls

23.	Video-conferencing equipment should support H.320 (ISDN Video conferencing) as well as H.323 (LAN Video Conferencing) standards. Should support H.261, H.263 & H.263 ++, H.264 Video standards.
24.	Should support 16:9 and 4:3 aspect ratio
25.	Automatic gain control, intelligent audio mixing.
26.	Should support for multiple Video sources like auxiliary camera, VCR, document camera, white board, dual Video should be direct i.e. abilities to send two simultaneous line Video sources e.g. Desktop Video and presenter's Video.
27.	The system should enable users through a remote device at either end to manipulate the camera angle, focus and various parameters to suit the user requirement.
28.	The camera module and microphones should have omni-directional coverage of 360 degrees.
29.	The network interface should support standard ISDN interfaces and protocols and auto Service Profile Identifier (SPID) and switch detection. Services are to be provided in conjunction with standard ISDN
30.	Should have conference dial out and dial in
31.	Should have an advanced IVR flow
32.	Must have support for both message overlay and closed caption
33.	Should have Conference chairperson
34.	Should have customizable GUI
35.	Should have Speaker Notification
36.	Should have user and managed mute control
37.	Should have IVR prompts for auto attendance
38.	Should administrator, operator, auditor, and chairperson views
Contact Centre Solution	
1.	The contact centre solution should be able to route voice/ VOIP calls from centralized Interactive Voice Response System (IVRS) to respective call center (s) along with interaction history of the calling party.
2.	The callers should be able to access the various services through state-of-art centralized integrated Interactive Voice Response System (IVRS). The information is envisaged to be available to the customer through telephone (IVRS) and call centres agents.
3.	The IVRS should establish two way communication on the same channel with customers through recorded synthesized voice in Hindi / English / Regional

	Language or in combination of languages to give information, reply to queries and provide other.
4.	IVRS should be modular and scalable in nature for easy expansion without requiring any change in the software.
5.	It should be possible to access IVRS through any of the access device such as Landline telephone, Mobile phone (GSM as well as CDMA) etc.
6.	IVRS should support various means of Alarm indications in case of system failures, e.g. Functional error, missing voice message prompt, etc., and shall generate error Logs.
7.	The system should have the ability to define business rules based upon which the system should quickly identify, classify and prioritize callers, and using sophisticated routing, to deliver interactions to the best qualified agent in the any of the connected local/remote call centre, regardless of interaction channel
8.	The application should provide CTI services such as: • Automatic display (screen pop) of information concerning a user/customer on the call agent screen prior to taking the call based on ANI, DNIS or IVR data. • Synchronized transfer of the data and the call to the call centre agent. • Transfer of data corresponding to any query raised by any IP agent regarding a query raised by a customer whose call is being attended by the call IP agent. • Call routing facilities such as business rule based routing, skills-based routing etc.
9.	The application should support integration to leading CTI middleware vendors.
10.	Should provide pre-integration with industry standard IVR servers and enhance routing & screen-pop by passing forward the information.
11.	Should provide facilities for outbound calling list management, and software based predictive or preview dialling.
12.	The application should allow service level plans to be varied by day, time of day, or a specific date.
13.	**Call Centre Agent's Desktop: The agents desktop shall have an application which shall fulfil the following functionalities :** • It should provide consistent agent interface across multiple media types like fax, SMS, telephone, email, and web call back. • The agent's desktop should have a "soft-phone" – an application that enables standard telephony functions through a GUI. • It should provide the agents with a help-desk functionality to guide the agents to answer a specific query intelligently. • It should also provide an easy access to agents to previous similar query which was answered successfully. • It should also be possible to identify a request to be a similar request made

	earlier. • It should be possible for agents to mark a query as complex/typical and put in to database for future reference by other agents. • It should be possible for agents to escalate the query.
14.	System should be able to integrate with e–mail / sms gateway so that appropriate messages can be sent to the relevant stakeholders after the interaction and any updates thereon.
15.	Should intelligently and automatically responds to email inquiries or routes inquires with skills based routing discipline to agents
16.	Should have an Intelligent distribution of email to agents
17.	**CTI Application Requirements** • The CTI link should allow a computer application to acquire control of the agent resources on the IP EPABX & change state of the agent phone through commands on the CTI link. • The CTI link should pass events & information of agent states & changes in agent states as well as incoming calls to the computer applications. • The CTI link should allow a computer application to take control of the call flow inside the IP EPABX & also allow the computer application to decide the most suitable action / agent for an incoming call.
18.	**Automatic Call Distribution (ACD) Requirements** • The ACD solution should be able to route the call to any remote call center agent using IP phones • Should have an ability to queue or hold the call for an agent if none is immediately available. • Should have an ability to keep the callers informed as to the status of the call and providing information to callers while they wait in queue. • System should be able to perform prioritized call routing
19.	**Supervisor Module** The call centre should provide a graphical console application program for the supervisor's workstation. This position shall facilitate the following features:- • Any supervisor shall be able to monitor or control any group in the call Centre. • It shall show the live activity of each agent in details as well as in a summarized fashion including information like total number of calls received, calls answered, average response time etc. • The Supervisor console shall also graphically display live status of the call session summary, number of call waiting in the queue, call traffic etc. • Live status of the group shall be shown, including waiting calls and calls being answered currently. • Access to the supervisor console shall be restricted. • It shall be possible for a supervisor to attend calls whenever necessary.

20.	Should have a comprehensive audit trail detailing every user activity including system/security administrators with before and after image

6.2 Backup / Achieved / Replication Software

Backup Solution

#	Description
1.	The proposed backup solution shall have same GUI across heterogeneous platform to ensure easy administration and available on various OS platforms such as Windows, Linux and UNIX platforms and be capable of supporting backup/ restores from various supported platforms.
2.	Backup Solution should have ability to backup data from one server platform and restore it to another server platform to eliminate dependence on a particular machine and for disaster recovery purposes.
3.	Backup Solution should support various level of backups including full, incremental, and user driven backup along with various retention period.
4.	Backup clients should be updated automatically using the client push feature
5.	Backup should support agentless backup for virtualization platform with non-staged granular recovery.
6.	Backup Software should support intelligent policy for virtualization.
7.	Backup Software must provide Source (Client & Media Server) & Target base data Deduplication capabilities.
8.	Backup Solution should Integrate with third party VTL, NAS, SAN which has data deduplication capabilities and Robotic/automated Tape library
9.	Backup Solution must have Wizard-driven configuration and modifications for backup, restoration and devices.
10.	The proposed backup solution shall have in-built frequency and calendar based scheduling system.
11.	Backup Solution must have Optimized way for data movement from client to disk target.
12.	Backup Solution should support (inflight & at rest) encryption.
13.	The proposed backup solution shall support tape mirroring of the same job running concurrently with primary backup.
14.	The proposed backup solution shall allow creating tape clone facility after the backup process.
15.	Backup Solution should have Capability to do trend analysis for capacity planning of backup environment.
16.	The proposed Backup Solution must offer capacity-based licensing. The license should be for the front-end capacity rather than back-end. There should be no incremental cost associated with longer retention periods.
17.	The solution should not require purchase of additional licenses for DR sites (copies of original data), also should not require purchase of additional licenses for replication to DR sites.
18.	The proposed backup dedupe license should be independent of hardware so replacing hardware should not incur new software license cost.
19	The proposed backup solution must include Agent/Modules for online backup of files, applications and databases such as MS SQL, Oracle, DB2, Sybase, Exchange, Sharepoint and File share backup(SMB)

20	The proposed backup solution should provide recovery from physical servers to Virtual and image level recovery.
21	The proposed backup solution should have Cloud plug-ins for backup data replication.
22	Backup Solution should have Inbuilt feature for extensive alerting and reporting with pre-configured and customizable formats.
23	Backup Replication at DR site, Cloud. Replication license should be included as part of solutions.
24	Backup software should support multiplexing and multistreaming and shall support the capability to write up to Min 32 data streams.
25	Backup Solutions should have capabilities to tape/disk out backup catalog and deduplication catalog.
26	Backup solution should have integrated data de-duplication engine with multi-vendor storage support to save de-duplication data. The de-duplication engine should also facilitate IP base replication of de-dupe data; without any extra charge.
27	The Proposed Backup solution must restore files, emails and other granular items from Microsoft Exchange, SharePoint, and Active Directory and for hypervisors such as VMware and Microsoft Hyper-V from a single-pass backup.
28	Backup solution must Support Backups/Restores for 1) Clustered servers (Industry popular clusters). 2) Virtual platform. 3) RAW SCSI volumes. 4) Block based backup & restore simultaneously.

Archival Solution

#	Description
1.	The solution must be capable of archiving content from multiple sources like messaging including MS Exchange, Domino File Servers , MS Sharepoint, VOIP etc
2.	The proposed solution must have integration with Email solution through SMTP archiving without the need of any additional hardware.
3.	The solution should have the capability to archive data from multiple electronic repository to single repository to achieve best single instance across multiple frontend source data.
4.	The solution must support a Single unified console to manage archiving from different sources like File server, sharepoint, Mailing solution etc
5.	The solution should provision a web based discovery mechanism to search relevant data across archives from multiple sources like file server, messaging, Sharepoint etc. The discovery mechanism should support a guided, hierarchal review of searched data with capability to filter, marking and legal hold to prevent deletion/expiry.
6.	The solution should facilitate a supervision mechanism for emails to ensure compliance of messaging content. The supervision mechanism should facilitate sampling of messages and subsequent review by authorized personnel
7.	The solution should support tagging of messages by message security solutions like anti-spam/anti-virus for efficient retention
8.	Proposed solution must support outlook on Windows & MAC machines.
9.	Archival solution must have support with IMAP compliant devices to access the emails.
10.	Proposed solution should support archiving both at premises and cloud.
11.	Proposed solution must have monitoring integration with messaging solution vendor.

12.	The solution should support Message Journaling as well as Envelope Journaling, capture BCC data and expansion of distribution lists
13.	The solution must support "Agentless" archiving of messages. There should be no need to deploy any agent on the messaging server.
14.	The solution must support search for mails based on undisclosed recipients criteria
15.	The solution should support seamless access using shortcuts from the native email client as well as browser based client. The solution should support all archiving actions like manually archive, search, restore, retrieve, delete from the native email client and browser based client
16.	The solution should support archiving based on either any or a combination of the following criteria: - Item Type (message, calendar etc.) - Date - Size - Email Attachment only - User - Organizational Unit
17.	Proposed solution must have advance way of archive disk/partition data backup to avoid backup of old partitions which must be possible with or without WORM devices.
18.	The solution must allow the administrators to configure the following in shortcuts: - Include recipient information in the shortcuts. - Include nothing / original message body / custom message body in shortcuts. - Include "X" number of characters in the shortcut. - Include a custom body defined from a configuration file in the shortcut etc.
19	The solution should leave a shortcut at either the time of archiving or later as well.
20	The solution should allow users to view archived items directly without having the need to restore them to the messaging server to avoid delays and impact on messaging solution. No network connections should be established between archiving server and messaging server at the time of retrieving archived items
21	The solution must support indexing and archiving of minimum 500+ commonly used file types.
22	The solution should support archiving of entire email folders and application of selective archiving policies based upon folders.
23	The solution must support dynamic retention period of archived items i.e. retention of archived items can be increased or decreased on fly.
24	The solution should facilitate "future proofing" of content by facilitating an HTML copy for long term retention and search
25	The solution should support "safety copies" of items to be kept on the mail server. The "safety copy" allows the archiving software to wait for the archived item to be backed up or replicated before the original item is removed from the mail server.
26	Archival solution must have option to set or configure disk property read and read-write access
27	Archival solution must have disk configurable option with High & Low watermark. In case, High watermark reaches, disk should automatically become Read only and other pre-configured disk should get read-write access to store fresh archived items.
28	The solution must have OWA integration in such a fashion that archived item can be browsed directly through archived browser tab instead of browsing through internet explorer (IE). IE can be additional feature.
29	The archival solution must have an integrated e-discovery solution which allows guided Discovery, review and analysis of data from the archives and non-archived data like desktop, sharepoint, file server, Documentum etc. It's required for future proofing.

30	Proposed Archival solution must have seamless and consistent end user search experience across multiple interface like Desktop/Laptop, mobile, tablets etc.

Replication Solution

#	Description
1	The proposed architecture should ensure that in event of Disaster at Primary Site, applications can be restarted at DR Site without any data loss.
2	The proposed architecture should focus on not only the data replication, but ensuring application availability with zero data loss at DR site.
3	The proposed solution must optimize additional infrastructure and storage resources in the architecture.
4	The proposed solution should be a storage agnostic solution. The solution should not only seamlessly integrate with current infrastructure, but also not impose any restriction on storage or platform technology that BSCDCL may deploy in future.
5	The proposed software must provide comprehensive hardware and platform support. Support for physical and virtual platforms, including Solaris, AIX, HP-UX, Linux, Windows, VMware, and KVM.
6	The proposed software should provide application level availability by ensuring that it not only replicates data within database but also structural changes to databases, application and database binaries etc. without any manual intervention.
7	Application high availability at primary & DR site should not be dependent on Operating system event logs. Solution should be capable to integrate directly with application start, stop and monitor service to avoid outage remedy solution because of Operating system log.
8	The proposed software should support real time tracking of configuration changes being done to Operating system, application binaries, any tunable added/modified etc. and alert administrators in case of configuration drift between primary and DR site.
9	Shall be able to handle long outages of network without affecting the consistency of data at secondary site. The replication solution should be provisioned for storing data for at least 4 days in case network is down for extended period.
10	The proposed software should provide for an automated fire-drill for testing of DR site. The testing mechanism should automatically validate the application startup at DR site at a pre-defined schedule defined.
11	The proposed software should provide availability across any distance—Builds local metropolitan and wide-area clusters for disaster recovery and local availability.
12	The proposed software should ensure no single point of failure. It has the ability to gracefully move an application to an available server in the event of a failure and coordinate the movement with storage ownership.
13	The proposed software should provide Multi-cluster management and reporting, including applications composed of multiple components running on different physical and virtual tiers, adding resilience to business services. Manages and reports on multiple local and remote clusters from a single unified web-based console.
14	The proposed software should provide seamless integration with Oracle, Exchange, SQL, SharePoint, and major applications/databases for increased application performance and availability.
15	It should also have the integration with replication technologies such as EMC SRDF/Mirrorview, Hitachi TrueCopy, IBM MetroMirror, Oracle DataGuard, Veritas Replicator, etc.

16	The proposed software should provide advanced application failover logic to ensure that application uptime is maximized, server resources are efficiently utilized, and detect failures faster than traditional clustering solutions and requires almost no CPU overhead
17	The proposed software should provide advanced clustering support for virtual machine architectures.
18	The proposed software should be simple to install, configure, and maintain. It should provide powerful wizards that enable simple, quick, and error-free setup of advanced, high availability, disaster recovery, and Fire Drill configurations.
19	The proposed software must be able to provide comprehensive insight into the storage environment, enabling improved usage and efficiency across all major operating systems, including Oracle Solaris, HP-UX, IBM AIX, Red Hat Enterprise Linux, SUSE Linux, Oracle Enterprise Linux (RHEL compatible mode), and Microsoft Windows, and storage hardware, including EMC, HDS, IBM, NetApp, HP, Dell Compellant, and more.
20	The proposed software should have deduplication and compression to reduce the primary storage footprint.
21	The proposed software should support automated storage tiering to seamlessly and transparently move data based on business value
22	The proposed software should have the ability to make data compatible between operating systems for simplified OS migration.
23	The proposed software should be able to support physical environment. It should support virtual disks in VMDK/VMFS format, and as well as RDM.
24	The proposed solution should have multi-pathing feature for I/O path availability and performance to efficiently spread I/Os across multiple paths for maximum performance, path failure protection, and fast failover.
25	Host Replication should be certified for performing replication to heterogeneous storage models from different OEMs (HP, IBM, EMC, SUN and Netapp)
26	The Host Replication technology should support different types of data whether structured or unstructured.
27	The proposed host base replication solution should be capable of maintaining data consistency at all times.

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 (minimum 10 users) of BSCDCL.

MSI will implement dedicated EMS solution to meet the SLA monitoring and other requirements as mentioned in the RFP. The implemented EMS solution to help BSCDCL in data driven decision making. In case the MSI uses any OEM product(s), the implementation should be as per best practices of the OEM. BSCDCL may engage STQC/other independent auditors for validating the deployment of EMS facilities as per RFP requirements, specially their capabilities for measuring and reporting SLAs & KPIs as defined in RFP. The entire EMS implementation shall be certified by the MSI also for its correctness, adequacy to meet RFP requirements and measurement of SLAs & KPIs etc. Various key components of the EMS are:

- SLA & Contract management System
- Network Monitoring System

- Server Monitoring System
- Helpdesk System
- Application Performance Management

Proposed EMS Solution shall be based on industry standard best practice framework such as ITIL etc. 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 BSCDCL to capture all the System based SLAs defined in this Tender and then calculate quarterly (or for any duration) penalty automatically. Measuring service performance requires incorporation of a wide variety of data sources of the ICCC project. The SLA solution should support the collection data from various sources in order to calculate Uptime / Performance / Security SLAs. Various features required in this component to EMS are -

- It must be a centralized monitoring solution for all IT assets (including servers, network equipment etc.)
- The solution must have integrated dashboard providing view of non performing components / issues with related to service on any active components
- The solution must follow governance, compliance and content validations to improve standardisation of service level contracts
- Application should be pre-configured so as to allow the users to generate timely reports on the SLAs on various parameters.
- The solution must support Service Level Agreements & Lifecycle Management including Version Control, Status Control, Effectively and audit Trail to ensure accountability for the project.
- The solution must have the ability to define and calculate key performance indicators from an End to End Business Service delivery perspective related to ICCC Project under discussion.
- The solution should support requirements of the auditors requiring technical audit of the whole system which MSI should allow the auditors to access the system.
- The solution most have an integrated dashboard, view of Contract Parties & current SLA delivery levels and view of Services & current SLA performance
- The solution should support SLA Alerts escalation and approval process.
- Solution should support effective root-cause analysis, support capabilities for investigating the root causes of failed service levels and must make it possible to find the underlying events that cause the service level contract to fail.
- Accept Data from a variety of formats.
- Support for Defining and Calculating service Credit and Penalty based on clauses in SLAs.

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 CCC should allow users to define benchmarks against performance parameters. Performance reports shall have the option to generate reports with or without benchmark comparison.
- The CCC 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 CCC 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 CCC 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 behaviour, trends, log analytics and performance to enhance customer experience across various channels
- The solution must provide rapid analysis where crash analytics and video session playback allows for rapid analysis and repair to deliver seamless user interactions
- The solution must provide operational efficiency capabilities that provide insight of app performance by version, carrier, geo, OS, network, real-time alerts on threshold violations impacting SLAs and prioritize alerts based on impact to business, revenue and gain end-to-end visibility into the mobile infrastructure.
- The solution must provide complete Insights into Application Flows, Heat Maps & Crash to enable improving the UI design, understand user interactions, build functionality based on real user data and create product & services differentiation.

6.4 Software Defined Security (SDS) for Applications /Services

#	Parameter and Minimum Specifications
1	The Proposed solution should have the ability to provide native application isolation and on-demand creation of security groups based on existing security policies.
2	The proposed Solution Architecture should Firewall any inter VM communication / Traffic. This Inter VM Firewalling within the same VLAN / Application Tier should not burden the Intranet Firewall but should be done closer to the Application inside the Host.
3	The proposed Firewall should be in Software Form factor and can be either present in the Virtualization/ Hypervisor layer or as a Virtual Machine in every Physical Host as agentless mode. It should preferably offer throughput of over 10Gbps Per Physical Host/Server/Blade.
4	The proposed solution should get managed from a centralized console and should be integrated with the Centralized Virtualization console for an easy and common Operational mode with that of the Virtual Machine.
5	Automated Security Policy Management - The Security Policy should be tied with each Virtual Machine and the Policy should automatically move with the movement of the Virtual Machine, thus bring Security Policy Portability along with the VM motion.
6	The solution shall provide inspection firewall that can be applied at the virtual network interface card level directly in front of specific workloads thus creating capability of Application isolation for Risk/Breach containment.
7	The solution should offer to Integrate with industry-leading solutions for antivirus, malware, intrusion prevention, and next-gen security services through Security Service Chaining
8	The solution should have the capability of creating unique Security Groups of the VMs based on Operating Systems, Workload Type (Web, App or DB), Machine Name, Services running, Regulatory requirement etc. and apply Automated and Centralized Security Policy based on this context or grouping.

6.5 Virtualization Software

#	Parameter	Minimum Specification
1.	Solution	Sits directly on the server hardware with no dependence on a general purpose OS for greater reliability and security.
2.	Guest OS Support	Windows client, Windows Server, Linux (at least Red Hat, SUSE, Ubuntu and CentOS, Solaris x86) etc.
3.	VM Capability	Create Virtual machines with up to 128 virtual processors, 6 TB virtual RAM and 2GB Video memory in virtual machines for all the guest operating system supported by the hypervisor.
4.	VM Live Migration	Live Virtual Machine migration between different generations of CPUs in the same cluster and without the need for shared storage option and between servers in a cluster, across clusters as well as long distances from one site to another (up to 150 milliseconds round trip time) with no disruption to users or loss of services, eliminating the need to schedule application downtime or business downtime.
5.	Storage Live Migration	Live migration of VM disk from one storage array to another without any VM downtime. Support this migration from one storage protocol to another eg: FC, NFS, iSCSI, DAS.
6.	High Availability	Proactive High availability capability that utilizes server health information and migrates VMs from degraded hosts before problem occurs.
7.	Always Available	Zero downtime, Zero data loss and continuous availability for the applications running in virtual machines in the event of physical host failure, without the cost and complexity of traditional hardware or software clustering solutions.
8.	Resource Addition	Add CPU, Memory & devices to virtual machines on the fly when needed, without disruption or downtime of working VMs for both windows and Linux based VMs.
9.	Resource Scheduler	Dynamically allocate and balance computing capacity across collections of hardware resources aggregated into one unified resource pool with optional control over movement of virtual machines like restricting VMs to run on selected physical hosts. Create a cluster out of multiple storage datastores and automate load balancing by using storage characteristics to determine the best place for a virtual machine's data to reside, both when it is created and when it is used over time.
10.	Security	VM-level encryption with no modifications in guest OS to protects unauthorized data access both at-rest and in-motion and also provides secure boot for protection for both the hypervisor and guest operating system by ensuring images have not been tampered with and preventing loading of unauthorized components. Integration of 3rd party endpoint security to secure the virtual machines with offloaded Firewall and HIPS solutions without the need for agents inside the virtual machines from day 1.

11.	Storage support	Support boot from iSCSI, FCoE, and Fibre Channel SAN. Integrate with NAS, FC, FCoE and iSCSI SAN and infrastructure from leading vendors leveraging high performance shared storage to centralize virtual machine file storage for greater manageability, flexibility and availability. Virtual Volumes which enables abstraction for external storage (SAN and NAS) devices making them Virtualization aware. Integration with Storage API's providing integration with supported third-party data protection, multi-pathing and disk array solutions.
12.	Virtual Switch	Span across a virtual datacenter and multiple hosts should be able to connect to it. This will simplify and enhance virtual-machine networking in virtualized environments and enables those environments to use third-party distributed virtual switches. In-built enhanced host-level packet capture tool which will provide functionalities like SPAN, RSPAN, ERSPAN and will capture traffic at uplink, virtual switch port and virtual NIC level. It should also be able to capture dropped packets and trace the path of a packet with time stamp details. “Latency Sensitivity” setting in a VM that can be tuned to help reduce virtual machine latency. Link aggregation feature in the virtual switch which will provide choice in hashing algorithms on which link aggregation in decided and this should also provide multiple link aggregation groups to be provided in a single host.
13.	VM based Replication	Efficient array-agnostic replication of virtual machine data over the LAN or WAN. This Replication should simplify management enabling replication at the virtual machine level and enabling RPOs as low as 15 minutes.
14.	VM Backup	Simple and cost effective backup and recovery for virtual machines which should allow admins to back up virtual machine data to disk without the need of agents and this backup solution should have built-in variable length de-duplication capability.
15.	I/O Control	Prioritize storage access by continuously monitoring I/O load of storage volume and dynamically allocate available I/O resources to virtual machines according to needs. Prioritize network access by continuously monitoring I/O load over network and dynamically allocate available I/O resources to virtual machines according to needs.
16.	OEM Support	Direct OEM 24x7x365 days with unlimited incident support and 30mins or less response time including the unlimited upgrades and updates. And should be Leaders in the Gartner's Magic Quadrant for at least last 5 years.

7. Annexure II-Technical Specifications

Technical Specification provided under are indicative, bidder carefully examine the requirements and may propose technical specification / design as per their solution to meet the objective of RFP.

7.1 Multi-Function Laser Printer

#	Parameter	Minimum Specifications
1.	Technology	Laser
2.	Monthly duty cycle/RMPV (pages)	200,000/5K-20K
3.	Print speed – simplex (A4)	Up to 41 ppm
4.	Scan speed – Black/Color simplex	Up to 50/30 ipm
5.	Scan speed – Black/Color duplex	Up to19/14 ipm
6.	Scan-to destinations	Email, Network folder, USB
7.	Processor (MHz)	600
8.	Memory (MB)	1,024
9.	Hard disk drive (HDD)/Capacity (GB)	Yes/240
10.	Connectivity	2 Hi-Speed USB 2.0; 1 Gigabit Ethernet 10/100/1000T network
11.	Print resolution – Max/Best print quality (dpi)	Up to 1200x1200
12.	Input capacity – Std/Max (sheets)	600/4,600
13.	Output size – Min/ Max (mm)	76.2 x127/312x469.9
14.	Automatic duplex	Yes
15.	Energy Efficiency	BEE or Energy Star certified
16.	Control panel display	20 m touchscreen

7.2 Laser Printer

#	Parameter	Minimum Specifications
1.	Print speed black (normal, A4)	Up to 25 ppm
2.	Print quality black (best):	Up to 1200 x 1200 dpi
3.	Print technology :	Monochrome Laser
4.	Duty cycle (monthly, A4)	Up to 15,000 pages
5.	Recommended monthly page	volume 250 to 2000

#	Parameter	Minimum Specifications
6.	Standard memory:	Minimum 128 MB
7.	Processor speed:	Minimum 700 MHz
8.	Paper handling standard/input	Up to 250-sheet input tray
9.	Paper handling standard/output	Up to 150-sheet output bin
10.	Media sizes supported	A4, A5, A6, B5, postcard
11.	Media types supported	Paper, transparencies, postcards, envelopes, labels
12.	Standard connectivity	Hi-Speed USB 2.0 port with USB data cable, Ethernet with RJ45 connectivity
13.	Duplex printing	Automatic (standard)
14.	Compatible operating systems	Microsoft Windows 7 Professional(64bit), Windows 8 Pro(64 bit), Windows 8.1, Windows 10, Server 2008 R2, Server 2012 R2, MAC OS 9.0, MAC OS X, Linux
15.	Power requirements:	Input voltage 220 to 240 VAC (+/- 10%), 50 Hz (+/- 2 Hz);
16.	Power consumption during printing	Less than 500W
17.	Energy Efficiency	BEE or Energy Star certified
18.	Front operating Panel	Graphical LCD display

7.3 Video Wall

The minimal specifications of video wall cubes are as below -

- The native resolution of each Visual Display Unit / Rear Projection Module should be 1920 X 1080 pixels (Full HD) and should offer min 16.7 million colors.
- The Light source lifetime of LED should be 80,000 hrs.(Eco)
- The brightness uniformity should be > 90%.
- The contrast shall be 1500:1 or higher.
- The Aspect Ratio of each of projection module should be 16:9.
- The screen should have adjustable low inter screen gap 0.2 mm to give seamless viewing experience.

7.4 Workstations (Desktop Computer)

#	Parameter	Minimum Specifications
1.	Processor	Latest generation 64bit X86 Quad core processor(3Ghz) or better
2.	Chipset	Latest series 64bit Chipset
3.	Motherboard	OEM Motherboard
4.	RAM	Minimum 8 GB DDR3 Memory @ 1600 Mhz. Slots should be free for future upgrade

#	Parameter	Minimum Specifications
5.	Graphics card	Minimum Graphics card with 2 GB video memory (non-shared)
6.	HDD	2 TB SATA-3 Hard drive @7200 rpm
7.	Media Drive	NO CD / DVD Drive
8.	Network interface	10/100/1000 Mbps autosensing on board integrated RJ-45 Ethernet port.
9.	Audio	Line/Mic IN, Line-out/Spr Out (3.5 mm)
10.	Ports	Minimum 6 USB ports (out of that 2 in front)
11.	Keyboard	104 keys minimum OEM keyboard
12.	Mouse	2 button optical scroll mouse (USB)
13.	Monitor	Min. 22" (*or 21.5"*) TFT LED monitor, Minimum 1920 x1080 resolution, 5 ms or better response time, TCO 05 (or higher) certified For Command Control Centers : 2 LED Monitors *attached to the same workstation (multi monitor)*
14.	Certification	Energy star 5.0/BEE star certified
15.	Operating System	64 bit pre-loaded OS with recovery disc
16.	Security	BIOS controlled electro-mechanical internal chassis lock for the system.
17.	Antivirus feature	Advanced antivirus, antispyware, desktop firewall, intrusion prevention (comprising of a single, deployable agent) which can be managed by a central server. (Support, updates, patches and errata for the entire contract/ project period)
18.	Power supply	SMPS;. Power supply should be 90% efficient with EPEAT Gold certification for the system.

7.5 Television Set (Meeting room)

- 46 Inch Full HD LED

7.6 Projector

#	Item	Minimum Specifications
1.	Display Technology	Poly-silicon TFT LCD
2.	Resolution	HD 1080p
3.	Colours	16.7 million Colours
4.	Brightness	2500 or more ANSI lumens (in Normal Mode)
5.	Contrast Ratio	2000:1 or more

6.	Video Input	One computer (D-Sub, Standard 15 pin VGA connector) One S-Video One HDMI
7.	Audio	Internal speaker
8.	Output ports	External Computer Monitor port, audio ports
9.	Remote Operations	Full function Infrared Remote Control
10.	Other features	Auto source detect, Auto-synchronisation, Keystone Correction

7.7 IP PABX System

#	Description	Parameter
1.	Technology	PCM-TDM , IP, Non-blocking
2.	Interface	Should support all telecom interfaces in Indian Telecom Service provider offerings
3.	Type of Interface	ISDN interface for digital, basic interface for Analog lines
4.	No. of lines - ,ISDN PRI lines & Analog / Digital Extensions	1 PRI from BSNL, 32 Extensions (IP / Analog / Digital)
5.	Type of Extension Support	Analog , Digital and IP
6.	Expansion of Extensions	Multiples of 8 / 16
7.	Run Distance	Not less than 800 mtrs. on 0.5mm dia. Cable
8.	Max. Loop resistance for analog trunk lines Extensions	2500 ohms including telephone
9.	Requirement at the time of supply	01 ISDN PRI, 24 Analog Ports & 8 Digital extension ports.. Expected to handle at least 30 external lines.
10.	Contact center Expansion available (Max. capacity)	It must support at least 16 Call center Agents

#	Description	Parameter
11.	Max. loop resistance for analog trunk lines	1200 ohms at –48 Volts DC
12.	Other	• ISDN supplementary services for Digital phone • Support for digital trunk lines • Working on 230v AC mains and DC voltage • Support for ACD call center with CTI and advanced call routing
13.	Design of EPABX System	Modular with universal slots, wall mountable
14.	Conferencing	5 party conferencing to be provided (to be configurable dynamically)
15.	Digital / IP Extension telephone instrument with programmable one touch keys	

7.8 Civil Work, Safety Instrumentation and Furniture (at command center)

a. False Ceiling

- Providing and fixing metal false ceiling with powder coated 0.5mm thick hot dipped galvanized steel tiles 595 x 595 mm with regular edge (10mm) suitable for 25mm grid supported on suitable powder coated galvanized steel grid as per manufacturer specification. The same shall be inclusive of cut outs for lighting, AC grills, Fire detectors, nozzles, etc.
- Providing and fixing 12 mm thick fire line Gypsum false ceiling and lighting troughs 300 mm as per design including 100 mm high cornices as lighting pelmets on G.I. frame work, in G.I. vertical supports at every 450mm c/c and horizontal runners at every 900mm c/c self-taping metal screws to proper line and level. The same shall be inclusive of making holes and required framing for fixing electrical fixtures, A.C. grills etc. GI vertical supports to be anchored to slab by means of anchor fasteners.

b. Furniture and Fixture

- Workstation size of min. 18" depth made with 1.5mm thick laminate of standard make over 18mm thick commercial board complete with wooden beading including cutting holes & fixing of cable manager etc. complete with French polish. Edges shall be factory post-formed. The desk shall have the necessary drawers, keyboard trays, cabinets etc. along with sliding / opening as per approved design with quality drawer slides, hinges, locks etc.

- Providing & making of storage unit with 18 mm thick MDF board along with 1.5 mm approved laminate colour outside and 2 coat of enamel paint inside the storage of size 1'6"x1'6"x2'4". The same should be provided with all the required accessories including the handle, lock, sliding channel and necessary hardware, etc. complete with French polish
- Cabin table of min. depth 2' made with 1.5mm thick laminate of standard make over 19mm thick commercial board complete with wooden beading including cutting holes & fixing of cable manager etc. complete with French polish.
- Providing, making & fixing 6" high laminated strip using 1.5mm thick laminate over 10mm thick commercial board on all vertical surface in the entire server & ancillary areas including low height partition, brick wall, partition wall, cladding etc. complete with French polish in all respect.
- Providing, making & fixing an enclosure for gas cylinder of Shutters and Partitions along with wooden support and 18 mm thick MDF board along with 1.5 mm approved laminate colour outside and 2 coat of enamel paint inside the shutter. The same should be provided with all the required accessories including the handle, lock, loaded hinges, tower bolt and necessary hardware etc. complete with French polish.

c. Partitions (wherever required as per approved drawing)

- Providing and fixing in position full height partition wall of 125 mm thick fire line gyp-board partition using 12.5 mm thick double fire line gyp-board on both sides with GI steel metal vertical stud frame of size 75 mm fixed in the floor and ceiling channels of 75 mm wide to provide a strong partition. Glass wool insulation inside shall be provided as required. Fixing is by self-tapping screw with vertical studs being at 610 mm intervals. The same should be inclusive of making cut-outs for switch board, sockets, grill etc. It shall also include preparing the surface smoothly and all as per manufacture's specification etc. finally finishing with one coat of approved brand of fire resistant coating.
- With glazing including the framework of 4" x 2" powder coated aluminium section complete (in areas like partition between server room & other auxiliary areas).
- Providing & fixing Fire Rated Wire Glass minimum 6 mm thick for all glazing in the partition wall complete. (External windows not included in this).
- All doors should be minimum 1200 mm (4 ft.) wide.

d. Painting

- Providing and applying Fire retardant paint of pre-approved make and shade to give an even shade over a primer coat as per manufacturers' recommendations after applying painting putty to level and plumb and finishing with 2 coats of fire retardant paint. Base coating shall be as per manufacturer's recommendation for coverage of paint.
- For all vertical Plain surface.
- For fire line gyp-board ceiling.
- Providing and laying POP punning over cement plaster in perfect line and level with thickness of 10 - 12 mm including making good chases, grooves, edge banding, scaffolding pockets etc.

- Applying approved fire retardant coating on all vertical surfaces, furniture etc. as per manufacturer's specification.

e. Steel Conduit

- All sections of conduit and relevant boxes shall be properly cleaned and glued using appropriate epoxy resin glue and the proper connecting pieces, like conduit fittings such as Mild Steel and should be so installed that they can remain accessible for existing cable or the installing of the additional cables.
- No conduit less than 20mm external diameter shall be used. Conduit runs shall be so arranged that the cables connected to separate main circuits shall be enclosed in separate conduits, and that all lead and return wire of each circuit shall be run to the same circuit.
- All conduits shall be smooth in bore, true in size and all ends where conduits are cut shall be carefully made true and all sharp edges trimmed. All joints between lengths of conduit or between conduit and fittings boxes shall be pushed firmly together and glued properly.
- All electrical wiring should be done as per CPWD specifications.

- The chase in the wall required in the recessed conduit system shall be neatly made and shall be of angle dimensions to permit the conduit to be fixed in the manner desired. Conduit in chase shall be hold by steel hooks of approved design of 60cm center the chases shall be filled up neatly after erection of conduit and brought to the original finish of the wall with cement concrete mixture 1:3:6 using 6mm thick stone aggregate and course sand.

f. Wiring

- PVC insulated copper conductor cable shall be used for sub circuit runs from the distribution boards to the points and shall be pulled into conduits. They shall be stranded copper conductors with thermoplastic insulation of 650 / 1100 volts grade. Colour code for wiring shall be followed.
- Looping system of wring shall be used, wires shall not be jointed. No reduction of strands is permitted at terminations.
- Wherever wiring is run through trunking or raceways, the wires emerging from individual distributions shall be bunched together with cable straps at required regular intervals. Identification ferrules indication the circuit and D.B. number shall be used for sub main, sub circuit wiring the ferrules shall be provided at both end of each sub main and sub-circuit.
- Where, single phase circuits are supplied from a three phase and a neutral distribution board, no conduit shall contain wiring fed from more than one phase in any one room in the premises, where all or part of the electrical load consists of lights, fans and/or other single phase current consuming devices, all shall be connected to the same phase of the supply.
- Circuits fed from distinct sources of supply or from different distribution boards or M.C.B.s shall not be bunched in one conduit. In large areas and other situations where the load is divided between two or three phases, no two single-phase switches connected to difference phase shall be mounted within two meters of each other.
- All splicing shall be done by means of terminal blocks or connectors and no twisting connection between conductors shall be allowed.

- Metal clad sockets shall be of die cast non-corroding zinc alloy and deeply recessed contact tubes. Visible scraping type earth terminal shall be provided. Socket shall have push on protective cap.
- All power sockets shall be piano type with associate's switch of same capacity. Switch and socket shall be enclosed in a M. S. sheet steel enclosure with the operating knob projecting. Entire assembly shall be suitable for wall mounting with Bakelite be connected on the live wire and neutrals of each circuit shall be continuous everywhere having no fuse or switch installed in the line excepting at the main panels and boards. Each power plug shall be connected to each separate and individual circuit unless specified otherwise. The power wiring shall be kept separate and distinct from lighting and fan wiring. Switch and socket for light and power shall be separate units and not combined one.
- Balancing of circuits in three phases installed shall be arranged before installation is taken up. Unless otherwise specified not more than ten light points shall be grouped on one circuit and the load per circuit shall not exceed 1000 watts.

g. Earthing

- All electrical components are to be earthen by connecting two earth tapes from the frame of the component ring and will be connected via several earth electrodes. The cable arm will be earthen through the cable glands. Earthling shall be in conformity with provision of rules 32, 61, 62, 67 & 68 of Indian Electricity rules 1956 and as per IS-3043. The entire applicable IT infrastructure in the Control Rooms shall be earthed.

- Earthing should be done for the entire power system and provisioning should be there to earth UPS systems, Power distribution units, and AC units etc. so as to avoid a ground differential. State shall provide the necessary space required to prepare the earthing pits.
- All metallic objects on the premises that are likely to be energized by electric currents should be effectively grounded.
- The connection to the earth or the electrode system should have sufficient low resistance in the range of 0 to 25 ohm to ensure prompt operation of respective protective devices in event of a ground fault, to provide the required safety from an electric shock to personnel & protect the equipment from voltage gradients which are likely to damage the equipment.
- Recommended levels for equipment grounding conductors should have very low impedance level less than 0.25 ohm.
- In case of a UPS and Transformer equipment, the Earth resistance shall be automatically measured on an online basis at a pre-configured interval and corrective action should be initiated based on the observation. The automatic Earthing measurements should be available on the UPS panel itself
- There should be enough space between data and power cabling and there should not be any cross wiring of the two, in order to avoid any interference, or corruption of data.
- The earth connections shall be properly made.

- A complete copper mesh earthing grid needs to be installed for the server farm area, every rack need to be connected to this earthing grid. A separate earthing pit needs to be in place for this copper mesh.
- Provide separate earthing pits for servers, UPS & generators as per the standards.
- Expectation is to have maintenance free chemical earthing.

h. Cable Work

- Cable ducts should be of such dimension that the cables laid in it do not touch one another. If found necessary the cable shall be fixed with clamps on the walls of the duct. Cables shall be laid on the walls/on the trays as required using suitable clamping/ fixing arrangement as required. Cables shall be neatly arranged on the trays in such manner that a criss-crossing is avoided and final take off to switch gear is easily facilitated.
- All cables will be identified close to their termination point by cable number as per circuit schedule. Cable numbers will be punched on 2mm thick aluminum strips and securely fastened to the. In case of control cables all covers shall be identified by their wire numbers by means of PVC ferrules. For trip circuit identification additional red ferrules are to be used only in the switch gear / control panels, cables shall be supported so as to prevent appreciable sagging. In general distance between supports shall not be greater than 600mm for horizontal run and 750mm for vertical run.
- Each section of the rising mains shall be provided with suitable wall straps so that same the can be mounted on the wall.
- Whenever the rising mains pass through the floor they shall be provided with a built-in fire proof barrier so that this barrier restricts the spread of fire through the rising mains from one section to the other adjacent section.
- Neoprene rubber gaskets shall be provided between the covers and channel to satisfy the operating conditions imposed by temperature weathering, durability etc.
- Necessary earthling arrangement shall be made alongside the rising mains enclosure by Mean of a GI strip of adequate size bolted to each section and shall be earthed at both ends. The rising mains enclosure shall be bolted type.
- The space between data and power cabling should be as per standards and there should not be any criss-cross wiring of the two, in order to avoid any interference, or corruption of data.

i. Fire Detection and alarm System

- Fire can have disastrous consequences and affect operations of a Control Room. It is required that there is early-detection of fire for effective functioning of the Control Room.

i. System Description

- The Fire alarm system shall be an automatic 1 ton (e.g. 8) zone single loop addressable fire detection and alarm system, utilizing conventional detection and alarm sounders.
- Detection shall be by means of automatic heat and smoke detectors located throughout the Control Room (ceiling, false floor and other appropriate areas where fire can take place) with break glass units on escape routes and exits.

ii. Control and Indicating Component

- The control panel shall be a microprocessor based single loop addressable unit, designed and manufactured to the requirements of EN54 Part 2 for the control and indicating component and EN54 Part 4 for the internal power supply.
- All controls of the system shall be via the control panel only.
- The system status shall be made available via panel mounted LEDs and a backlit 8 line x 40-character alphanumeric liquid crystal display.
- All system controls and programming will be accessed via an alphanumeric keypad. The control panel will incorporate form fill menu driven fields for data entry and retrieval.
- The system will include a detection verification feature. The user shall have the option to action a time response to a fire condition. This time shall be programmable up to 10 minutes to allow for investigation of the fire condition before activating alarm outputs. The operation of a manual call point shall override any verify command.

iii. Manual Controls

- Start sounders
- Silence sounders
- Reset system
- Cancel fault buzzer
- Display test
- Delay sounder operation
- Verify fire condition
- Disable loop

iv. Smoke detectors:

Smoke detectors shall be of the optical or ionisation type. Devices shall be compatible with the CIE conforming to the requirements of EN54 Part 7 and be LPCB approved. The detectors shall have twin LEDs to indicate the device has operated and shall fit a common addressable base.

v. Heat detectors

- Heat detectors shall be of the fixed temperature (58° C) or rate of temperature rise type with a fixed temperature operating point.
- Devices shall be compatible with the CIE conforming to the requirements of EN54 Part 5 and be LPCB approved.
- The detectors shall have a single LED to indicate the device has operated and shall fit a common addressable base.

vi. Addressable detector bases

- All bases shall be compatible with the type of detector heads fitted and the control system component used. Each base shall comprise all necessary electronics including a short circuit isolator.

- The device shall be automatically addressed by the CIE on power up of the loop without the need of the insertion of a pre-programmed EPROM or setting of DIL switches.
- Detector bases shall fit onto an industry standard conduit box.

vii. Audible Alarms

- Electronic sounders shall be coloured red with adjustable sound outputs and at least 3 sound signals. The sounders should be suitable for operation with a 24V DC supply providing a sound output of at least 100dBA at 1 meter and 75 dBA min, for a bed head or sounder base type device. The sounder frequency shall be in the range of 500Hz to 1000Hz.

viii. Commissioning

- The fire detection and alarm system will be programmable and configurable via an alpha numeric keypad on the control panel.

ix. High Sensitivity Smoke Detection System

- General – The HSSD system shall provide an early warning of fire in its incipient stage, analyse the risk and provide alarm and actions appropriate to the risk. The system shall include, but not be limited to, a Display Control Panel, Detector Assembly and the properly designed sampling pipe network. The system component shall be supplied by the manufacturer or by its authorized distributor.

x. Regulatory Requirements

- National Electrical Code (NEC)
- Factory Mutual
- Local Authority having Jurisdiction

j. Water leak detection System

- Water leak detection System should be designed to protect the Air-conditioned premises and to alert the personnel about the leak in the AC systems. The system should be capable of interfacing to Water leak detection sensors, condensation sensors & I/O modules.
- Events should be clearly reported on LCD/LED display with full English language description of the nature of the fault in the panel. The successful bidder should make detailed working drawings and coordinate them with other agencies at site. Water Leak Detection systems should be integrated with BAS.

i. EQUIPMENT

The Water leak detection system should comprise of Tape Sensors, Water Leak detection modules, Condensation detectors, I/O modules and sounders all connected to a Control Panel.

ii. CONTROL PANEL

- The control panel should be computerized 4/8/12 zone multiplex controller with a facility to add on dialer and speech processor. The system should be programmed, armed or disarmed through a control key pad. The control key pad should have a 16 character LCD display for viewing various events. The code to arm or disarm the system should be changed only by entering a master code.
- The system should have 4/8/12 zones and all the detectors should be connected through a 2 core cable. Each area of the premises should be divided into specific zones such that any zone should be isolated by the user if required.
- The entire system should be backed up by a maintenance free rechargeable battery to take care of system's power requirements whenever power fails.
- The system should be totally tamper proof and should activate an alarm if the control panel is opened, the sensors tampered with or if the system cables are cut even in the disarmed state.
- The system should log 500 events and optionally printer should be connected for generating reports.
- The Detectors, I/O Modules, Remote Keypads and other Devices should be connected to a system on a single 2/4/6 Core Cable Bus to avoid individual cabling of zones.
- The system should have a Buffer memory of minimum 250 events and log each event with exact date and time.
- The controller should have a Serial Port for connecting to a computer.
- The controller should work on 220/240V AC power supply and it should also have a built in battery backup.
- The memory inside the controller should be backed up by a lithium battery. The controller should work effectively over a temperature range of -10 Deg. C to + 55 Deg. C. and 0 to 90% of Humidity.

iii. WATER LEAK DETECTION SENSOR

Water Leak Detection sensors should be able to mount in DIN rails, inside AHU's, power distribution units or other equipment where localized leak detection is

required. The detectors should be resistant to oxidation and erosion. The detector should have relay output for connection to the controller. LED alarm indication should also be provided. The detectors should operate in AC or DC supply.

iv. TAPE SENSORS

Tape sensors are used to detect water leaks usually under floors. Tape sensors for use with water leak detectors should be covered with plastic netting to prevent short circuits when used in metal trays or conduits, and enables the tape to be folded at right angles to allow easy routing.

v. HOOTER / SOUNDER

The hooter / sounder should give audible alarm when any sensor operates. It should be complete with electronic oscillations, magnetic coil (sound coil) and accessories ready for mounting (fixing). The sound output from the Hooter should not be less than 85 decibels at the source point.

k. Access Control System

The Access Control System shall be deployed with the objective of allowing entry and exit to and from the premises to authorized personnel only. The system deployed shall be based on Biometric Technology. An access control system consisting of a central PC, intelligent controllers, power supplies and all associated accessories is required to make a fully operational on line access control system. Access control shall be provided for doors. These doors shall be provided with electric locks, and shall operate on fail-safe principle. The lock shall remain unlocked in the event of a fire alarm or in the event of a power failure. The fire alarm supplier shall make potential free contacts available for releasing the locks in a fire condition especially for staircase and main doors. Entry to the restricted area shall be by showing a proximity card near the reader and exit shall be using a push button installed in the secure area. The system shall monitor the status of the doors through magnetic reed contacts. The system should be designed and implemented to provide following functionality:

- Controlled Entries to defined access points
- Controlled exits from defined access points
- Controlled entries and exits for visitors
- Configurable system for user defined access policy for each access point
- Record, report and archive each and every activity (permission granted and / or rejected) for each access point.
- User defined reporting and log formats
- Fail safe operation in case of no-power condition and abnormal condition such as fire, theft, intrusion, loss of access control, etc.
- Day, Date, Time and duration based access rights should be user configurable for each access point and for each user.
- One user can have different policy / access rights for different access points.

l. Rodent Repellent system:

The entry of Rodents and other unwanted pests shall be controlled using non-chemical, non-toxic devices. Ultrasonic pest repellents shall be provided in the false flooring and ceiling to repel the pests without killing them. However periodic pest control using Chemical spray can be done once in 3 months as a contingency measure to effectively fight the pest menace.

- Configuration : Master console with necessary transducer
- Operating Frequency : Above 20 KHz (Variable)
- Sound Output : 50 dB to 110 dB (at 1 meter)
- Power output : 800 mW per transducer
- Power consumption : 15 W approximately
- Power Supply : 230 V AC 50 Hz
- Mounting : Wall / Table Mounting

m. Instruction about Civil Work

a. Building design must be in accordance with international standards.
b. MSI has to provide the Building Design Parameters which are essential for building
   State of the Art Building of ICCC
   i. Layout Design
   ii. Cabling
c. Layout
   i. Type of cable (Fire resistant etc.)
d. Ducting
e. MSI should define the standard of on building construction.
f. It is expected that design of CCC building is demonstrated through 3D video.
g. MSI should recommend the international standards and suggest what specific requirement of building design are required for building a state of the art Integrated Command and Control Center.
h. Building design must be futuristic, using 3D modelling, which can be refined and revise the final view of the actual ICCC.
i. The ICCC physical building design should also be modular and able to accommodate other BMC systems within ICCC premises.
j. MSI will be required to get approval on engineering drawings of ICCC from BSCDCL.
k. During the review of design documents, BSCDCL may suggest some changes or provide feedback on design parameters. MSI will be required to incorporate such inputs.
l. BSCDCL may authorize any third party do to review of design documents.
m. After final approval of BSCDCL on design documents, building work will be initiated by BSCDCL.

7.9 DG Set

#	Item	Minimum Specifications
1	General Specifications	• Auto Starting DG Set mounted on a common base frame with AVM (Anti-Vibration) pads, residential silencer with exhaust piping,

		complete conforming to ISO 8528 specifications and CPCB certified for emissions. • KVA rating as per the requirement to provide the supply for CCC
2	Engine	Radiator cooled, multi cylinder, 1500 RPM diesel engine, with electronic/manual governor and electrical starting arrangement complete with battery, conforming to BS 5514/ ISO 3046/ IS 10002
3	Fuel	High Speed Diesel (HSD)
5	Alternator	Self-exciting, self-regulating type alternator rated at 0.8 PF or better, 415 Volts, 3 Phase, 4 wires, 50 cycles/sec, 1500 RPM, conforming to IS 4722/ BS 5000, Windings of 100% Copper, class H insulation, Protection as per IP 23.
6	AMF (Auto Main Failure) Panel	AMF Panel fitted inside the enclosure, with the following: It should have the following meters/indicators • Incoming and outgoing voltage • Current in all phases • Frequency • KVA and power factor • Time indication for hours/minutes of operation • Fuel Level in fuel tank, low fuel indication • Emergency Stop button • Auto/Manual/Test selector switch • MCCB/Circuit breaker for short-circuit and overload protection • Control Fuses • Earth Terminal • Any other switch, instrument, relay etc. essential for Automatic functioning of DG set with AMF panel
7	Acoustic Enclosure	• The DG set shall be provided with acoustic enclosure / canopy to reduce the sound level and to house the entire DG set (Engine & Alternator set) assembly outside (open-air). • The enclosure must be weather resistant powder coated, with insulation designed to meet latest MOEF/CPCB norms for DG sets, capable to withstand climate. The enclosure must have ventilation system, doors for easy access for maintenance, secure locking arrangement, complete and
8	Fuel Tank Capacity	It should be sufficient and suitable for containing fuel for minimum 12 hours continuous operation, Complete with level indicator, fuel inlet and outlet, air vent, drain plug, inlet arrangement for direct filling and set of fuel hoses for inlet and return.

7.10 Server (Application / Database or Other)

#	Parameter	Minimum Specifications
1.	Make And Model	To be specified by the bidder
2.	Processor	Latest generation x86 processor with highest cache and highest frequency (on processor with highest cache), within the selected category of cores, should be provided, e.g. while selecting 8 core processor, bidder needs to select the processor in 8 core category with highest frequency in the highest cache
3.		Min. 2 Physical sockets or higher
4.	Main Memory	Min. 8GB per core expandable to 196 GB
5.	RAS Features	Hot Pluggable Disk Drives
6.		Redundant Power Supply at server / chassis level
7.		Redundant hot swappable fans at server / chassis level
8.	Hard Disks	2 Nos. Hot-swap 146 GB or higher SAS/SCSI Disk Drives.
9.	RAID	Integrated RAID offering Striping, Mirroring (RAID 0, 1)
10.	Network Interface	Minimum 2Nos. 10/100/1000 Mbps Ethernet ports
11.		Minimum 2Nos. 8Gbps FC HBA ports or FCOE ports (wherever connectivity to Storage)
12.		Both Ethernet / FC ports should be in redundant mode
13.	USB	Minimum 1 USB 2.0 ports or an option for connecting USB devices
14.	Virtualization	The server should support virtualization technology and a software defined datacenter network infrastructure

7.11 Blade Chassis

#	Item	Minimum Requirement Description
1.	Blade Chassis	Blade chassis shall be 19" standard Width rack mountable and provide appropriate rack mount kit.
2.	Blade Chassis	The power supply modules should be hot pluggable and should be able to support fully populated chassis with all the servers with highest CPU and memory configuration in the offered series
3.	Blade Chassis (Redundancy)	The power subsystem should support all of the following modes of power redundancy (No redundancy, N+1 , N+N or grid)
4.	Blade Chassis (Redundancy)	The power subsystem should be support N + N power redundancy for a fully populated chassis with the 2 socket (CPU) servers
5.	Blade Chassis (Redundancy)	Should be configured to provide full redundant cooling to all blade slots
6.	Fabric Channel & Ethernet Interconnects	Bidder should provide converged fabric (FCOE) based modules in redundancy to provide 10 Gbps of uplink aggregated bandwidth per server
7.	Management	It should support remote KVM / virtual KVM capability for management and administration.
8.	Blade Chassis (DVD)	Should support virtual DVD and virtual floppy internally / externally
9.	Interface	The Fabric switches should support the direct connection to FCoE enabled storage arrays
10.	Management	Supports a stateless environment where server identity is created by the administrator who defines the server BIOS version, MAC ID, NIC firmware version, WWPN , FC-HBA firmware version , Adapter QoS , Management module firmware version, UUIDs , Server Boot Policies, KVM IP etc
11.	Blade Chassis	Servers can be automatically assigned to the resource pools based on qualification criteria
12.	Management	Firmware upgrade / rollback should be possible for all the components in the infrastructure including the server, chassis management modules , Ethernet switch modules, SAN switch modules, Other IO modules from the same console that is used to manage the individual blades
13.	Management	Role Based Access Control so that the resources can be managed by respective resource administrator.
14.	Server Management	Movement of server identity from one slot to another in the event of server failure. The failover can be movement within a single chassis or across multiple chassis
15.	Power Management	Administrators have the flexibility to define power policies so that the power can be limited to a specific server
16.	Power Management	Administrators should be able to decide the threshold / cap on the maximum power that the chassis can draw.
17.		The system should not be an end of life / end of service product.
18.	Support	The system should not be an end of life / end of service product.

#	Item	Minimum Requirement Description

7.12 Storage Specification

#	Parameter	Minimum Specifications
1.	Solution/Type	• The Solution should be using NL-SAS/SAS Disks for Video camera storage purpose and SSDs/Flash for all other applications. • Solution proposed should yield low cost per TB, while meeting the performance parameters • Licenses for the actual protocols used in the storage solution must be provided from day 1.
2.	Storage	• The SSD storage should provide inline deduplication and inline compression to reduce the capacity requirement and the solution can factor upto 2x capacity efficiency for this purpose. If storage OEMs do not support inline deduplication and inline compression, then they cannot assume any storage efficiency and should provide the required usable capacity to compensate for lack of benefits of these features
3.	Hardware Platform	• Rack mounted form-factor • Modular design to support controllers and disk drives expansion
4.	Connectivity	• The storage system shall be capable of providing host connectivity as per solution offered (Unified/SAN/NAS/Scale out NAS) as to meet operational SLA requirements.
5.	Controllers	• At least 2 Controllers in active/active mode • The controllers / Storage nodes should be upgradable seamlessly, without any disruptions / downtime to production workflow for performance, capacity enhancement and software / firmware upgrades.
6.	RAID support	• Should support various RAID levels (Minimum RAID6 or equivalent)
7.	Cache	• Minimum 128 GB of useable cache spread across all controllers of the storage system. This should be scalable to 256GB in a scale-up or scale-out fashion. If cache is provided in additional hardware for unified storage solution, then cache must be over and above 128 GB.
8.	Redundancy and High Availability	• The Storage System should be able to protect the data against single point of failure with respect to hard disks, connectivity interfaces, fans and power supplies

#	Parameter	Minimum Specifications
9.	Storage Management software	• All the necessary software (GUI Based) to configure and manage the storage space, RAID configuration, logical drives allocation, snapshots etc. are to be provided for the entire system proposed. • Licenses for the storage management software should include disk capacity/count of the complete solution and any additional disks to be plugged-in in the future, up to the max disk capacity of the existing controllers/units. • A single command console for entire storage solution. • Should also include storage performance monitoring and management software • Should provide the functionality of proactive monitoring of Disk drive and Storage system for all possible disk failures • Should be able to take "snapshots" (or equivalent feature) of the stored data to another logical drive for backup purposes
10.	Data Protection	The storage array must have complete cache protection mechanism either by de-staging data to disk or providing complete cache data protection with battery backup for up to 4 hours
11.	IOPS	Offered Primary Storage shall support up for the operation. Please suggest how we reached this value
12.	Operating system support	The storage system should support latest versions of operating systems like Linux, RHEL, SUSE, Windows, Apple, etc.
13.	File system	The File system managing the SAN Storage should support the management of Secondary Storage to move the data from Primary to Secondary Storage.
14.	Firmware	The storage system should support non-disruptive updation/upgrade of firmware for controllers and disks.
15.	Diagnostic	The storage system should have facility to report any failures & errors through Intranet for diagnosis and quick resolution of problems.
16.	Interface	The storage management software should come with web-based/CLI interface for configuring the SAN system from anywhere using TCP/IP network.
17.	Cloud Integration	The proposed solution must provide flexibility to move the application and its associated data from private cloud to DEITY empaneled public cloud , across two different DEITY empaneled public cloud providers and from DEITY empaneled Public Cloud to Private Cloud depending on requirements of various departments. This movement of data should be carried out with minimal downtime, over the Network in an encrypted form. The proposed solution should allow flexibility to allow Primary Site to be on private cloud and its DR to be hosted on DEITY empaneled public cloud without any limitations.

#	Parameter	Minimum Specifications
		The proposed solution should provide for a cloud backup gateway which provides flexibility to backup/archive applications and data from public/private cloud to another public/private cloud.

7.13 Core Switch

#	Minimum Specifications
1.	Should be a chassis based switch and have minimum 32 x 40G QSFP+ or more ports distributed across minimum two or more interface line-cards fully populated with Mode Fiber Transceiver. In addition, it must have 48x 10G BaseT ports and 48x 1/10G SFP+ ports fully populated with multi-mode fiber transceiver.
2.	There should not be any single point of failure in the switch. All the main components like CPU module, switching fabric, power supplies and fans etc. should be in redundant configuration.
3.	It must have minimum five or more vacant interface payload slots (after populating all the required above interfaces).
4.	Chassis must support 40G and 100G interface line cards.
5	Should have minimum of 3.84 Tbps full duplex or more per interface slot throughput.
6	All the interfaces / line-cards should be non-blocking and wire-speed for 64 bytes of packet size and have distributed forwarding architecture.
7	Should have 128K IPv4 Routes, 32K IPv6 Routes, 12K ACL's, 160K MAC Address, 4K active VLAN's and 8 hardware queues per port.
8	Should support minimum of 32 no of ports per LAG / vLAG / Ether channel.
9	Should have IPv6 Static routes, OSPFv3, PIM Sparse / Dense mode (SM /DM), Policy-based routing (PBR), Virtual routing and forwarding (VRF), BGP and Netflow/ Jflow/ Sflow.
10	Should have minimum of 64MB or more of packet buffer size for traffic to support huge file transfers on all the proposed line-cards.
11	Should support the separation of data and control plane, to be controlled by SDN Controller, utilizing ACI / openflow or equivalent protocol.
12	The OEM must feature in the Leaders/ Challengers segment of the "Gartner Magic Quadrant for Data Center Networking".
13	It is preferred that Switch & transceiver to be from same OEM.

7.14 Core Router

#	Minimum Specifications
1.	Chassis should have a minimum 16 x 1/10G SFP+ or more ports populated with Multi-mode 10G SR transceivers from day 1. In addition, it must have an additional 16 x 10/100/1000 BaseT RJ45 ports.
2.	There should not be any single point of failure in the Router. All the main components like Supervisor / CPU module, management module, power supplies and fans etc should be in redundant configuration. It should have distributed forwarding and there should not be any performance degradation in case of any switching/routing engine failure.

3.	It must have minimum two or more vacant interface payload slots from day 1 (after populating all the required above interfaces).
4.	Should have minimum of 400 Gbps or more per interface slot throughput from day 1 with all the above asked redundancy.
5	All the interfaces / line-cards should be non-blocking and wire-speed for 64 bytes of packet size and have distributed forwarding architecture.
6	Should have 1M IPv4 Routes, 200K IPv6 Routes, 32K IPv6 Multicast routes, 1M MAC Address and 4K active VLAN's.
7	Chassis must support 40G and 100G interface line cards
8	Should have IPv6 Static routes, OSPFv3, PIM Sparse / Dense mode (SM /DM), Policy-based routing (PBR), Virtual routing and forwarding (VRF), BGP, BFD, MPLS and Netflow/Jflow/Sflow.
9	The OEM must feature in the Leaders/ Challengers segment of the "Gartner Magic Quadrant for Data Center Networking".
10	It is preferred that Router & transceiver should be from same OEM.

7.15 Internet Router

#	Minimum Specifications
1.	Chassis should have a minimum 8 x 10G SFP+ or more ports populated with Multi-mode 10G SR transceivers from day 1. In addition, it must have an additional 8 x 10/100/1000 BaseT RJ45 ports from day 1.
2.	There should not be any single point of failure in the Router. All the main components like Supervisor / CPU module, management module, power supplies and fans etc should be in redundant configuration. It should have distributed forwarding and there should not be any performance degradation in case of any switching/routing engine failure.
3.	It must have minimum two or more vacant interface payload slots (after populating all the required above interfaces).
4.	Should have minimum of 400 Gbps or more per interface slot throughput with all the above asked redundancy.
5	All the interfaces / line-cards should be non-blocking and wire-speed for 64 bytes of packet size and have distributed forwarding architecture.
6	Should have 1M IPv4 Routes, 200K IPv6 Routes, 32K IPv6 Multicast routes, 1M MAC Address and 4K active VLAN's .
7	Chassis must support 40G and 100G interface line cards from day 1
8	Should have IPv6 Static routes, OSPFv3, PIM Sparse / Dense mode (SM /DM), Policy-based routing (PBR), Virtual routing and forwarding (VRF), BGP, BFD, MPLS and Netflow/Jflow/Sflow.
9	The OEM must feature in the Leaders/ Challengers segment of the "Gartner Magic Quadrant for Data Center Networking".
10	It is preferred that Router & transceiver should be from same OEM.

7.16 SAN Switch

#	Parameter	Minimum Specifications
1.	Power Specification	200-240V, 50-60 Hz
2.	Operating temperature range	0° to 40° C
3.	Operating Relative Humidity range (non-condensing)	10 to 90% relative humidity
4.	Total no. of ports on the proposed switch	24
5.	Throughput of each FC port	8/16Gbps
6.	Support for 4/8/16 Gb/s HBAs	YES
Protocol Supported		
7.	FC	Yes
8.	FCP	Yes
9.	FC-AL	Yes
10.	Designed for high availability with no Single Point of Failure	Yes
Power Supply		
11.	Hot Swappable Power supply proposed	Yes
12.	(N+1) redundant power supply proposed	Yes
Cooling Fans		
13.	Hot Swappable Cooling Fans proposed	Yes
14.	(N+1) redundant Cooling Fans proposed	Yes
15.	Capability for streaming the data in multiple paths with Optimization algorithms for streaming data through shortest available path.	Yes
16.	Capabilities for cascading of switches	Yes
17.	Non-disruptive firmware update	Yes
18.	End to end performance monitoring	Yes
19.	Capability to interface with host based adapters (HBA) of multiple OEM, supporting multiple Operating System including but not limited to AIX, HP-UX, Linux, Solaris, Windows, etc.	Yes
Zoning And Security		
20.	The switch must support hardware ACL-based Port Security, Virtual SANs (VSANs), and Port Zoning.	Yes
21.	Policy based security and centralised fabric management	Yes
22.	Support for Encrypted password	Yes
23.	Support for PKI Digital certificates	Yes
24.	Support for FCAP or FC-SP authentication	Yes

#	Parameter	Minimum Specifications
25.	Support for RADIUS, SSL / HTTPS, SSH, SNMP V3	Yes
26.	Support for LUN masking	Yes
Support For Hardware Based Trunking		
27.	Compatibility with proposed network devices	Yes
28.	Compatibility with proposed servers	Yes
29.	The system should not be an end of life / end of service product.	Yes

7.17 Aggregation/ Data center Switches (L3 Manageable)

#	Parameter	Minimum Specifications
1.	Ports	• 10/100/1000 Base-TX Ethernet ports/FX and extra 2 numbers of Base-SX/LX ports should be one either 24 or 48 • FX/TX Splits for a switch as per location requirement All ports can auto-negotiate between 10Mbps/ 100Mbps/ 1000Mbps, half-duplex or full duplex and flow control for half-duplex ports.
2.	Switch type	Layer 3
3.	MAC	Support 8K or 16K MAC address. (as per solution offered)
4.	Forwarding rate	Packet Forwarding Rate should be 70.0 Mbps or better
5.	Port Features	Must support Port Mirroring, Port Trunking and 802.3ad LACP Link Aggregation port trunks
6.	Flow Control	Support IEEE 802.3x flow control for full-duplex mode ports.
7.	Protocols	• Support 802.1D, 802.1S, 802.1w, Rate limiting • Support 802.1X Security standards • Support 802.1Q VLAN encapsulation, IGMP v1, v2 and v3 snooping • 802.1p Priority Queues, port mirroring, DiffServ • Support based on 802.1p priority bits with at least 8 queues • DHCP support & DHCP snooping/relay/optional 82/ server support • Shaped Round Robin (SRR) or WRR scheduling support. • Support for IPV6 ready features with dual stack • Support up to 255 VLANs and up to 4K VLAN IDs • Support IGMP Snooping, IGMP Querying and Multicasting

		Should support Loop protection and Loop detection, Should support Ring protection (when used in aggregation location)
8.	Access Control	• Support port security • Support 802.1x (Port based network access control). • Support for MAC filtering. Should support TACACS+ and RADIUS authentication
9.	VLAN	• Support 802.1Q Tagged VLAN and port based VLANs and Private VLAN • The switch must support dynamic VLAN Registration or equivalent Dynamic Trunking protocol or equivalent
10.	Protocol and Traffic	• Network Time Protocol or equivalent Simple Network Time Protocol support • Switch should support traffic segmentation Traffic classification should be based on user-definable application types: TOS, DSCP, Port based, TCP/UDP port number
11.	Management	• Switch needs to have RS-232/USB console port for management via a console terminal/PC • Must have support SNMP v1,v2 and v3 • Should support 4 groups of RMON Should have accessibility using Telnet, SSH, Console access, easier software upgrade through network using TFTP etc. Configuration management through CLI, GUI based software utility and using web interface

7.18 KVM Module

#	Item	Minimum Specifications
1.	KVM Requirement	Keyboard, Video Display Unit and Mouse Unit (KVM) for the IT Infrastructure Management at Data Center
2.	Form Factor	19” rack mountable
3.	Ports	minimum 8 ports
4.	Server Connections	It should support both USB and PS/2 connections.
5.	Auto-Scan	It should be capable to auto scan servers
6.	Rack Access	It should support local user port for rack access
7.	SNMP	The KVM switch should be SNMP enabled. It should be operable from remote locations
8.	OS Support	It should support multiple operating system

9.	Power Supply	It should have dual power with failover and built-in surge protection
10.	Multi-User support	It should support multi-user access and collaboration

7.19 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 deduplicated 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.

7.20Rack with KVM over IP

#	Parameter	Minimum Specifications
1.	Type	• 19” 42U racks mounted on the floor • Floor Standing Server Rack - 42U with Heavy Duty Extruded Aluminium Frame for rigidity. Top cover with FHU provision. Top & Bottom cover with cable entry gland plates. Heavy Duty Top and Bottom frame of MS. Two pairs of 19" mounting angles with 'U' marking. Depth support channels - 3 pairs with an overall weight carrying Capacity of 500Kgs. • All racks should have mounting hardware 2 Packs, Blanking Panel. • Stationery Shelf (2 sets per Rack) • All racks must be lockable on all sides with unique key for each rack • Racks should have Rear Cable Management channels, Roof and base cable access
2.	Wire managers	Two vertical and four horizontal
3.	Power Distribution Units	• 2 per rack • Power Distribution Unit - Vertically Mounted, 32AMPs with 25 Power Outputs. (20 Power outs of IEC 320 C13 Sockets & 5 Power outs of 5/15 Amp Sockets), Electronically controlled circuits for Surge & Spike protection, LED readout for the total current being drawn from the channel, 32AMPS MCB, 5 KV AC isolated input to Ground & Output to Ground
4.	Doors	• The racks must have steel (solid / grill / mesh) front / rear doors and side panels. Racks should NOT have glass doors / panels. • Front and Back doors should be perforated with at least 63% or higher perforations. • Both the front and rear doors should be designed with quick release hinges allowing for quick and easy detachment without the use of tools.
5.	Fans and Fan Tray	• Fan 90CFM 230V AC, 4" dia (4 Nos. per Rack) • Fan Housing Unit 4 Fan Position (Top Mounted) (1 no. per Rack) - Monitored - Thermostat based - The Fans should

		switch on based on the Temperature within the rack. The temperature setting should be factory settable. This unit should also include - humidity & temperature sensor
6.	Metal	Aluminium extruded profile
7.	Side Panel	Detachable side panels (set of 2 per Rack)

7.21 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 on 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

7.22 Firewall (Internal/ External)

#	Parameter & minimum specification
	General and Performance Specifications.
1.	The Firewall should have integrated Firewall and VPN functionality.
2.	Firewall packet handling performance should be adequate to deliver the required throughput.
3.	Firewall should have a redundant power supply.
	Operational Modes.
4.	The Firewall should support Layer 2 (Transparent) mode and Layer 3 mode.
5.	Firewall should support static NAT; Policy based NAT and PAT (Port Addressed Translation).
	Firewall.
6.	Firewall should provide TCP reassembly for fragmented packet protection.
7.	Firewall should support integration with URL/Content filtering systems.
	VPN.
8.	Firewall should be capable of dynamic routing on VPN.
9.	Firewall should support client based SSL/TLS as well as IPSec VPN Tunnels.
	High Availability.

#	Parameter & minimum specification
10.	Firewall should support Active/Passive High Availability.
11.	Firewall should support Active/Active High Availability.
12.	Firewall should support Stateful failover of firewall sessions.
13.	Firewall should support device failure detection.
14.	Firewall should support link failure detection.
15.	Firewall should support authentication for all members.
16.	Firewall should support encryption of all traffic.
	Routing.
17.	Support for OSPF and BGP routing protocol
18.	Firewall should support static routes
19.	Should support Multicast with features like RPF, IGMP/ IGMP Proxy, and PIM.
	IPv6 Support
20.	Should support dual stack IPv4 / IPv6 Firewall and VPN.
21.	Support for IPv4 to/from IPv6 translations or tunneling.
22.	Should support Virtualization (Virtual Firewall, Security zones and VLAN).
	Firewall Management
23.	Firewall should support Web based (HTTP and HTTPS) configuration and management.
24.	Firewall should support Command Line Interface using console and SSH.
25.	Firewall should support management via VPN tunnel on any interface.
	Logging.
26.	Should support Syslog server logging.
27.	Should have support for SNMP V1 to V3.
28.	Support for voice protocols: H.323, SIP, and NAT/ ALG for H.323/ SIP.
29.	Firewall should have Automated certificate enrolment (SCEP). PKI Support.
	Administration.
30.	Firewall should support multilevel administration privilege.
31.	Firewall should support software upgrades using secure web Interface
32.	Firewall should support Command Line Interface using console SSH.

7.23 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.

7.24 Integrated Building management system

Sr #	Description
1.	A. The MSI shall supply, install and commission BAS, Access control and Physical security system for ICCC Building Office. MSI has to also provide all necessary hardware and all operating and applications software necessary to perform the control sequences of operation as called for in this specification B. The MSI shall Supply, install and commission a complete Building Automation System (BAS) including all necessary hardware and all operating and applications software necessary to perform the control sequences of operation as called for in this specification. All components of the system –, application controllers, unitary controllers, etc. shall communicate using the BACnet protocol, as defined by ASHRAE Standard 135-2007, or EIA standard 709.1, the LonTalk™ protocol, or Modbus protocol. At a minimum, provide controls for the following: 1. Air handling units 2. Return air fans 3. Exhaust and supply fans 4. Chilled water system including pumps, chillers, and cooling towers 5. Boilers including hot water pumps 6. Computer room air handling units 7. Refrigerant leak detection system 8. Smoke evacuation sequence of AHUs and return fans including smoke control dampers and fire command override panel. 9. Finned tube radiation control 10. Variable volume and constant volume box control including interlocks with finned tube radiation. 11. Cabinet unit heater controls 12. Monitoring points for packaged equipment such as emergency generators, 13. Power wiring to DDC devices, smoke control dampers and BAS panels except as otherwise specified. C. Except as otherwise noted, the control system shall consist of all necessary Ethernet Network Controllers, Standalone Digital Control Units, workstations, software, sensors, transducers, relays, valves, dampers, damper operators, control panels, and other accessory equipment, along with a complete system of electrical interlocking wiring to fill the intent of the specification and provide for a complete and operable system. Except as otherwise specified, provide operators for equipment such as dampers if the equipment manufacturer does not provide these. Coordinate requirements with the various Contractors. D. The MSI shall review and study all HVAC drawings and the entire specification to familiarize themselves with the equipment and system operation and to verify the quantities and types of dampers, operators, alarms, etc. to be provided. E. All interlocking wiring, wiring and installation of control devices associated with the equipment listed below shall be provided. When the BAS system is fully installed

	and operational, the MSI and representatives of the Owner will review and check out the system. At that time, the MSI shall demonstrate the operation of the system and prove that it complies with the intent of the drawings and specifications. F. Provide services and manpower necessary for commissioning of the system in coordination with the existing HVAC Contractor, Balancing Contractor and Owner's representative. G.
2.	**BAS -System Description** A. In accordance to the scope of work, the system shall also provide a graphical, web-based, operator interface that allows for instant access to any system through a standard browser. The contractor must provide PC-based programming workstations, operator workstations and microcomputer controllers of modular design providing distributed processing capability, and allowing future expansion of both input/output points and processing/control functions. The system shall consist of the following components: • Administration and Programming Workstation(s) • Ethernet-based Network Router and/or Network Server Controller(s) These controllers will connect directly to the Operator Workstation over Ethernet at a minimum of 100mbps, and provide communication to the Standalone Digital Control Units and/or other Input/Output Modules. Network Server Controllers shall conform to BACnet device profile B-BC. Network controllers that utilize RS232 serial communications or ARCNET to communicate with the workstations will not be accpted. • Network Controllers shall be tested and certified by the BACnet Testing Laboratory (BTL) as Network Server Controllers (B-BC). • Standalone Digital Control Units (SDCUs): Provide the necessary quantity and types of SDCUs to meet the requirements of the project for mechanical equipment control including air handlers, central plant control, and terminal unit control. Each SDCU will operate completely standalone, containing all of the I/O and programs to control its associated equipment. Each BACnet protocol SDCU shall conform to the BACnet device profile B-AAC. • BACnet SDCUs shall be tested and certified by the BACnet Testing Laboratory (BTL) as Advanced Application Controllers (B-AAC). B. The Local Area Network (LAN) shall be either a 10 or 100 Mpbs Ethernet network supporting BACnet, Modbus, Java, XML, HTTP, and CORBA IIOP for maximum flexibility for integration of building data with enterprise information systems and providing support for multiple Network Server Controllers (NSCs), user workstations and a local host computer system. C. The Enterprise Ethernet (IEEE 802.3) LAN shall utilize Carrier Sense Multiple/Access/Collision Detect (CSMA/CD), Address Resolution Protocol (ARP) and User Datagram Protocol (UDP) operating at 10 or 100 Mbps. D. The system shall enable an open architecture that utilizes EIA standard 709.1, the LonTalk™ protocol and/or ANSI / ASHRAE™ Standard 135-2007, BACnet functionality to assure interoperability between all system components. Native support for the LonTalk™ protocol and the ANSI / ASHRAE™ Standard 135-2007, BACnet protocol are required to assure that the project is fully supported by the

	HVAC open protocols to reduce future building maintenance, upgrade, and expansion costs. E. The system shall enable an architecture that utilizes a MS/TP selectable 9.6-76.8 KBaud protocol, as the common communication protocol between all controllers and integral ANSI / ASHRAE™ Standard 135-2008, BACnet functionality to assure interoperability between all system components. The AAC shall be capable of communicating as a MS/TP device or as a BACnet IP device communicating at 10/100 Mbps on a TCP/IP trunk. The ANSI / ASHRAE™ Standard 135-2008, BACnet protocol is required to assure that the project is fully supported by the leading HVAC open protocol to reduce future building maintenance, upgrade, and expansion costs. F. LonTalk™ packets may be encapsulated into TCP/IP messages to take advantage of existing infrastructure or to increase network bandwidth where necessary or desired. • Any such encapsulation of the LonTalk™ protocol into IP datagrams shall conform to existing LonMark™ guide functionality lines for such encapsulation and shall be based on industry standard protocols. • The products used in constructing the BMS shall be LonMark™ compliant. • In those instances in which Lon-Mark™ devices are not available, the BMS contractor shall provide device resource files and external interface definitions for LonMark devices. G. The software tools required for network management of the LonTalk™ protocol and the ANSI / ASHRAE™ Standard 135-2008, BACnet protocol must be provided with the system. Drawings are diagrammatic only. Equipment and labor not specifically referred to herein or on the plans and are required to meet the functional intent, shall be provided without additional cost to the Owner. Minimum BACnet compliance is Level 4; with the ability to support data read and write functionality. Physical connection of BACnet devices shall be via Ethernet IP or MS/TP. Physical connection of LonWorks devices shall be via Ethernet IP or FTT-10A. H. The system shall support Modbus TCP and RTU protocols natively, and not require the use of gateways. I. The field bus shall support the use of wireless communications. J. Complete temperature control system to be DDC with electronic sensors and electronic/electric actuation of Mechanical Equipment Room (MER) valves and dampers and electronic actuation of terminal equipment valves and actuators as specified herein. The BAS is intended to seamlessly connect devices throughout the building regardless of subsystem type, i.e. variable frequency drives, low voltage lighting systems, electrical circuit breakers, power metering and card access should easily coexist on the same network channel. • The supplied system must incorporate the ability to access all data using Java and HTML5 enabled browsers without requiring proprietary operator interface and configuration programs. • A hierarchical topology is required to assure reasonable system response times and to manage the flow and sharing of data without unduly burdening the customer's internal Intranet network. K. Provide the Commissioning, configuration and diagnostic tool (CCDT), color display personnel computer, software, and interfaces to provide uploading/downloading of High Point Count Controllers (AAC), Unitary

	Equipment Controllers (UEC) and VAV controllers (VAVDDC) monitoring all BACnet objects, monitoring overrides of all controller physical input/output points, and editing of controller resident time schedules. L. Provide a Portable Operator's Terminal (POT) color display personnel computer, software, and interfaces to provide uploading/downloading of Custom Application Controller and Application Specific Controllers databases, monitoring of all LonMark™ Standard Network Variables Types (SNVTs) including display of all bound SNVTs, monitoring and overrides of all controller physical input/output points, and editing of controller resident time schedules. POT connectivity shall be via digital wall sensor connected to controller. M. Deployed system must satisfy system requirements to meet DIARMF (U.S. Department of Defense Information Assurance Risk Management Framework) compliance. Only exception is if system is employing a PEMS system such as described in subsection 1.6 Q. below. N. The system shall have the capability to provide a web-based AFDD (automated fault detection and diagnostic) system. The AFDD system shall be able to interface directly with the project BAS and energy/performance metering system to provide information on HVAC systems that are being controlled. Pricing is to be a separate line item from the BAS proposal. See specification section 25 08 01 for exact requirements. O. The system shall have the capability to provide a web-based APEO (automated predictive energy optimization) system and enable effective participation in local utility Demand Response (DR) programs. The vendor shall provide software and ongoing services that will identify actionable energy saving and peak reduction opportunities to assist the facility in achieving its energy and sustainability objectives, and automatically and continuously operate the systems necessary to achieve the targeted savings and reductions. P. The system shall have the capability to provide a web-enabled PEMS (power and energy management system) monitoring system intended to monitor an entire electrical distribution infrastructure, from incoming utility feeds down to low voltage distribution points. It shall be designed to monitor and manage energy consumption throughout an enterprise, whether within a single facility or across a network of facilities, to improve energy availability and reliability, and to measure and manage energy efficiency. It shall be a standard product offering with no custom programming required. It shall provide a seamless user experience ("Single pane of glass") for managing the mechanical systems (HVAC and lighting) and monitoring the power distribution system (transformers, breakers, relays, switches, capacitors, UPS, invertors, etc.)
	BAS -System Architecture A.General 1. The Building Automation System (BAS) shall consist of Network Server/Controllers (NSCs), a family of Standalone Digital Control Units (SDCUs), Administration and Programming Workstations (APWs), and Web-based Operator Workstations (WOWs). The BAS shall provide control, alarm detection, scheduling, reporting and information management for the entire facility, and Wide Area Network (WAN) if applicable.

	2. An Enterprise Level BAS shall consist of an Enterprise Server, which enables multiple NSCs (including all graphics, alarms, schedules, trends, programming, and configuration) to be accessible from a single Workstation simultaneously for operations and engineering tasks. 3. The Enterprise Level BAS shall be able to host up to 250 servers, or NSCs, beneath it. 4. For Enterprise reporting capability and robust reporting capability outside of the trend chart and listing ability of the Workstation, a Reports Server shall be installed on a Microsoft Windows based computer. The Reports Server can be installed on the same computer as the Enterprise Server. 5. The system shall be designed with a top-level 10/100bT Ethernet network, using the BACnet/IP, LonWorks IP, and/or Modbus TCP protocol. 6. Modbus RTU/ASCII (and J-bus), Modbus TCP, BACnet MS/TP, BACnet IP, LonTalk FTT-10A, and WebServices shall be native to the NSCs. There shall not be a need to provide multiple NSCs to support all the network protocols, nor should there be a need to supply additional software to allow all three protocols to be natively supported. A sub-network of SDCUs using the BACnet MS/TP, LonTalk FTT-10A, and/or Modbus RTU protocol shall connect the local, stand-alone controllers with Ethernet-level Network Server Controllers/IP Routers. B. TCP/IP Level 1. The TCP/IP layer connects all of the buildings on a single Wide Area Network (WAN) isolated behind the campus firewall. Fixed IP addresses for connections to the campus WAN shall be used for each device that connects to the WAN. C. Fieldbus Level with Standalone Digital Control Units (SDCUs) 1. The fieldbus layer shall support all of the following types of SDCUs: a. BACnet SDCU requirements: The system shall consist of one or more BACnet MS/TP field buses managed by the Network Server Controller. Minimum speed shall be 76.8kbps. The field bus layer consists of an RS485, token passing bus that supports up to 127 Standalone Digital Control Units (SDCUs) for operation of HVAC and lighting equipment. These devices shall conform to BACnet standard 135-2007. The NSCs shall be capable of at least two BACnet MS/TP field buses for a total capability of 254 SDCUs per NSC. b. LonWorks SDCU requirements: The system shall consist of one or more LonWorks FTT-10A field buses managed by the Network Server Controller. Minimum speed shall be 76.8kbps. The field bus layer shall consist of up to 64 Lonworks SDCUs using peer-to-peer, event-driven communication for operation of HVAC and lighting equipment. c. Modbus SDCU requirements: The system shall consist of one or more Modbus RTU (RS-485 or RS-232) field buses

managed by the Network Server Controller. The field bus layer shall consist of up to 31 SDCUs for operation of HVAC, power metering, and lighting equipment. If utilizing Modbus TCP, the field bus layer shall consist of up to 100 SDCUs for operation of HVAC, power metering, and lighting equipment. The NSCs shall be capable of at least two Modbus RTU field buses for a total capability of 62 SDCUs per NSC.

d. NETWORK 8000 SDCU requirements: The system shall consist of one or more ASD or LCM field buses managed by the Network Server Controller. The field bus layer shall consist of up to 128 ASD SDCUs or 31 LCM SDCUs for operation of HVAC, power metering, and lighting equipment.
e. I/NET SDCU requirements: The system shall consist of one or more controller LANs and subLANs managed by the Network Server Controller. The network shall consist of up to 100,000 I/NET points capable through numerous links and devices for operation of HVAC, power metering, and lighting equipment.

D. BAS LAN Segmentation

1. The BAS shall be capable of being segmented, through software, into multiple local area networks (LANs) distributed over a wide area network (WAN). Workstations can manage a single LAN (or building), and/or the entire system with all portions of that LAN maintaining its own, current database.

E. Standard Network Support

1. All NSCs, Workstation(s) and Servers shall be capable of residing directly on the owner's Ethernet TCP/IP LAN/WAN with no required gateways. Furthermore, the NSC's, Workstation(s), and Server(s) shall be capable of using standard, commercially available, off-the-shelf Ethernet infrastructure components such as routers, switches and hubs. With this design the owner may utilize the investment of an existing or new enterprise network or structured cabling system. This also allows the option of the maintenance of the LAN/WAN to be performed by the owner's Information Systems Department as all devices utilize standard TCP/IP components.

F. System Expansion

1. The BAS system shall be scalable and expandable at all levels of the system using the same software interface, and the same TCP/IP level and fieldbus level controllers. Systems that require replacement of either the workstation software or field controllers in order to expand the system shall not be acceptable.
2. Web-based operation shall be supported directly by the NSCs and require no additional software.
3. The system shall be capable of using graphical and/or line application programming language for the Network Server Controllers.

G. Support For Open Systems Protocols

1. All Network Server Controllers must natively support the BACnet IP, BACnet MS/TP, LonWorks FTT-10, Modbus TCP, Modbus RTU (RS-485 and RS-232), and Modbus ASCII protocols.

Operator Workstation Requirements

H.General

1. The operator workstation portion of the BAS shall consist of one or more full-powered configuration and programming workstations, and one or more web-based operator workstations. For this project provide a minimum of 10 concurrent operator users and/or 2 concurrent engineering users within the enterprise server.
2. The programming and configuration workstation software shall allow any user with adequate permission to create and/or modify any or all parts of the NSC and/or Enterprise Server database.

I. General Administration and Programming Workstation Software

1. System architecture shall be truly client server in that the Workstation shall operate as the client while the NSCs shall operate as the servers. The client is responsible for the data presentation and validation of inputs while the server is responsible for data gathering and delivery.
2. The workstation functions shall include monitoring and programming of all DDC controllers. Monitoring consists of alarming, reporting, graphic displays, long term data storage, automatic data collection, and operator-initiated control actions such as schedule and set point adjustments.
3. Programming of SDCUs shall be capable of being done either off-line or on-line from any operator workstation. All information will be available in graphic or text displays stored at the NSC. Graphic displays will feature animation effects to enhance the presentation of the data, to alert operators of problems, and to facilitate location of information throughout the DDC system. All operator functions shall be selectable through a mouse.

J. User Interface:

1. The BAS workstation software shall allow the creation of a custom, browser-style interface linked to the user when logging into any workstation. Additionally, it shall be possible to create customized workspaces that can be assigned to user groups. This interface shall support the creation of “hot-spots” that the user may link to view/edit any object in the system or run any object editor or configuration tool contained in the software. Furthermore, this interface must be able to be configured to become a user’s “PC Desktop” – with all the links that a user needs to run other applications. This, along with the Windows user security capabilities, will enable a system administrator to setup workstation accounts that not only limit the capabilities of the user within the BAS software, but may also limit what a user can do on

	the PC and/or LAN/WAN. This might be used to ensure, for example, that the user of an alarm monitoring workstation is unable to shutdown the active alarm viewer and/or unable to load software onto the PC. 2. System shall be able to automatically switch between displayed metric vs. imperial units based on the workstation/web stations localization. 3. Web stations shall have the capability to automatically re-direct to an HTTPS connection to ensure more secure communications. 4. Personalized layouts and panels within workstations shall be extended to web stations to ensure consistent user experiences between the two user interfaces. 5. Servers and clients shall have the ability to be located in different time zones, which are then synchronized via the NTP server. 6. Workstation shall indicate at all times the communication status between it and the server. K. User Security 1. The software shall be designed so that each user of the software can have a unique username and password. This username/password combination shall be linked to a set of capabilities within the software, set by and editable only by, a system administrator. The sets of capabilities shall range from View only, Acknowledge alarms, Enable/disable and change values, Program, and Administer. The system shall allow the above capabilities to be applied independently to each and every class of object in the system. The system must allow a minimum of 256 users to be configured per workstation. Additionally, the software shall enable the ability to add/remove users. 2. Additional requirements include mandatory change of passwords: a) At first logon with default credentials b) Of admin passwords before deploying via Project Configuration Servers L. Automatic monitoring 1. The software shall allow for the automatic collection of data and reporting from any controller or NSC. The frequency of data collection shall be user-configurable. M. Alarm Management 1. The software shall be capable of accepting alarms directly from NSCs or controllers, or generating alarms based on evaluation of data in controllers and comparing to limits or conditional equations configured through the software. Any alarm (regardless of its origination) will be integrated into the overall alarm management system and will appear in all standard alarm reports, be available for operator acknowledgment, and have the option for displaying graphics, or reports. 2. Alarm management features shall include:

	a. A minimum of 1000 alarm notification levels at the NSC, workstation, and web station levels. At the Enterprise level the minimum number of active and viewable alarms shall be 10,000. Each notification level will establish a unique set of parameters for controlling alarm display, distribution, acknowledgment, keyboard annunciation, and record keeping. b. Automatic logging in the database of the alarm message, point name, point value, source device, timestamp of alarm, username and time of acknowledgement, username and time of alarm silence (soft acknowledgement). c. Playing an audible sound on alarm initiation or return to normal. d. Sending an email page to anyone specifically listed on the initial occurrence of an alarm. The ability to utilize email paging of alarms shall be a standard feature of the software integrated with the operating system's mail application interface (MAPI). No special software interfaces shall be required and no email client software must be running in order for email to be distributed. The email notification shall be able to be sent to an individual user or a user group. e. Individual alarms shall be able to be re-routed to a user at user-specified times and dates. For example, a critical high temp alarm can be configured to be routed to a Facilities Dept. workstation during normal working hours (7am-6pm, Mon-Fri) and to a Central Alarming workstation at all other times. f. An active alarm viewer shall be included which can be customized for each user or user type to hide or display any alarm attributes. g. The active alarm viewer can be configured such that an operator must type in text in an alarm entry and/or pick from a drop-down list of user actions for certain alarms. h. The active alarm viewer can be configured such that an operator must type in text in an alarm entry and/or pick from a drop-down list of causes for certain alarms. This ensures accountability (audit trail) for the response to critical alarms. i. The active alarm viewer can be configured such that an operator must confirm that all of the steps in a check list have been accomplished prior to acknowledging the alarm. j. The active alarm viewer shall, if filtered, show the quantity of visible and total number of alarms that are not equal to 'normal' and the quantity of disabled and hidden alarms. k. An operator shall have the capability to assign an alarm to another user of the system. l. Time schedules shall be able to be used to set control notifications to users.

m. An operator shall have the capability to save and apply alarm favorites.

N. Report Generation

1. The Reports Server shall be able to process large amounts of data and produce meaningful reports to facilitate analysis and optimization of each installation.
2. Reports shall be possible to generate and view from the operator Workstation, and/or Webstation, and/or directly from a reports-only web interface.
3. A library of predefined automatically generated reports that prompt users for input prior to generation shall be available. The properties and configurations made to these reports shall be possible to save as Dashboard reports, so that the configurations are saved for future used.
4. It shall be possible to create reports standard tools, such as Microsoft Report Builder 2.0 or Visual Studio, shall be used for customized reports.
5. Additional reports or sets of reports shall be downloadable, transferrable, and importable
6. All reports shall be able to be set up to automatically run or be generated on demand.
7. Each report shall be capable of being automatically emailed to a recipient in Microsoft Word, Excel, and/or Adobe .pdf format.
8. Reports can be of any length and contain any point attributes from any controller on the network.
9. Image management functionality shall be possible to enable the system administrators to easily upload new logos or images to the system.
10. It shall be possible to run other executable programs whenever a report is initiated.
11. Report Generator activity can be tied to the alarm management system, so that any of the configured reports can be displayed in response to an alarm condition.
12. Minimum supplied reports shall include:
    a. Activities Per Server Report
    b. Activities Per User Report
    c. Alarm Amount by Category Report
    d. Alarm Amount by Type Report
    e. Alarms Per Sever Report
    f. Current Alarm Report
    g. Most Active Alarm Report
    h. System Errors Per Server Report
    i. Top Activities Report
    j. Top Alarms Report
    k. Top System Errors Report
    l. Trend Log Comparison Report
    m. User Logins Report
    n. Users and Groups Reports

13. Minimum Energy Reports shall include:
    a. Energy Monitoring Calendar Consumption Report: Shall provide an interactive report that shows the energy usage on one or multiple selected days.
    b. Energy Monitoring Consumption Breakdown Report: Shall provide a report on energy consumption broken down using sub-metering.
    c. Energy Monitoring Consumption Report: Shall show the energy consumption against a specified target value.

O. Scheduling

1. From the workstation or webstation, it shall be possible to configure and download schedules for any of the controllers on the network.
2. Time of day schedules shall be in a calendar style and viewable in both a graphical and tabular view.
3. Schedules shall be programmable for a minimum of one year in advance.
4. To change the schedule for a particular day, a user shall simply select the day and make the desired modifications.
5. Additionally, from the operator web stations, each schedule will appear on the screen viewable as the entire year, monthly, week and day. A simple mouse click shall allow switching between views. It shall also be possible to scroll from one month to the next and view or alter any of the schedule times.
6. Schedules will be assigned to specific controllers and stored in their local RAM memory. Any changes made at the workstation will be automatically updated to the corresponding schedule in the controller.
7. It shall be possible to assign a lead schedule such that shadow/local schedules are updated based upon changes in the Lead.
8. It shall be possible to assign a list(s) of exception event days, dates, date ranges to a schedule.
9. It shall be possible to view combined views showing the calendar and all prioritized exemptions on one screen.
10. It should accommodate a minimum of 16 priority levels.
11. Values should be able to be controlled directly from a schedule, without the need for special program logic.

P. Saving/Reloading

1. The workstation software shall have an application to save and restore NSC and field controller memory files.
2. For the NSC, this application shall not be limited to saving and reloading an entire controller – it must also be able to save/reload individual objects in the controller. This allows off-line debugging of control programs, for example, and then reloading of just the modified information.

Q.Audit Trail

1. The workstation software shall automatically log and timestamp every operation that a user performs at a workstation, from logging on and off a workstation to changing a point value, modifying a program, enabling/disabling an object, viewing a graphic display, running a report, modifying a schedule, etc.
2. It shall be possible to view a history of alarms, user actions, and commands for any system object individually or at least the last 5000 records of all events for the entire system from Workstation.
3. The Enterprise server shall be able to store up to 5 million events.
4. It shall be possible to save custom filtered views of event information that are viewable and configurable in Workstation.
5. It shall be capable to search and view all forced values within the system.

R. Fault Tolerant Enterprise Server Operation (Top level NSC)

1. A single component failure in the system shall not cause the entire system to fail. All system users shall be informed of any detectable component failure via an alarm event. System users shall not be logged off as a result of a system failure or switchover.

S. Web-based Operator Software

1. General:
   a. Day-to-day operation of the system shall be accessible through a standard web browser interface, allowing technicians and operators to view any part of the system from anywhere on the network.
   b. The system shall be able to be accessed on site via a mobile device environment with, at a minimum, access to overwrite and view system values.
2. Graphic Displays
   a. The browser-based interface must share the same graphical displays as the Administration and Programming Workstations, presenting dynamic data on site layouts, floor plans, and equipment graphics. The browser's graphics shall support commands to change set points, enable/disable equipment and start/stop equipment.
   b. Through the browser interface, operators must be able to navigate through the entire system, and change the value or status of any point in any controller. Changes are effective immediately to the controller, with a record of the change stored in the system database.
3. Alarm Management
   a. Systems requiring additional client software to be installed on a PC for viewing the web station from that PC will not be considered.
   b. Through the browser interface, a live alarm viewer identical to the alarm viewer on the Administration and Programming

	workstation shall be presented, if the user's password allows it. Users must be able to receive alarms, silence alarms, and acknowledge alarms through a browser. If desired, specific operator text must be able to be added to the alarm record before acknowledgement, attachments shall be viewable, and alarm checklists shall be available. T. Groups and Schedules 1. Through the browser interface, operators must be able to view pre-defined groups of points, with their values updated automatically. 2. Through the browser interface, operators must be able to change schedules – change start and stop times, add new times to a schedule, and modify calendars. U. User Accounts and Audit Trail 1. The same user accounts shall be used for the browser interface and for the operator workstations. Operators must not be forced to memorize multiple passwords. 2. All commands and user activity through the browser interface shall be recorded in the system's activity log, which can be later searched and retrieved by user, date, or both. V. Web Services 1. The installed system shall be able to use web services to "consume" Information within the Network Server/Controllers (NSCs) with other products and systems. Inability to perform web services within the NSCs will be unacceptable. 2. Shall be able to "consume" data into the system via SOAP and REST web services.
	Network Server Controllers (NSCs)-DDC Panel A. Network Router Controllers shall combine both network routing functions, control functions, and server functions into a single unit. B. The BACnet NSC shall be classified as a "native" BACnet device, supporting the BACnet Network Server Controller (B-BC) profile. Controllers that support a lesser profile such as B-SA are not acceptable. NSCs shall be tested and certified by the BACnet Testing Laboratory (BTL) as BACnet Network Server Controllers (B-BC). C. The Network Server Controller shall provide the interface between the LAN or WAN and the field control devices, and provide global supervisory control functions over the control devices connected to the NRS. D. The NSCs shall be capable of whitelisting IPs to restrict access to a pre-defined list of hosts or devices. E. They shall also be responsible for monitoring and controlling their own HVAC equipment such as an AHU or boiler. F. They shall also contain graphics, trends, trend charts, alarm views, and other similar presentation objects that can be served to workstations or web-based interfaces. A sufficient number of NSCs shall be supplied to fully meet the requirements of this specification and the attached point list. G. It shall be capable of executing application control programs to provide: 1. Calendar functions

2. Scheduling
3. Trending
4. Alarm monitoring and routing
5. Time synchronization by means of an Internet site including automatic synchronization
6. Native integration of LonWorks controller data and Modbus controller data or BACnet controller data and Modbus controller data
7. Network Management functions for all LonWorks based devices

H. Hardware Specifications

1. Memory:
   a. The operating system of the controller, application programs, and all other portions of the configuration database, shall be stored in non-volatile, FLASH memory. Servers/Controllers shall contain enough memory for the current application, plus required history logging, plus a minimum of 20% additional free memory.
2. Each NRC shall provide the following on-board hardware for communication:
   a. One 10/100bT Ethernet for communication to Workstations, other NRCs and onto the Internet
   b. Two RS-485 ports for communication to BACnet MSTP bus or serial Modbus (software configurable)
   c. One TP/FT port for communication to LonWorks devices.
   d. One device USB port
   e. One host USB port
3. The NSC shall conform to a small footprint no larger than 100W x 125H x 75D mm (3.94W x 4.92H x 2.95D in).

I. Modular Expandability:

1. The system shall employ a modular I/O design to allow expansion. Input and output capacity is to be provided through plug-in modules of various types. It shall be possible to combine I/O modules as desired to meet the I/O requirements for individual control applications.
2. One shall be able to “hot-change” (hot-swap) the I/O modules preserving the system on-line without any intervention on the software; addressing and configuration shall be automatic.
3. If for any reason the backplane of the modular I/O system were to fail, I/O module addresses will be protected.

J. Hardware Override Switches:

1. All digital outputs shall, optionally, include three position manual override switches to allow selection of the ON, OFF, or AUTO output state. These switches shall be built into the unit and shall provide feedback to the controller so that the position of the override switch can be obtained through software. In addition each analog output shall be equipped with an override potentiometer to allow manual adjustment of the analog output

signal over its full range, when the 3 position manual override switch is placed in the ON position.

K. Universal Input Temperatures

1. All universal inputs directly connected to the NSC via modular expansion shall be capable of using the following thermistors for use in the system without any external converters needed.
   1) 10 kohm Type I (Continuum)
   2) 10 kohm Type II (I/NET)
   3) 10 kohm Type III (Satchwell)
   4) 10 kohm Type IV (FD)
   5) Linearized 10 kohm Type V (FD w/11k shunt)
   6) Linearized 10 kohm (Satchwell)
   7) 1.8 kohm (Xenta)
   8) 1 kohm (Balco)
   9) 20 kohm (Honeywell)
   10) 2.2 kohm (Johnson)
2. In addition to the above, the system shall be capable of using the below RTD sensors, however it is not required that all universal inputs be compatible with them.
   1) PT100 (Siemens)
   2) PT1000 (Sauter)
   3) Ni1000 (Danfoss)

L. Local Status Indicator Lamps:

1. The NSC shall provide as a minimum LED indication of CPU status, Ethernet LAN status, and field bus status. For each input or output, provide LED indication of the value of the point (On/Off). The LED indication shall support software configuration to set whether the illumination of the LED corresponds to On or Off or whether the color when illuminated is Red or Green.

M. Real Time Clock (RTC):

1. Each NSC shall include a real time clock, accurate to 10 seconds per day. The RTC shall provide the following: time of day, day, month, year, and day of week. Each NSC will allow for its own UTC offset, depending upon the time zone. When the time zone is set, the NSC will also store the appropriate times for daylight savings time.
2. The RTC date and time shall also be accurate, up to 30 days, when the NSC is powerless.
3. No batteries may be used to for the backup of the RTC.

N. Power Supply:

1. The 24 VDC power supply for the NSCs shall provide 30 watts of available power for the NSC and associated IO modules. The system shall support the use of more than one power supply if heavily power consuming modules are required.
2. The power supply, NSC, and I/O modules shall connect power wise and communication wise via the separate terminal base allowing for ease of replacement and no separate or loose wiring.

O. Automatic Restart After Power Failure:
   1. Upon restoration of power after an outage, the NSC shall automatically and without human intervention update all monitored functions, resume operation based on current, synchronize time and status, and implement special start-up strategies as required.

P. Data Retention:
   1. During a power failure, the NSC shall retain all programs, configuration data, historical data, and all other data that is configured to be retained. There shall be no time restriction for this retention and it must not use batteries to achieve it.

Q. Software Specifications
   1. The operating system of the controller, application programs, and all other portions of the configuration database such as graphics, trends, alarms, views, etc., shall be stored in non-volatile, FLASH memory. There will be no restrictions placed on the type of application programs in the system. Each NSC shall be capable of parallel processing, executing all control programs simultaneously. Any program may affect the operation of any other program. Each program shall have the full access of all I/O facilities of the processor. This execution of control function shall not be interrupted due to normal user communications including interrogation, program entry, printout of the program for storage, etc.
   2. Each NSC shall have an available capacity of 4 GB of memory. This shall represent 2 GB for application and historical data and 2 GB dedicated for backup storage.

R. User Programming Language:
   1. The application software shall be user programmable. This includes all strategies, sequences of operation, control algorithms, parameters, and set points. The source program shall be either a script-based structured text or graphical function block based and fully programmable by the user. The language shall be structured to allow for the configuration of control programs, schedules, alarms, reports, telecommunications, local displays, mathematical calculations, and histories. Users shall be able to place comments anywhere in the body of either script or function block programs.
   2. Network Server Controllers that use a “canned” program method will not be accepted.

S. Control Software:
   1. The NSC shall have the ability to perform the following pre-tested control algorithms:
      a. Proportional, Integral plus Derivative Control (PID)
      b. Two Position Control
      c. Digital Filter
      d. Ratio Calculator
      e. Equipment Cycling Protection

T. Mathematical Functions:
   1. Each controller shall be capable of performing basic mathematical functions (+, -, *, /), squares, square roots, exponential, logarithms, Boolean logic statements, or combinations of both. The controllers shall be capable of performing complex logical statements including operators such as >, <, =, and, or, exclusive or, etc. These must be able to be used in the same equations with the mathematical operators and nested up to five parentheses deep.

U. NSCs shall have the ability to perform any or all of the following energy management routines:
   1. Time of Day Scheduling
   2. Calendar Based Scheduling
   3. Holiday Scheduling
   4. Temporary Schedule Overrides
   5. Optimal Start
   6. Optimal Stop
   7. Night Setback Control
   8. Enthalpy Switchover (Economizer)
   9. Peak Demand Limiting
   10. Temperature Compensated Duty Cycling
   11. CFM Tracking
   12. Heating/Cooling Interlock
   13. Hot/Cold Deck Reset
   14. Hot Water Reset
   15. Chilled Water Reset
   16. Condenser Water Reset
   17. Chiller Sequencing

V. History Logging:
   1. Each NSC controller shall be capable of LOCALLY logging any input, output, calculated value or other system variable either over user defined time intervals ranging from 1 second to 1440 minutes or based upon a user configurable change of value. A minimum of 1000 logs, with a minimum of 100,000 records, shall be stored. Each log can record either the instantaneous, average, minimum or maximum value of the point. Logged data shall be downloadable to a higher level NSC long term archiving based upon user-defined time intervals, or manual command.
   2. For extended trend logging a minimum of 1500 trends shall be capable, with a minimum number of 600,000 records within.
   3. Management of a power meter replacement to ensure meter log data is accurate shall be possible in the NSC.
   4. Every hardware input and output point, hosted within the NSC and attached I/O modules, shall be trended automatically without the requirement for manual creation, and each of these logs shall log values based upon a change of value and store at least 500 trend samples before replacing the oldest sample with new data.

5. The presentation of logged data shall be built into the server capabilities of the NSC. Presentation can be in time stamped list formats or in a chart format with fully configurable pen colors, weights, scales and time spans.
6. Tooltips shall be present, magnetic, and visible based on users preference.
7. Comments shall be visible whenever viewing the trend log list.

W. Alarm Management:

1. For each system point, alarms can be created based on high/low limits or in comparison to other point values. All alarms will be tested each scan of the NSC and can result in the display of one or more alarm messages or reports.
2. There is no limit to the number of alarms that can be created for any point
3. Alarms can be configured to be generated based upon a single system condition or multiple system conditions.
4. Alarms will be generated based on an evaluation of the alarm conditions and can be presented to the user in a fully configurable order, by priority, by time, by category, etc. These configurable alarm views will be presented to a user upon logging into the system regardless of whether the log in takes place at a WorkStation or a Webstation.
5. The alarm management system shall support the ability to create and select cause and action notes to be selected and associated with an alarm event. Checklists shall also be possible in order to present to an operator a suggested mode of troubleshooting. When acknowledging an alarm, it shall be possible to assign it to a user of the system such that the user is notified of the assignment and is made responsible for the alarm resolution.
6. Alarms must be capable of being routed to any BACnet workstation that conforms to the B-OWS device profile and uses the BACnet/IP protocol.

X. Embedded Web Server

1. Each NSC must have the ability to serve out web pages containing the same information that is available from the WorkStation. The development of the screens to accomplish shall not require any additional engineering labor over that required to show them at the WorkStation itself.

BACnet Fieldbus and BACnet SDCUs –DDC panel

A.Networking

1. IP Network: All devices that connect to the WAN shall be capable of operating at 10 megabits per second or 100 megabits per second.
2. IP To Field Bus Routing Devices
   a. A Network Server Controller shall be used to provide this functionality.

b. These devices shall be configurable locally with IP crossover cable and configurable via the IP network.
c. The routing configuration shall be such that only data packets from the field bus devices that need to travel over the IP level of the architecture are forwarded.

B. Field Bus Wiring and Termination
1. The wiring of components shall use a bus or daisy chain concept with no tees, stubs, or free topology.
2. Each field bus shall have a termination resistor at both ends of each segment.
3. The field bus shall support the use of wireless communications.

C. Repeaters
1. Repeaters are required to connect two segments.
2. Repeaters shall be installed in an enclosure. The enclosure may be in an interstitial space.

D. Field Bus Devices
1. General Requirements
a. Devices shall have a light indicating that they are powered.
b. Devices shall be locally powered. Link powered devices (power is furnished from a central source over the field bus cable) are not acceptable.
c. Application programs shall be stored in a manner such that a loss of power does not result in a loss of the application program or configuration parameter settings. (Battery backup, flash memory, etc.)

E. Network Server Controllers (NSCs)
a. If NSCs have embedded I/O, all of the requirements for I/O that are described under Advance Application Controllers shall apply.
b. Shall support the export of data to NSCs from other vendors that support the data sharing, read property service.
c. Shall support the export of data using Change of Value (COV) initiation to NSCs from other vendors that support the subscription to data using the COV concept.
d. Shall support the export of data to any BACnet OWS that supports the data sharing, read property service.
e. Shall support the export of data using Change of Value (COV) initiation to any BACnet OWS that supports the subscription to data using the COV concept.
f. Shall provide trend log support for all of the devices on the field bus. They shall provide sufficient memory to store up to 300 samples for each variable required to be trended by the sequence of control.
g. Shall support the exporting of trend log data to any BACnet OWS that supports the read range BACnet service for trending.

h. Shall provide time schedule support for all of the devices on the field bus.
i. Shall support the editing of time schedule entries from any BACnet OWS that supports the BACnet service for writing of time schedule parameters.
j. Shall provide alarm message initiation for all alarms conditions from any of the field bus devices.
k. Shall deliver alarm messages to any BACnet OWS that supports the BACnet service for receiving alarm messages and is configured to be a recipient of the notification.
l. Shall support alarm acknowledgement from any BACnet OWS that supports the BACnet service for executing alarm/event acknowledgement.
m. Shall support the control of the out of service property and assignment of value or state to analog and binary objects from any BACnet OWS that supports writing to the out of service property and the value property of analog and binary objects.
n. Shall support the receipt and response to Time Synchronization commands from any device that supports the BACnet service for initiating time synchronization commands.
o. Shall support the "Who is?" and "I am." BACnet service.
p. Shall support the ""Who has?" and "I have." BACnet service.
q. Shall support Backup and Restore commands from any BACnet OWS that supports the initiation of Backup and Restore commands.
r. Shall be BTL certified.

F. Advance Application Controllers (B-AAC)

1. The key characteristics of a B-AAC are:
   a. They have physical input and output circuits for the connection of analog input devices, binary input devices, pulse input devices, analog output devices, and binary output devices. The number and type of input and output devices supported will vary by model.
   b. They may or may not provide support for additional input and output devices beyond the number of circuits that are provided on the basic circuit board. Support for additional I/O shall be provided by additional circuit boards that physically connect to the basic controller.
   c. The application to be executed by a B-AAC is created by an application engineer using the vendor's application programming tool.
   d. If local time schedules are embedded, the B-AAC shall support the editing of time schedule entries from any BACnet OWS that supports the BACnet service for writing of time schedule parameters.

e. If local trend logging is embedded, the B-AAC shall support the exporting of trend log data to any BACnet OWS that supports the read range BACnet service for trending.
f. If local alarm message initiation is embedded, the B-AAC shall:
   1) Deliver alarm messages to any BACnet OWS that supports the BACnet service for receiving alarm messages and is configured to be a recipient off the alarm message.
   2) Support alarm acknowledgement from any BACnet OWS that supports the BACnet service for executing alarm/event acknowledgement,
g. Shall support the reading of analog and binary data from any BACnet OWS or Building Controller that supports the BACnet service for the reading of data.
h. Shall support the control of the out of service property and assignment of value or state to analog and binary objects from any BACnet OWS that supports writing to the out of service property and the value property of analog and binary objects.
i. Shall support the receipt and response to Time Synchronization commands from a BACnet Building Controller.
j. Shall support the "Who is" and "I am." BACnet services.
k. Shall support the "Who has" and "I have." BACnet services.

2. Analog Input Circuits
   a. The resolution of the A/D chip shall not be greater than 0.01 Volts per increment. For an A/D converter that has a measurement range of 0 to 10 VDC and is 10 bit, the resolution is 10/1024 or 0.00976 Volts per increment.
   b. For non-flow sensors, the control logic shall provide support for the use of a calibration offset such that the raw measured value is added to the (+/-) offset to create a calibration value to be used by the control logic and reported to the Operator Workstation (OWS).
   c. For flow sensors, the control logic shall provide support for the use of an adjustable gain and an adjustable offset such that a two point calibration concept can be executed (both a low range value and a high range value are adjusted to match values determined by a calibration instrument).
   d. For non-linear sensors such as thermistors and flow sensors the B-AAC shall provide software support for the linearization of the input signal.
3. Binary Input Circuits
   a. Dry contact sensors shall wire to the controller with two wires.

	b. An external power supply in the sensor circuit shall not be required. 4. Pulse Input Circuits a. Pulse input sensors shall wire to the controller with two wires. b. An external power supply in the sensor circuit shall not be required. c. The pulse input circuit shall be able to process up to 20 pulses per second. 5. True Analog Output Circuits a. The logical commands shall be processed by a digital to analog (D/A) converter chip. The 0% to 100% control signal shall be scalable to the full output range which shall be either 0 to 10 VDC, 4 to 20 milliamps or 0 to 20 milliamps or to ranges within the full output range (Example: 0 to 100% creates 3 to 6 VDC where the full output range is 0 to 10 VDC). b. The resolution of the D/A chip shall not be greater than 0.04 Volts per increment or 0.08 milliamps per increment. 6. Binary Output Circuits a. Single pole, single throw or single pole, double throw relays with support for up to 230 VAC and a maximum current of 2 amps. b. Voltage sourcing or externally powered triacs with support for up to 30 VAC and 0.5 amps at 24 VAC. 7. Program Execution a. Process control loops shall operate in parallel and not in sequence unless specifically required to operate in sequence by the sequence of control. b. The sample rate for a process control loop shall be adjustable and shall support a minimum sample rate of 1 second. c. The sample rate for process variables shall be adjustable and shall support a minimum sample rate of 1 second. d. The sample rate for algorithm updates shall be adjustable and shall support a minimum sample rate of 1 second. e. The application shall have the ability to determine if a power cycle to the controller has occurred and the application programmer shall be able to use the indication of a power cycle to modify the sequence of controller immediately following a power cycle. 8. Local Interface a. The controller shall support the connection of a portable interface device such as a laptop computer or vendor unique hand-held device. The ability to execute any tasks other than viewing data shall be password protected. Via this local interface, an operator shall be able to: 1) Adjust application parameters.

	2) Execute manual control of input and output points. 3) View dynamic data. G.Application Specific Devices 1. Application specific devices shall have fixed function configurable applications. 2. If the application can be altered by the vendor's application programmable tool, the device is an advanced application controller and not an application specific device. 3. Application specific devices shall be BTL certified.
	DDC Sensors and Point Hardware H.Temperature Sensors 1. All temperature devices shall use precision thermistors accurate to +/- 1 degree F over a range of –30 to 230 degrees F. Space temperature sensors shall be accurate to +/- .5 degrees F over a range of 40 to 100 degrees F. 2. Room Sensor: Standard space sensors shall be available in an [off white] [black] enclosure made of high impact ABS plastic for mounting on a standard electrical box. 1) Where manual overrides are required, the sensor housing shall feature both an optional sliding mechanism for adjusting the space temperature set point, as well as a push button for selecting after hours operation. 2) Where a local display is specified, the sensor shall incorporate an LCD display for viewing the space temperature, set point and other operator selectable parameters. Using built in buttons, operators shall be able to adjust set points directly from the sensor. 3. Duct Probe Sensor: Sensing element shall be fully encapsulated in potting material within a stainless steel probe. Useable in air handling applications where the coil or duct area is less than 14 square feet. 4. Duct Averaging Sensor: Averaging sensors shall be employed in ducts which are larger than 14 square feet. The averaging sensor tube shall contain at least one thermistor for every 3 feet, with a minimum tube length of 6 feet. The averaging sensor shall be constructed of rigid or flexible copper tubing. 5. Pipe Immersion Sensor: Immersion sensors shall be employed for measurement of temperature in all chilled and hot water applications as well as refrigerant applications. Provide sensor probe length suitable for application. Provide each sensor with a corresponding pipe-mounted sensor well, unless indicated otherwise. Sensor wells shall be stainless steel for non-corrosive fluids below 250 degrees F and 300 series stainless steel for all other applications. 6. Outside Air Sensor: Provide the sensing element on the building's north side. Sensing element shall be fully encapsulated in potting material within a stainless steel probe. Probe shall be

	encased in PVC solar radiation shield and mounted in a weatherproof enclosure. Operating range -40 to 122 F, 7. A pneumatic signal shall not be allowed for sensing temperature. I. Humidity Wall Transmitter 1. Transmitters shall be accurate to +/- [1] [2] % at full scale. 2. Transmitter shall have replaceable sensing element. 3. Sensor type shall be thin-film capacitive. 4. Sensor element shall contain multipoint calibration on-board in nonvolatile memory 5. Operating range shall be 0 - 100% RH noncondensing, 50 to 95 F 6. Output shall be field selectable 4-20 mA or 0-5/0-10 VDC. 7. Transmitter shall accept 12-30 VDC or 24 VAC supply power. 8. Transmitter shall be available in an [off white] [black] enclosure made of high impact ABS plastic for mounting on a standard electrical box. 9. Transmitter shall have LCD display 10. Transmitter shall be available with a certification of NIST calibration 11. Transmitter shall have integrated temperature sensor J. Humidity Duct Transmitter 1. Transmitters shall be accurate to +/- [1] [2] % at full scale. 2. Transmitter shall be fully encapsulated in potting material within a stainless steel probe. 3. Transmitter shall have replaceable sensing element. 4. Sensor type shall be thin-film capacitive. 5. Sensor element shall contain multipoint calibration on-board in nonvolatile memory 6. Operating range shall be 0 - 100% RH noncondensing, -40 to 122 F 7. Output shall be 4-20 mA or 0-5/0-10 VDC. 8. Transmitter shall accept 12-30 VDC or 24 VAC supply power. 9. Transmitter shall be available with a certification of NIST calibration 10. Transmitter shall have integrated temperature sensor K.Humidity Outdoor Transmitter 1. Transmitters shall be accurate to +/- 2% at full scale. 2. Transmitter shall be fully encapsulated in potting material within a stainless steel probe. Probe shall be encased in PVC solar radiation shield and mounted in a weatherproof enclosure. 3. Transmitter shall have replaceable sensing element. 4. Sensor type shall be thin-film capacitive. 5. Sensor element shall contain multipoint calibration on-board in non-volatile memory 6. Operating range shall be 0 - 100% RH noncondensing, -40 to 122 F 7. Output shall be 4-20 mA or 0-5/0-10 VDC. 8. Transmitter shall accept 12-30 VDC or 24 VAC supply power.

	9. Transmitter shall be available with a certification of NIST calibration 10. Transmitter shall have integrated temperature sensor L. Carbon Dioxide Wall Transmitter: 1. Sensor type shall be Non-dispersive infrared (NDIR). 2. Accuracy shall be ±30 ppm ±2% of measured value with annual drift of ±10 ppm. Minimum five year recommended calibration interval. 3. Repeatability shall be ±20 ppm ±1% of measured value 4. Response Time shall be <60 seconds for 90% step change 5. Outputs shall be field selectable [Analog: 4-20mA or 0-5/0-10VDC] [Protocol: Modbus or BACnet] with [SPDT Relay 1A@30VDC] [temperature setpoint slider] 6. Transmitter shall accept 12-30 VDC or 24 VAC supply power. 7. Temperature Range: [32° to 122°F (CO2 only)] [50° to 95°F (with humidity option)] 8. Output range shall be programmable 0-2000 or 0-5000 ppm 9. Transmitter shall be available in an [off white] [black] enclosure for mounting on a standard electrical box. 10. Transmitter shall have LCD display for commissioning and provide additional faceplate to conceal LCD display where occupants may misinterpret CO2 readings. 11. Transmitter shall have integrated humidity sensor, temperature sensor M. Carbon Dioxide Duct Transmitter: 1. Sensor type shall be Non-dispersive infrared (NDIR). 2. Accuracy shall be ±30 ppm ±2% of measured value with annual drift of ±10 ppm. Minimum five year recommended calibration interval. 3. Repeatability shall be ±20 ppm ±1% of measured value 4. Response Time shall be <60 seconds for 90% step change 5. Outputs shall be field selectable Analog: 4-20mA or 0-5/0-10VDC with SPDT Relay 1A@30VDC 6. Transmitter shall accept 12-30 VDC or 24 VAC supply power. 7. Temperature Range: 32° to 122°F 8. Output range shall be programmable 0-2000 or 0-5000 ppm 9. Enclosure shall not require remote pickup tubes and make use of integrated H-beam probe to channel air flow to sensor. 10. Enclosure lid shall require no screws and make use of snap on features for attachment 11. Enclosure shall be made of high impact ABS plastic 12. Transmitter shall have LCD display 13. Transmitter shall have integrated humidity sensor, temperature sensor N.Air Pressure Transmitters. 1. Sensor shall be microprocessor profiled ceramic capacitive sensing element

	2. Transmitter shall have 14 selectable ranges from 0.1 – 10" WC 3. Transmitter shall be +/- 1% accurate in each selected range including linearity, repeatability, hysteresis, stability, and temperature compensation. 4. Transmitter shall be field configurable to mount on wall or duct with static probe 5. Transmitter shall be field selectable for Unidirectional or Bidirectional 6. Maximum operating pressure shall be 200% of design pressure. 7. Output shall be field selectable 4-20 mA or 0-5/0-10 VDC linear. 8. Transmitter shall accept 12-30 VDC or 24 VAC supply power 9. Response time shall be field selectable T95 in 20 sec or T95 in 2 sec 10. Transmitter shall have an LCD display 11. Units shall be field selectable for WC or PA 12. Transmitter shall have provision for zeroing by pushbutton or digital input. 13. Transmitter shall be available with a certification of NIST calibration O.Liquid Differential Pressure Transmitters: 1. Transmitter shall be microprocessor based 2. Transmitter shall use two independent gauge pressure sensors to measure and calculate differential pressure 3. Transmitter shall have 4 switch selectable ranges 4. Transmitter shall have test mode to produce full-scale output automatically. 5. Transmitter shall have provision for zeroing by pushbutton or digital input. 6. Transmitter shall have field selectable outputs of 0-5V, 0-10V, and 4-20mA. 7. Transmitter shall have field selectable electronic surge damping 8. Transmitter shall have an electronic port swap feature 9. Transmitter shall accept 12-30 VDC or 24 VAC supply power 10. Sensor shall be 17-4 PH stainless steel where it contacts the working fluid. 11. Performance: a. Accuracy shall be ±1% F.S. and ±2% F.S. for lowest selectable range b. Long term stability shall be ±0.25% c. Sensor temperature operating range shall be -4° to 185°F d. Operating environment shall be 14° to 131°F; 10-90% RH noncondensing e. Proof pressure shall be 2x max. F.S. range f. Burst pressure shall be 5x max. F.S. range 12. Transmitter shall be encased in a NEMA 4 enclosure 13. Enclosure shall be white powder-coated aluminum 14. Transmitter shall be available with a certification of NIST calibration

15. [Transmitter shall be preinstalled on a bypass valve manifold]

P. Current Sensors

1. Current status switches shall be used to monitor fans, pumps, motors and electrical loads. Current switches shall be available in split core models, and offer either a digital or an analog signal to the automation system.

Q. Current Status Switches for Constant Load Devices

1. General: Factory programmed current sensor to detect motor undercurrent situations such as belt or coupling loss on constant loads. Sensor shall store motor current as operating parameter in non-volatile memory. Push-button to clear memory.
2. Visual LED indicator for status.
3. Split core sensor, induced powered from monitored load and isolated to 600 VAC rms. Sensor shall indicate status from 0.5 A to 175 A.
4. Normally open current sensor output. 0.1A at 30 VAC/DC.
5. Basis of Design: Veris Model H608.

R. Current Status Switches for Constant Load Devices (Auto Calibration)

1. General: Microprocessor based, self-learning, self-calibrating current switch. Calibration-free status for both under and overcurrent, LCD display, and slide-switch selectable trip point limits. At initial power-up automatically learns average current on the line with no action required by the installer
2. Split core sensor, induced powered from monitored load and isolated to 600 VAC rms. Sensor shall indicate status from 2.5 A to 200 A.
3. Display: Backlit LCD; illuminates when monitored current exceeds 4.5A
4. Nominal Trip Point: ±40%, ±60%, or on/off (user selectable)
5. Normally open current sensor output. 0.1A at 30 VAC/DC.

S. Current Status Switches for Variable Frequency Drive Application

1. General: Microprocessor controlled, self-learning, self-calibrating current sensor to detect motor undercurrent and overcurrent situations such as belt loss, coupling shear, and mechanical failure on variable loads. Sensor shall store motor current as operating parameter in non-volatile memory. Push-button to clear memory and relearn.
2. Visual LED indicator for status.
3. Alarm Limits: ±20% of learned current in every 5 Hz freq. band
4. Split core sensor, induced powered from monitored load and isolated to 600 VAC rms. Sensor shall indicate status from 1.5 A to 150 A and from 12 to 115 Hz.
5. Normally open current sensor output. 0.1A at 30 VAC/DC.

T. Liquid Flow, Insertion Type Turbine Flowmeter:

1. General: Turbine-type insertion flow meter designed for use in pipe sizes 1 1/2" and greater. Available in hot tap configuration with isolation valves and mounting hardware to install or remove the sensor from pipeline that is difficult to shut down or drain
2. Performance:
    1) Accuracy ±1% of rate over optimum flow range; ≥10 upstream and ≥5 downstream straight pipe diameters, uninterrupted flow
    2) Repeatability ±0.5%
    3) Velocity Range: 0.3 to 20 FPS
    4) Pressure Drop 0.5 psi or less @ 10 ft/sec for all pipe sizes 1.5" dia and up
    5) Pressure Rating: 1000 psi @ 70°F
3. Maximum Temperature Rating: 300°F
4. Materials: Stainless Steel or Brass body; Stainless steel impeller
5. Transmitter:
    1) Power Supply: 12 - 30VAC or 8 - 35VDC.
        a) Output: [Frequency] [4-20 mA] [Scaled Pulse]
    2) Temperature Range: 14° to 150°F
    3) Display: 8 character 3/8" LCD (Optional)
    4) Enclosure: NEMA 4, Polypropylene with Viton® sealed acrylic cover

U.Liquid Flow/Energy Transmitter, Non-invasive Ultrasonic (Clamp-on):

1. General: Clamp-on digital correlation transit-time ultrasonic flow meter designed for clean liquids or liquids containing small amounts of suspended solids or aeration. Optional temperature sensors for BTU calculations.
2. Liquid: water, brine, raw sewage, ethylene, glycol, glycerin, others. Contact manufacturer for other fluid compatibility
3. Pipe Surface Temperature: Pipe dia 1/2" to 2":-40-185°F; Pipe dia > 2": -40-250°F
4. Performance:
    1) Flow Accuracy:
        a) Pipe dia 1/2" to 3/4" 1% of full scale
        b) Pipe dia 1" to 2" 1% of reading from 4-40 FPS
        c) Pipe dia 2" to 100" 1% of reading from 1-40 FPS
    2) Flow Repeatability ±0.01% of reading
    3) Velocity Range: (Bidirectional flow)
        a) Pipe dia 1/2" to 2" 2 to 40 FPS
        b) Pipe dia 2" to 100" 1 to 40 FPS
    4) Flow Sensitivity 0.001 FPS
    5) Temperature Accuracy (energy): 32-212°F; Absolute 0.45°F; Difference 0.18°F

6) Temperature Sensitivity: 0.05°F
7) Temperature Repeatability: ±0.05% of reading

5. Transmitter:
   1) Power Supply: 95 to 264 VAC, 47 to 63 Hz or 10 to 28 VDC.
   2) Output: [RJ45] [Modbus TCP/IP] [Ethernet/IP] [BACnet/IP] [Pulse] [4-20 mA] [RS-485 Modbus RTU}
   3) Temperature Range: -40 to +185°F
   4) Display: 2 line backlit LCD with keypad
   5) Enclosure: NEMA 4, (IP65), Powder-coated aluminium, polycarbonate
6. Agency Rating: UL 1604, EN 60079-0/15, CSA C22.2, CSA Class 1 (Pipe > 2")

V.Analog Electric/Pneumatic Transducer:

1. General: Micro-controlled poppet valve for high accuracy and with no air loss in the system. Field configurable for pressure sensing in multiple applications.
2. Power Supply: 22-30VDC, 20-30VAC
3. Control Input: 4-20mA, 0-10V, 0-5V; jumper selectable
4. Performance:
   1) Accuracy: 1% full scale; combined linearity, hysteresis, repeatability
   2) Compensated Temperature Range: 25° to 140°F
   3) Temp Coefficient: ±0.05%°C
   4) Operating Environment: 10-90% RH, non-condensing; 25° to 140°F
5. Supply Pressure: 45 psig max.
6. Manual Override: Jumper selectable mode, digital pushbutton adjust
7. Alarm Contact: 100mA@30VAC/DC (Optional)
8. Control Range 0-20 psig or 3-15 psig; jumper selectable
9. Pressure Differential 0.1 psig (supply to branch)
10. Pressure Indication Electronic, 3-1/2 digit LCD
11. Housing: Mounted on standard SnapTrack; Optional clear dust cover

W. Control Valves

1. Provide automatic control valves suitable for the specified controlled media (steam, water or glycol). Provide valves which mate and match the material of the connected piping. Equip control valves with the actuators of required input power type and control signal type to accurately position the flow control element and provide sufficient force to achieve required leakage specification.
2. Control valves shall meet the heating and cooling loads specified, and close off against the differential pressure conditions within the application. Valves should be sized to operate accurately and with stability from 10 to 100% of the maximum design flow.

3. Trim material shall be stainless steel for steam and high differential pressure applications.
4. Electric actuation should be provided on all terminal unit reheat applications unless electric heat is provided.

X. Dampers

1. Automatic dampers, furnished by the Building Automation Contractor shall be single or multiple blade as required. Dampers are to be installed by the HVAC Contractor under the supervision of the MSI. All blank-off plates and conversions necessary to install smaller than duct size dampers are the responsibility of the Sheet Metal Contractor.
2. Damper frames are to be constructed of 13 gauge galvanized sheet steel mechanically joined with linkage concealed in the side channel to eliminate noise as friction. Compressible spring stainless steel side seals and acetyl or bronze bearings shall also be provided.
3. Damper blade width shall not exceed eight inches. Seals and 3/8 inch square steel zinc plated pins are required. Blade rotation is to be parallel or opposed as shown on the schedules.
4. For high performance applications, control dampers will meet or exceed the UL Class I leakage rating.
5. Control and smoke dampers shall be Ruskin, or approved equal.
6. Provide opposed blade dampers for modulating applications and parallel blade for two position control.

Y. Damper Actuators

1. Damper actuators shall be electronic, and shall be direct coupled over the shaft, without the need for connecting linkage. The actuator shall have electronic overload circuitry to prevent damage. For power-failure/safety applications, an internal mechanical, spring return mechanism shall be built into the actuator housing. Non-spring return actuators shall have an external manual gear release to allow positioning of the damper when the actuator is not powered.

Z. Smoke Detectors

1. Air duct smoke detectors shall be by Air Products & Controls or approved equal. The detectors shall operate at air velocities from 300 feet per minute to 4000 feet per minute.
2. The smoke detector shall utilize a photoelectric detector head.
3. The housing shall permit mechanical installation without removal of the detector cover.
4. The detectors shall be listed by Underwriters Laboratories and meet the requirements of UL 268A.

AA. Airflow Measuring Stations

1. Provide a thermal anemometer using instrument grade self heated thermistor sensors with thermistor temperature sensors.
2. The flow station shall operate over a range of 0 to 5,000 feet/min with an accuracy of +/- 2% over 500 feet/min and +/- 10 ft/min for reading less than 500 feet/min.

7.24.1 Access Control System

- Access Controller Ethernet Based
  - The Access Controller's should be designed for both critical government & private sector security applications.
  - Below input & output modules should be onboard with the Controllers.
    - Universal Inputs : 12
    - Reader Inputs : 8
    - Tamper Input : 1
    - Digital Lock Output : 4
  - The Access Controller's should be designed to support both entry & egress readers while supplying +5 or +12 VDC to each reader.
  - The controller should support the data transfer rates upto 100 Mbps and should have IPSec/IKE encryption and authentication. Encryption (up to 192-bit) and authentication may be enabled for communication to and from workstations and controllers. Controller should utilizes Internet Protocol Security (IPSec) and Internet Key Exchange (IKE) for its encryption to assure tamperproof communications over the Ethernet.
  - The Controller should be perfect for large systems. A controller servicing up to 8 areas can hold 480,000 personnel records. With such a large local storage capacity, access decisions can be made swiftly without waiting for validation by a remote server.
  - Controller should have inbuilt 32 MB of flash memory and 128 MB of DDR SDRAM. The flash memory is used to preserve 12 MB of application and run-time data. The dynamic RAM is partitioned for dedicated functions: a full 12 MB for applications, 48 MB for personnel records and 8 MB for the operating system. The unused memory should be available for future enhancements. Personnel record data should be preserved using onboard batteries that can hold the data for at least 7 days without the use of an external UPS. If the controller has its application stored in flash and power loss lasts longer than what the battery can supply for RAM, the controller will send a message to Cyber Station and request that the personnel records automatically be reloaded when the power returns.
  - The reader inputs should be powered by a dedicated processor allowing the controllers to support current and future devices for advanced applications. The hardware should be ready to support 260-bit encrypted data messages from the reader.
  - It is important for controller to be able to contain potential threats when they are detected. The Controller should respond to Area Lockdown commands set from Access control software providing a quick method of sealing off areas. A simple click of a graphic or an automatic program response is all that is needed to disable card readers and exit requests in any given area. First responder personnel can still gain access to the area if their record is marked with "executive privilege".
  - The Controller should be able to adapt access rights to a change in condition or "threat" levels. Each personnel record should be assigned a clearance level for each area to which they have access. When the condition is more severe than the

person's clearance level then access is automatically denied. The Condition Level may be set manually through workstation or automatically through a program. A program can even be used to monitor national threat levels and adjust Condition Levels accordingly.

- Each controller should support the use of two expansion modules plus an Display unit. The expansion module is used for expanding the controller for special or access to doors. Modules can also be used to provide a cost effective entry reader only solution.
- The Access controller should support up to 32 Infinet nodes. The RS-485 programmable port can be set to support a wired or wireless Infinet field bus.
- The Controllers should be ready to support a wide range of card formats. Ideal for retrofits, The Controller lets you preserve existing cards by accepting standard formats (Weigand, ABA, HID Corporate-1000, CardKey) as well as custom formats (Custom Weigand, Custom ABA). The Controller should support formats up to 260-bits making the controllers ready for government installations that must meet HSPD-12 and FIPS 201 standards.
- SNMP (Simple Network Messaging Protocol) messages may be sent to network monitoring software to inform IT managers as to the health and presence of the access controller on the corporate network. The Access Controller should also support the SNMP alarming option.

Parameters	Specifications
Controller	Microprocessor Based with 8 Readers 12 Inputs, 4 DO , 10/100 bT
Memory	DDR SDRAM: 128 MB Flash: 32 MB
Power	24 VAC , 50/60 Hz 12-28 VDC auto-sensing , 50/60 Hz
Power Consumption	90 VA (AC) 50 W (DC)
Real time Clock	Battery backed by an Internal Battery
Operation Environment	0-50 * C 10-90% RH (Non-Condensing)
Enclosure	UL open class, flammability rating of UL94-5V, IP 10
Mounting	Wall mount using fasteners.
Internal Battery	NiMH , 3.6 VDC, 800 mAh
Battery Backup	Minimum 7 days DDR SDRAM and real-time clock

Ethernet LAN Interface	10/100 Ethernet; ethernet cable with RJ-45 connector.
Serial Comm. Inteface	One RS-485 programmable port, software configurable for Infinet, wireless adapter, RoamIO2 or third-party system.
Input Voltage Range	0-5.115 volts DC
Input Impedance	10K ohm to 5.120V or 5M ohm with pull-up resistor disabled
Input Resolution	5.0 mV
Input Accuracy	±15mV (±0.56°C from -23°C to +66°C or ±1°F from -10°F to +150°F)
Alarm Inputs	12
Card Reader/Keypad Inputs	8, Each input can be connected to a card reader, dedicated keypad, or reader/keypad combination.
Card Reader Type	Wiegand, ABA, or CardKey (jumper selectable)
Max Number of Bits/Card	Up to 260 bits/card
Card Reader Power	+5 VDC @ 120 mA or +12 VDC @ 180 mA (jumper selectable)
Door Outputs	4 Nos. Form C relays with a manual override switch
Output Rating	24 VAC/30 VDC @ 3 A
Overrides	3-position manual override switch on each output for manual control of relay. LED override status indicator.
Status Indicator LEDs	CPU Active, Trasmit & Receive Data , Status of Ethernet activity & link etc.
Dip Switches	Universal inputs, 10 K ohm pull-up disable/enable
Listing & Certifications	FCC , ICES, CE, C-Tick, WEEE, UL/CUL , UL.

- **Input/output Expansion Module:** Up to two I/O modules and an xP-Display may be connected to a controller.

Parameters	Specifications
Operating Environment	32°–120°F (0–49°C), 10–95% RH (non-condensing)
Communications Interface	Through built-in Expansion Port on controller

Status Indicator LEDs	CPU Module is Active
Switches	RESET
Listing	CE,UL & FCC

7.24.2 Smart card/Biometric fingerprint reader

Parameters	Specifications
Read Range	Card Up to 4" (10.2 cm) Key/Tag Up to 1.25" (3.2 cm)
Mounting	Mounting plate attaches to US/EU/ Asian back box, 52-60 mm Screw hole spacing (vertical or horizontal). LCD/Keypad reader Housing latches onto mounting plate; fingerprint module secured to reader with a screw.
Power Supply	9-12 VDC, Linear supply
Operating Temperature	32° F to 113° F (0° C to 45° C)
Operating Humidity	5% to 95% relative humidity non-condensing
Transmit Frequency	13.56 Mhz
Cable Distance	Wiegand/Clock-and-Data Interface: 500 ft (150 m) (22AWG), RS232: 50 ft (15 m), RS485: 4000 ft (1220 m), USB: 16 ft (4 m), UART: 1 ft (0.30 m).
Card Compatibility	iCLASS 15693 & 14443B - read-only on 16k bit (2k Byte), 32k bit (4k Byte); HID Application iCLASS 15693 & 14443B - read/write (RWKLB575 only) on 16k bit (2k Byte), 32k bit (4k Byte); Application Space
Certifications	UL,CE,FCC, C-Tick.
Housing Material	UL94 Polycarbonate
Resolution	500 dpi, 256-bit gray scale, 18 x 22 mm sensor area
Timing	Card read < 0.5 sec Fingerprint capture < 2 sec, typical 1 sec Verification of captured finger < 1 sec
False Accept/Reject Rate	FAR < 0.01%, FRR < 0.01%

7.24.3 Electromagnetic Lock (LED with Lamp Indicator)

Parameters	Specifications
Magnet Size	250 x 42 x 26 mm
Armature Size	180 x 38 x 11 mm
Holding Force	Up to 600 lbs
Current Drain	480 mA+/- 10% / 12 VDC
Temperature	(-10 to 55) * C (14 to 131) * F
Weight	2.0 Kg

7.24.4 Fixed Dome Cameras for Indoor Surveillance

#	Parameter	Minimum Specifications
1.	Video Compression	H.264
2.	Video Resolution	1920x1080
3.	Frame rate	25 fps in all resolutions
4.	Image Sensor	1/4" / 1/3" Progressive Scan CMOS
5.	Lens Type	Varifocal, C/CS Mount, IR Correction
6.	Lens	Fixed IRIS 2.8-10mm, F1.7, 10x digital zoom
7.	Minimum Illumination	0.9 lux
8.	Image settings	Compression, colour, brightness, sharpness, contrast, white balance, exposure control, backlight compensation, rotation
9.	Protocol	HTTP, HTTPS, FTP, SMTP, RTSP, RTP, TCP, UDP, RTCP, DHCP, UPnP, QoS, IPV4, IPV6
10.	Security	Password Protection, IP Address filtering, User Access Log
11.	Operating conditions	0 to 50°C
12.	Casing	Tamper Resistant casing for Indoor Environment

7.24.5 Door Frame Metal Detector

S. No.	Parameter	Minimum Specifications
1.	Technology	Microprocessor based
2.	No. of Zones	Minimum 6 Zones or Better
3.	Operation Frequency	User Selectable
4.	Sensitivity	100 sensitivity steps per program or better
5.	Metal Detection	Should detect: • Ferrous, Non-Ferrous, Ferrite Alloys • Uniformly in entire frame • In all orientation and • In all possible speed of interception Detection at correct zone levels without interference/false identification of adjacent zones.
6.	Alarm Signal	• Audible Alarm • Alphanumeric display & zone display • Remote alarm relay. • Option for remote zonal display unit. • Metering signals proportional to the mass of the detected target
7.	Reset Time	Minimum 0.3 seconds
8.	Traffic Light Status indicator	An LED indicating Green/Red status of the traffic light should be installed on the • Control unit display panel • Top and bottom of both side panels on the exit side of the metal
9.	Interference Suppression	• Should not interfere with adjacent installed DFMD's • Total immunity to environmental/ Radio Signals • Optimum compensation for external stationary metal
10.	Power Supply	• 220V AC 50 Hz. Mains • Battery Operated from and provided with 12V SMF battery of suitable capacity for 4 hours backup.
11.	Calibration	• Automatic & Manual • Built in Keypad • Provision for Remote control unit for parameter settings • Reset time adjustable

12.	Counter	Intelligent traffic counter for transit
13.	Safety	• Should conform to international standards of safety/radiations • Should be safe for heart pace makers • Should be data safe
14.	Self-Diagnostics	User friendly self-testing diagnostics to identify faulty condition
15.	Ambient temperature	From 0°C to 60°C
16.	Humidity	Up to 90% No Condensation
17.	Control Panel	Easily accessible, modular design with Standard plugs and connectors.
18.	Network Connectivity	• Compatibility to integrated physical security system via TCP IP • Adaptability to remote monitoring systems.
19.	Integration	• Integration with Other Access Control Devices like Turnstiles, Flap gates etc • Integration capability with cameras
20.	Construction	Light Weight, rigid, laminated side panels and cross piece, all plastic boots for panel protection base wheels for easy mobility.
21.	Standards	• Meets Electrical Safety and Compatibility Requirements • International Standards (IS) Command • CE/FCC/IEC/IEEE certified.

7.24.6 Hand Held Metal Detector

#	Parameter	Minimum Specifications
1.	Display	The HHMD may be of LED display type or of LCD display type (type offered shall be clearly indicated in the offer). The following minimum LED indications should be available in the HHMD:- • ON indication, • Metal detection indication, • Low battery Indication
2.	Dimension	Area of search coil: Minimum 125 Sq. cm
3.	Sensitivity	There will not be any sensitivity control switch and calibration shall be automatic. The number of beeps will indicate the size of metal. Sensitivity should be very high so as to easily detect the following. It shall detect objects concealed in ferrite. • Ferrous

		Coins, Paper Pin, Paper clip, Knife/Blade, Stainless steel blade • Non Ferrous Aluminium tube, Copper plate, Brass plate
4.	Audio Alarm	Audio Alarm should: • be loud enough on detection of any metal • give an idea about the size of the objects by the number of beeps Detection of objects • detect ferrous and non-ferrous metals alloys in any possible orientation • Give distinct and different audio output in case of Ferrite detection
5.	Power Source	• Rechargeable - NiCD/NiMH pack each sufficient 50 hour operation without audio and 25 hours with audio on one charge • The HHMD should have inbuilt charging capacity
6.	Construction	Light Weight, Rugged, High Impact ABS case with reinforced coil compartment
7.	Tuning	Automatic
8.	Safety	Magnetic field generated by the HHMD should be harmless to magnetic media, electronic devices and heart pace makers.
9.	Temperature	From 0°C to 50°C
10.	Standards	Should conform IS:12126:1987/CE certified
11.	Miscellaneous	• Cleaning Kit • Technical manual • User handbook

7.24.7 Boom Barriers

#	Parameter	Minimum Specifications
1.	Barrier Length	3 to 6 Meters (Depending upon Site requirement)
2.	Opening/ Closing Time	Maximum 2 secs
3.	Maximum Torque	600NM
4.	Duty Cycle	100%
5.	MCBF	Minimum 5000000 Cycles
6.	Power	230VAC

7.	Motor Power Supply	230VAC or 24VDC
8.	Operating Temperature	0 Deg C to 60 Deg C
9.	Operating Humidity	More than 95%
10.	IP Rating	IP 65 or better

8. Annexure III: Common guidelines/ comments regarding the compliance of equipment/ systems

1. The specifications mentioned for various IT / Non-IT components are indicative requirements and should be treated for benchmarking purpose only. Bidders are required to undertake their own requirement analysis and may propose higher specifications that are better suited to the requirements.

2. Any manufacturer and product name mentioned in the Tender should not be treated as a recommendation of the manufacturer / product.

3. None of the IT / Non-IT equipment's proposed by the Bidder should be End of Life product. It is essential that the technical proposal is accompanied by the OEM certificate in the format given in Section 5.11 (Form 10) of Volume I of this Tender, where-in the OEM will certify that the product is not end of life & shall support for at least 7 years from the date of Bid Submission.

4. Technical Bid should be accompanied by OEM's product brochure / datasheet. Bidders should provide complete make, model, part numbers and sub-part numbers for all equipment/software quoted, in the Technical Bid.

5. Bidder should ensure that only one make and model is proposed for one component in Technical Bid for example all workstations must belong to a single OEM and must be of the same model etc.

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

7. All equipment, parts should be original and new.

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

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

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

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

12. The Successful Bidder should also propose the specifications of any additional hardware/Non IT infrastructure, if required for the system.

13. The design consideration of the system is given in this volume. The Successful Bidder must provide the architecture of the solution it is proposing.

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

15. All the hardware and software supplied should be from the reputed Original Equipment Manufacturers (OEMs) and approved by BSCDCL.

16. All licenses should be in the name of the BSCDCL and should be Perpetual.

17. The proposed solution of MSI should meet the minimum specification requirements for respective component, bidder need to size the solution components to meet the project requirement. In case any of the system / appliance could not meet the performance requirement during the implementation testing or operations phase, MSI will be responsible to change the same with equivalent/better product without any additional cost to BSCDCL.

18. All components to be maintained in redundancy with Active - Active / Active- Passive Clustering based on the SLA requirements, architecture and performance. Bidder need to provide the compliance with respect to each clause and clear reference-able document, highlighting how the stated requirement is being met. All components should be sized to meet the required performance and SLA level when one of the redundant devices is down.

19. The proposed solution should be optimized for power, rack space, bandwidth while ensuring high availability and no single point of failure across the architecture.

20. The proposed systems and IT Infrastructure components like servers, storage, network etc. should be of enterprise class and must be current as per OEMs latest offering, in line with advancements of technology in these domains. Bidder need to provide the published benchmarks for the stated systems along with the sizing assessment sheet being certified by the OEM for the stated systems. All the components should be able to handle expected loads and provision the desired transaction times and throughputs.

21. The proposed systems and IT infrastructures components like servers, storage, network devices and software systems should be latest as per current technology trends and it should be upgradable. It is MSI's responsibility to proactively take care of system obsolescence planning. The systems should not become obsolescent before 5 years (of O&M). For proposed hardware and software systems, support from OEMs should be available for at-least 5 years (of O&M). Failing which it will be MSI's responsibility to provide support free of cost for initial 5 years of O&M.

22. Servers should be based on x86 platform in high density form factor to ensure optimal power and space usage. However, bidder may suggest rack form factor for any specific server usage,

stating clearly the benefits being derived without compromising on the power and cooling factors.

23. The database layer should utilize the database servers for consolidating the database requirements. The architecture should have horizontal scalability. Benefits/additional security, reliability, availability features at the server level architecture would be given due consideration during evaluation

24. Redundancies/teaming should be maintained at different interconnecting fabrics so as to avoid any single point of failure / performance bottleneck

25. Networking equipment should be capable of processing IPV4 & IPV6 traffic. Security features that are delivered shall be IP v 6 ready.

26. All devices should be IPv4 and IPv6 ready from day-1. MSI shall deploy IPv4 and IPV6 dual stack supported network from day-1. The proposed solution and all appliances should meet this requirement. The MSI shall also be responsible for security adherence on both IPv4 and IPv6.

27. Bidder should utilize virtualization technology to optimise the solution and provide benefits for the overall Cost of ownership and ease of maintenance.

28. Proposed environment at DC should support set up and operations of multiple OEMs / brands of servers and storage without having any compatibility issue.

29. In future if BSCDCL plans to monetize the project, MSI should not have any objection. Rather it will be expected by the MSI to provide full support to BSCDCL.

30. If BSCDCL decides to retain the command centre operators (some or all or none) provided by MSI after the project tenure, MSI will not have any objection.

31. The IT infrastructure proposed for BSCDCL system should comply with the below :

S. No.	Item	To be provided of the OEM listed in latest Gartner report (2015-2016)	Quadrant
1.	Servers (x86)	Magic Quadrant for Servers	Leaders/Challengers
2.	Storage	Magic Quadrant for Storage & Disk Arrays	Leaders/Challengers
3.	Network Equipment: Switches & Routers	Magic Quadrant for Data Centre Network Infrastructure	Leaders/Challengers
4.	Firewall	Magic Quadrant for Enterprise Network	Leaders/Challengers

S. No.	Item	To be provided of the OEM listed in latest Gartner report (2015-2016)	Quadrant
		Firewalls,	
5.	Endpoint Protection (Anti-Virus)	Magic Quadrant for Endpoint Protection	Leaders/Challengers
6.	Database (RDBMS)	Magic Quadrant for Operational Database Management Systems	Leaders/Challengers
7.	Document Management System	Magic Quadrant for Enterprise Content Management	Leaders/Challengers

- Bidder need to submit a copy of relevant section of the Gartner report along with technical proposal.

* During the Demonstration at technical evaluation stage, the Technical Committee will give special attention to verify the quality, robustness and appropriateness of the proposed cameras for field scenario/conditions. If any brand / product are found un-suitable, Bidder may get dis-qualified or may be asked to replace the product with better brands meeting the tender requirements, without any change in commercial bid.

9. Annexure IV: GIS Layers

BSCDCL has prepared a GIS application for providing GIS MAP based services. GIS layers are already created under GIS application for BSCDCL. The details of the GIS Layer is given in below table:

GIS Layer Category	GIS Layer Sub-category	Description
Boundary	Vidhan Sabha Boundary	Vidhan Sabha Name
	Village Boundary	BHU code
		Village Name
	Ward Boundary	Ward No
		Ward Name
		Zone No
		Population
		SC Population
		ST Population
		Assembly Constituency
		Corporator Name
		Ward Officer
		Zone Officer
		Corporator Number
		Ward Officer Number
		Zone Officer Number
	Plot Boundary	
	Zone Boundary	Zone No
		Zone Officer Name
		Zone Officer Number
	BMC Boundary	Total Zones
		Total Wards
		Total Population
		SC Population
		ST Population
	Planning Boundary 2031	
		State Name
		State Code
		City
Commercials	Automobile Showroom	Name
		Category
		Locality
		Road Name
		Address
		Website
		Email

		Phone
	Business	Name
		Locality
		Road Name
		Address
		Website
		Email
		Phone
	Industries	Name
		Locality
		Road Name
		Address
		Website
		Email
		Phone
	Godown	Name
		Locality
		Road Name
		Address
		Website
		Email
		Phone
	Commercial Building	Name
		Locality
		Road Name
		Address
		Website
		Email
		Phone
	Workshop	Name
		Locality
		Road Name
		Address
		Website
		Email
		Phone
Education	College	Name
		Locality
		Address
		Website
		Email
		Phone
	Learning Institute	Name
		Locality

		Road Name
		Address
		Website
		Email
		Phone
	Library	Name
		Locality
		Road Name
		Address
		Website
		Email
		Phone
	University	Name
		Locality
		Road Name
		Address
		Website
		Email
		Phone
	School	Name
		Locality
		Road Name
		Address
		Website
		Email
		Phone
	Engineering College	Institute Type
		Address
		Phone
		Email
		Image
		Name
Emergency	Police Station	Name
		Category
		Locality
		Address
		Phone
	Fire Station	Name
		Website
		Email
		Phone
		Image
Financial Services	Financial Company	Name
		LOcality
		Road Name
		Address

		Website
		Email
		Phone
	Insurance Company	Name
		Category
		Road Name
		Address
		Website
		Email
		Phone
	ATM	Name
		LOcality
		Road Name
		Address
		Website
		Email
		Phone
	Bank	Name
		LOcality
		Address
		Website
		Email
		Phone
Fuel Stations	Petrol Pump	Name
		LOcality
		Road Name
		Address
		Website
	Gas Agency	Address
		Contact Number
		Name of Proprietor
		Customer Care No
		Mobile
Government Office	Government Office	Name
		Locality
		Road Name
		Address
		Website
		Email
		Phone
Health Services	Medical Store	Name
		Address
		Website
		Email
		Phone
	Medical Facilities	Name
		Category

		Locality
		Road Name
		Address
		Website
		Email
		Phone
	Hospital	Name
		Address
		Website
		Email
		Phone
	Dispensary	Name
		Category
		Address
		Website
		Email
		Phone
	Clinic	Name
Market Places	Shopping Centre	Name
		Locality
		Address
		Website
		Email
		Phone
	Shop	Name
		Locality
		Address
		Website
		Email
		Phone
	Haat Bazar	Category
		Opening Day
		Name
	Major Malls	Name
		Address
		Website
		Email
		Phone
Public Services	Toilets	Address
		Image URL
		Name
	Parking	City Name
		Catagory
		Area
		Name
	Crematorium Ground	Name
		Category

		Locality
		Address
		Website
		Email
		Phone
	Post -Office	Name
		Category
		Locality
		Road Name
		Address
		Website
		Email
		Phone
	Rainbasera	Category
		City
		Zone & Ward No
		Daily Staying Persons
		Rainbsera Officer Name
		Rainbasera Officer Contact No
		Drinking Water Availability
		Light Availability
		Toilet Availability
		Locker Availability
		AC Availability
	Community Hall	Name
		Category
		Locality
		Address
		Website
		Email
		Phone
Religious	Temple	Name
		Address
	Masjid	Name
		Address
	Gurudwara	Name
		Address
	Church	Name
		Address
	Ashram	Name
		Category
		Locality
		Road Name
		Address
Residential	Hostel	Name
		Address
		Website

		Email
		Phone
	Apartment/Buildings	Name
		Address
		Website
		Email
		Phone
Sports and Youth Services	Sports Stadium	Name
		Category
		Address
		Phone
	Swimming Pools	Name
		Category
		Phone
	Bus Stop Up	Status
		Name
		Bus Route
	Bus Stop Down	Status
		Name
		Bus Route
	Railway Station	locality
		Name
		Phone
	Railway Line	Type
		Name
		Category
		Locality
		Road Name
		Address
		Website
		Email
		Phone
	Roads	
Tourism & Recreation	Cinema Hall	Address
		Phone
		Email
		Image URL
		Website
		Image
		Name
	Hotel	Name
		Category
		Locality
		Address

		Website
		Email
		Phone
	Restaurant	Name
		Locality
		Road Name
		Address
		Website
		Email
		Phone
	Club	Name
		Category
		Locality
		Address
		Website
		Email
		Phone
	Recreation	Name
		Address
	Scenic	Name
		Address
Utility	Water Tank	Name
		Address
		Locality
	Electric Substation	Name
		Address
		Locality
	Solid Waste Dumping Yard	Ward No
		Catagory
		Name
Urban Poor Housing	Slums	Populations
		House Holds
		Name
	Rajiv Awas Yojana (RAY)	Land Value
		Ward No
		Populations
		House Holds
		Name
		Land Owner
	Basic Services For Urban Poor	Category
		Total House
		Name

10. Annexure V- ICCC -Design Consideration

10.3 Key Design Considerations

Key design considerations taken into account are as follows –

- System is Designed for Projected Population of 2031.
- Designed for 24x7 online availability of application.
- Scalable solution on open protocols
- No propriety devices/ applications
- API based architecture for Integration with other web applications and Mobile applications

The key guiding principles considered for building the integrated Smart Governance solution are the following:

- **Transformational nature of Smart City applications** - Instead of imitating paper process in electronic form, applications should look to fully embrace mobile adoption, digital signature, online authentication, etc. to transform the processes completely and offer wider choice and no/low touch point for residents to interact directly. It is critical that project design are aligned to larger trends and designed for next decade rather than past.
- **Continuous adoption of rapidly evolving Technology** - Technology evolves too fast and Government projects similar to Smart City with its long procurement cycles do not align naturally to adapt to this trend. Also, any changes to existing implementations require contract changes, new RFP (Request for Proposal), etc. Hence the entire system would be built to be open (standards, open API, plug-n-play capabilities like virtual environments ,creating sandbox), components coupled loosely to allow changes in sub-system level without affecting other parts, architected to work completely within a heterogeneous compute, storage, and multi-vendor environment. Simulated services environment can help agencies to save cost, Infrastructure and time in testing multiple application integrations.
- **Selection of best solution at best rate as and when required** - Large integrated systems of Smart City operations should be designed to get best cost and performance advantages of natural technology curve (constant increase of speed and decrease of cost) and still aligned to open procurement practices of the Government. For this to happen, architecture should be open and vendor neutral, use commodity hardware, and designed for horizontal scale. This allows buying of commodity compute, storage, etc. only when needed at best price.
- **Distributed Access and Multi-channel service delivery -**With high penetration of mobile devices and very large percentage of internet usage using mobile devices, it is imperative that the Smart City applications provide multiple channels of service delivery

to its stakeholders. An important consideration is that the access devices and their screen capabilities (including browser variations) are numerous and constantly evolve. Hence, it is imperative to design the system such that the ecosystem of Smart City-integrated mobile apps also evolves.

- **Security and privacy of data** - Security and privacy of data within the integrated Smart City system will be foundational keeping in view of the sensitivity of data and critical nature of the infrastructure envisioned to be built for Smart City operations. Security and privacy of data should be fundamental in design of the system without sacrificing utility of the system. When creating a system of this scale, it is imperative that handling of the sensitivity and criticality of data are not afterthoughts, but designed into the strategy of the system from day one.
- **Provision of a Sustainable, Scalable Solution-** The motive of the technological enhancements to provide a system that would be sustainable for the next few years. The expectation is that the system should sustain at least 10 years from GO-Live. The solution would be done keeping in mind the scalability of the system. The simplified procurement processes and ease of compliance is expected to lead to huge growth in contract's base. Every component of BSCDCL system needs to scale horizontally to very large volume of data.

The Application Software will have the capability to scale up to tomorrow's requirements like given below:

- Managing the entire Property Life Cycle (Data Collaboration between various govt. departmental systems)
- Maintaining Information on Citizen Life Cycle (Right from Birth to Marriage, Health, Education, Driving License, Interactions with BSCDCL)
- **API Approach-** BSCDCL has decided to adopt Open API as the guiding paradigm to achieve the above goals. Though BSCDCL system would develop a portal but that would not be the only way for interacting with the BSCDCL system as the stakeholders via his choice of third party applications, which will provide all user interfaces and convenience via desktop, mobile, other interfaces, will be able to interact with the BSCDCL system. These applications will connect with the BSCDCL system via secure BSCDCL system APIs. This architectural approach has been taken as the UI based integration through a ubiquitous web portal requires manual interaction and does not fit most consumption scenarios. The following benefits are envisaged from API based integration,
    - Consumption across technologies and platforms(mobile, tablets, desktops, etc.) based on the individual requirements
    - Automated upload and download of data
    - Ability to adapt to changing taxation and other business rules and end user usage models
    - Integration with customer software (GIS, Accounting systems).
    - Simulated services environment can help agencies to save cost, Infrastructure and time in testing multiple application integrations.
    - Open APIs should have a security and management layer for all interfaces.

- **Business Rule Driven Approach-**All configurations including policy decisions, business parameters, rules, etc. shall be captured in a central place within the system. The system shall provide facility to the decision makers to add new or edit/delete existing policies or make changes with appropriate permission control and audit trace. Managing these in a central repository ensures only once source of truth is used across many application servers and reduces issues of inconsistent application behaviour. Decoupling of the business parameters/rules/master data from the rest of the solution architecture and making them configurable allows for a great deal of flexibility.
- **Data Distribution Service-**As a future roadmap it is envisaged that the functionalities provided by the BSCDCL Smart City system should be available as services that could be offered to other stakeholders on request. Keeping this in mind the system shall be able to provide data on subscription-publication basis. The organization of the information exchange between modules is fundamental to publish-subscribe (PS) systems. The PS model connects anonymous information producers (publishers) with information consumers (subscribers). The overall distributed application (the PS system) is composed of processes. The goal of the DDS architecture is to facilitate efficient distribution of data in a distributed system. Participant using DDS can 'read' or 'write' data efficiently and naturally with a typed interface. Underneath, the DDS middleware will distribute the data so that each reading participant can access the 'most current' values.

10.4 Guiding Architecture Principle

The IT architecture principles defined in this section are the underlying general rules and guidelines that will drive the subsequent development, use and maintenance of architectural standards, frameworks and future state target architecture.

BSCDCL system will be built on the following core principles:

10.4.1 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 BSCDCL system is envisaged as a faceless system with 100% API driven architecture at the core of it. BSCDCL portal will be one such application on top of these APIs, rather than being fused into the platform as a monolithic system.

Open APIs designed to be used form the core design mechanism to ensure openness, multi-user ecosystem, specific vendor/system independence, and most importantly providing tax payers and other ecosystem players with choice of using innovative applications on various devices (mobile, tablet, etc.) that are built on top of these APIs.

10.4.2 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.

10.4.3 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.

10.4.4 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.

10.4.5 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.

10.4.6 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/MSI pre-existing product or work must be wrapped in a vendor neutral API so that at any time the OEM product can be replaced without affecting rest of the system. In addition, there must be at least 2 independent OEM products available using same standard before it can be used to ensure system is not locked in to single vendor implementation.

10.4.7 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.

10.4.8 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
  - Support integration with native device API
  - Support utilization of all native device features
  - Support development of applications in a common programing language
  - Support integration with mobile vendor SDKs for app development and testing
  - Support HTML5, CSS3, JS features for smartphone devices
  - Support common protocol adapters for connection to back office systems (i.e. HTTP, HTTPS, SOAP, XML for format)
  - Support JSON to XML or provide XHTML message transformations
  - Support multi-lingual and language internalization
  - Support encrypted messaging between server and client components

10.4.9 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 BSCDCL system should be prevented
- Ensure minimum data loss(expected zero data loss)

10.4.10 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.

10.4.11 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.

10.4.12 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.

10.4.13 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

10.5 Integration Architecture

This section recommends the proposed integration architecture aligning with the overarching architectural principles.

The following are the integration specifications for the various integration scenarios -

Real-time integration

All the Smart City applications will be deployed in the Data Center while any external application of the Smart City ecosystem will reside in outside premises.

The need for a Service Oriented Architecture (SOA) and API Governance architecture is felt that will facilitate BSCDCL in defining an enterprise integration platform. An SOA and API Lifecycle Management platform will help in data exchange across applications in real-time mode (both synchronous and asynchronous), promote loose coupling with ease of maintenance and change, facilitate rapid composition of complex services, achieve scalability through modularity, and improved business visibility and help secure API based business critical transaction.

SOA /API is an architectural style that allows the integration of heterogeneous applications & users into flexible and lightweight architecture. Discrete business functions contained in enterprise applications could be organized as layers of interoperable, standards-based shared "services" that can be combined, reused, discovered and leveraged by other applications and processes. The proposed integration architecture is depicted below. All real-time data integration across the enterprise applications will be through middleware based enterprise integration platform.

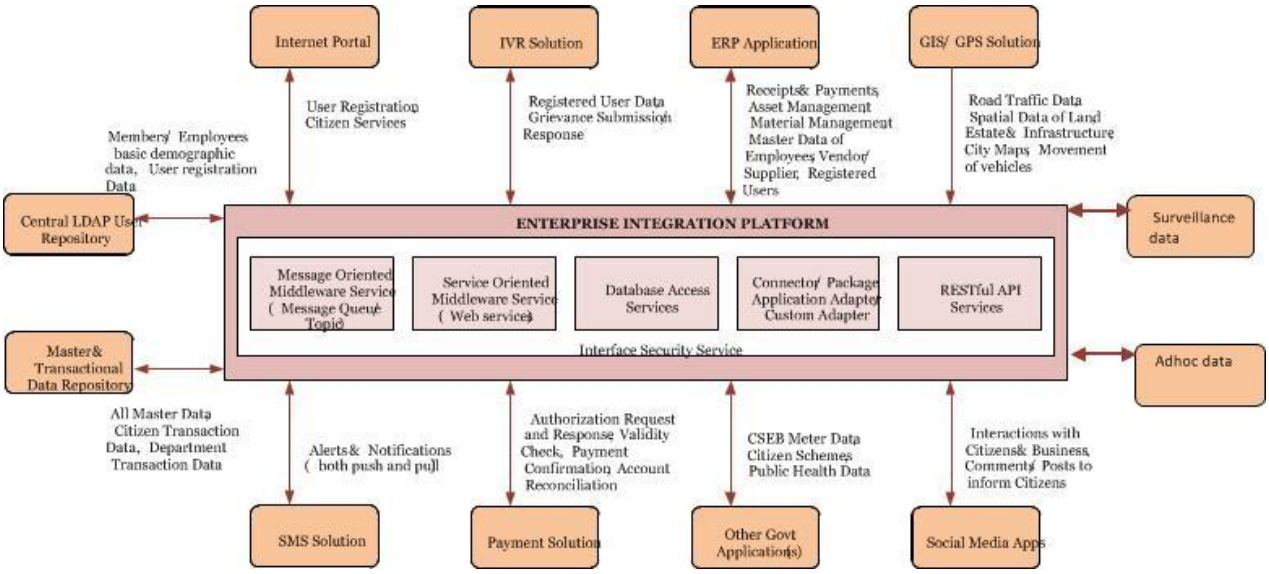


Figure 1: Integration Framework

The following are the various integration modes and techniques that could be leveraged -

- SOAP / REST web service based interfacing technique will be leveraged as the real-time point to point synchronous integration mode with external or third party systems. The following integration points could be considered for SOAP web service based interfacing -
    - Payment gateway of the authorized banks to enable authorized users make financial transactions for the Smart City services availed by them. This should support a unified interface to integrate with all Payment Service Providers using web services over secured protocols.
    - Should protects against threats and OWASP vulnerabilities and controls access with Single Sign-On and identity management, providing end-to-end security for apps, mobile, and IoT.
    - Solution should be able to protect against cross-site scripting (XSS), injection attacks (Xpath SQL , XQuery etc.) and DoS attacks.
    - SMS application, acting as the SMS Gateway, will make use of Java Communication APIs for SMS communication to GSM network using the GSM modem, which can be both event-driven as well as time-driven. The API will be exposed to initiate the broadcasting or alert notification.
    - Social Media Apps and NoSQL data stores to exchange photos, videos and message feeds, based on interactions with Citizens and Business as well as comments/posts to inform stakeholders
    - IVR/Customer Support solution with ERP and Transactional Data Repository to exchange citizen and business demographic, registration and payment data as well as transactional data related to citizen services and municipal operations.
    - GIS/GPS solution with traffic management, surveillance and land & estate management applications to capture the data pertaining to location traces left by GPS-enabled smartphones and Wi-Fi network logins, road traffic condition, movement of vehicles and spatial data of land, estate and Smart City infrastructure.

- Message based interfacing technique will be leveraged for real-time asynchronous integration mode. The following integration points could be considered for message based interfacing -
    - Central LDAP with ERP to synchronize member and employee user registration data
    - Payment solution and ERP to exchange payment data for tracking of beneficiary's payment transactions against different services (citizen, workers, transporter, vendor), master data (employee, vendor/supplier, location, facilities, price table)
    - Employee attendance data with ERP (HR Module) to capture data pertaining to employee location and attendance
    - Departmental applications with ERP (Asset Management module) to exchange data for procurement and maintenance of any assets or infrastructure items for each department.
    - Municipal operations application with ERP (Material Management module) to capture materials related transaction and inventory data for public works
    - Other government applications with Smart City application to exchange data for government procurement, public health schemes, welfare schemes, citizen health and BEB meters.
- RESTful API service based interfacing technique will be leveraged for the following integration areas-
    - Access and use of various services provided by the different departments for citizens and business community will be done through a RESTful, stateless API layer.
    - Access and use of various internal functions related to operations and administration of Smart City for departmental and BSCDCL 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 BSCDCL 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 BSCDCL, but it is a mandatory requirement that all the SMS based services (alerts and notifications) should be available as part of the solution. Following are some of the key requirements for the SMS services through the solution:

- Should contain required details/information and targeted to the applicant or designated officers of tax departments and other stakeholders and users as per prevailing TRAI norms
- Facilitate access through access codes for different types of services
- Support automated alerts that allows to set up triggers that will automatically send out reminders
- Provide provision for International SMS
- Provide provision to receive messages directly from users
- Provide provision for personalized priority messages
- Resend the SMS in case of failure of the message
- Provide messaging templates

Email Services: Email services are envisaged to be made available as part of the solution design to send alerts/intimations/automated messages to registered email ids, based on preferences set up/opted by individual users. An authenticated SMTP mail service (also known as a SMTP relay or smart host) is envisaged to be integrated with the solution for sending mail from the solution, and delivered to intended inbox. Support antispam features.

Payment Gateway: The solution is envisaged to have integration with payment gateways, to enable authorized Users make financial transactions, as per rights and privileges provided to him/her. The service provider is required to make the provisions for integration with such third party gateways and provide payment services, as per requirement of the BSCDCL. Some of the key features of payment gateway are mentioned below:

- Should support secure integration with Payment Service Providers
- Should support a unified interface to integrate with all Payment Service Providers
- Should support integration with Payment Service Providers using web services and over HTTP/S protocol
- Should manage messages exchange between UI and payment service providers
- Should support beneficiary's payment transactions tracking against various services
- Should support bank accounts reconciliation
- Should provide logs for all transactions performed through the Payment Gateway for future financial dispute resolution that might arise between entities and either beneficiaries or Payment Service Providers
- Should maintain and keep transactions logs for time period required and specified by the financial regulations followed in country

- Should support redundant Payment Discovery
- Should submit Periodic Reconciliation Report to government entities
- Should support transaction reports to monitor and track payments
- Should support real-time online credit card authorization for merchants
- Should support compliance with emerging trends and multiple payment options such debit card, credit card, cash cards and other payment gateways
- Should provide fraud screening features
- Should support browser based remote administration
- Should support multicurrency processing and settlement directly to merchant account
- Should support processing of one-time or recurring transactions using tokenization
- Should support real time integration with SMS and emails

IVR Services: IVR services are envisaged as part of Call Centre facility, which will be integrated with the solution, to provide information and services to the people who would contact the Call Centre: Some of the key features of the IVR services are mentioned below:

- Should provide multi-lingual content support
- Should facilitate access through access codes for different types of services
- Should support Web Service Integration
- Should support Dual Tone Multi Frequency (DTMF) using telephone touchpad - in-band and out-of-band
- Should support for Voice Extensible Markup Language (VoiceXML)
- Should support speech recognition that interprets spoken words as texts (Advanced Speech Recognition).
- Should support playing of pre-recorded sounds
- Should support redirection to human assistance, as per defined rules
- Should be able to generate Data Records – (CDRs) and have exporting capabilities to other systems
- Should provide provision for voice mailbox and voice recognition

There are multiple ways of integration of the solution with other systems is envisaged. These may be through Web Services, Message Queuing, File based or API based. The integration and data sharing mechanism may be either in Batch Mode or Needs basis (synchronous or asynchronous). Some of the key requirements of the interface/integration are mentioned below:

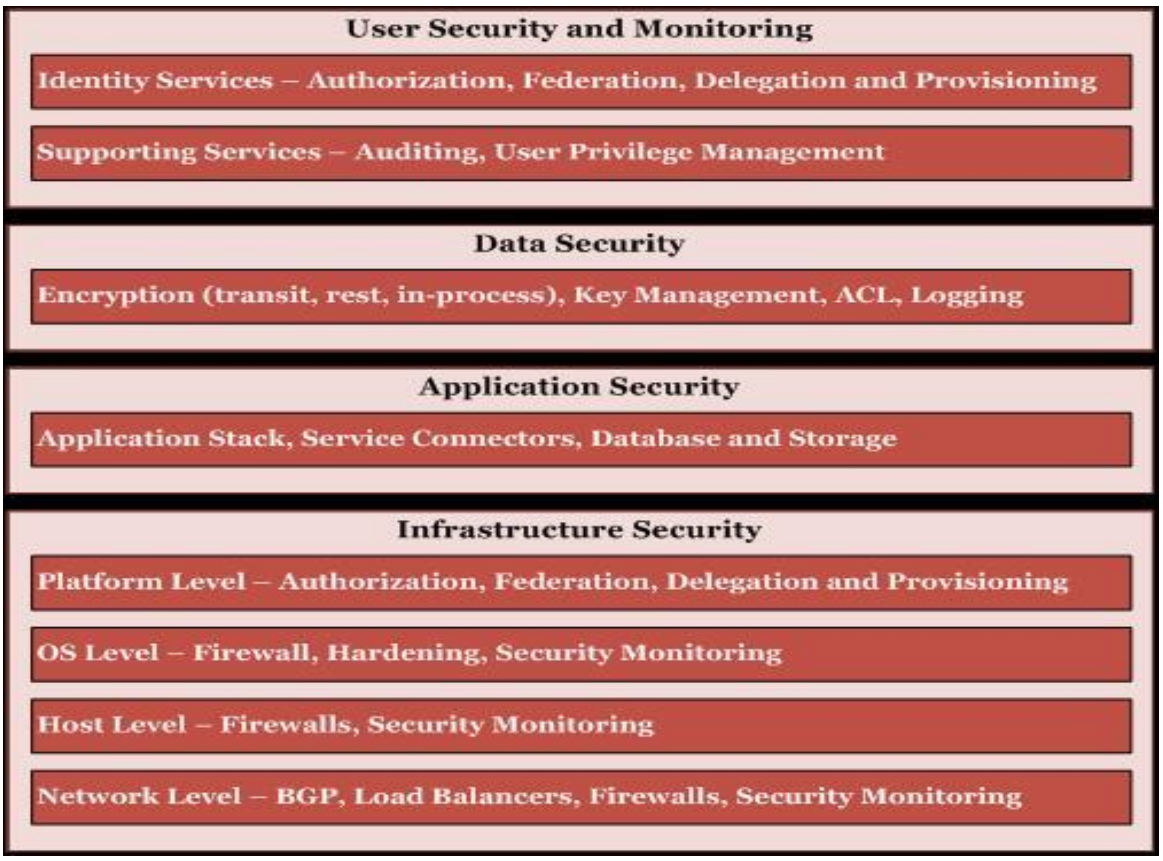
- Interface Definition
- Interface Owner
- Interface Type
- Interface Format
- Frequency
- Source System
- API/Service/Store Procedure
- Entitlement Service
- Consuming System
- Interface Layout (or) Schema

- Should have provision for exceptional scenarios
- Should have syntax details such as data type, length, mandatory/option, default values, range values etc.
- Error code should be defined for every validation or business rule
- Inputs and outputs should be defined
- Should be backward compatible to earlier datasets
- Data exchange should provide transactional assurance
- Response time and performance characteristics should be defined for data exchange
- The failover scenarios should be identified
- Data exchange should be auditable

10.6 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.



Some of the key security principles are explained below.

MSI must comply with the Cyber Security Model framework circulated vide Ministry of Urban Development's OM No. K-15016/61/2016-SC-I dated 20th May 2016 and another guidelines issued by MoUD for Control and Command Center.

10.6.1 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.

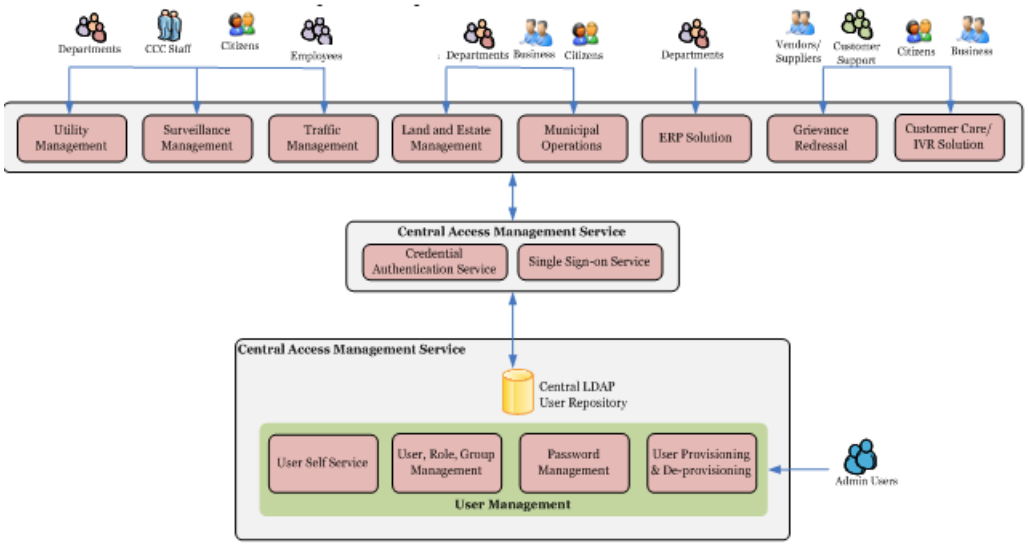
- For applications handling sensitive data it is recommended that in the least one factor authentication key in the form of a password is essential. Strong password complexity rules should be enforced to ensure confidentiality and integrity of the data
- For applications handling highly sensitive data 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 BSCDCL 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

10.6.2 Data Security

Traditional Structured Enterprise Data

BSCDCL 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 BSCDCL 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 BSCDCL 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 behaviour.

Additionally for any service based on cloud environment, there are three main security challenges namely multi-tenancy, divided responsibility and dynamic environment. In this context, one of the key concerns for the customers would be protection of sensitive/confidential/personal data through access control, encryption, integrity and origin verification.

In cloud environments, the amount of data at rest, in transit and in use is considerably larger than in traditional networks. So the following technologies should be considered to discover and remedy security vulnerabilities related to integrity protection of data to be used by the IT systems of BSCDCL 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.

10.6.3 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
- For effective prevention of SQL injection vulnerabilities, MSI should have monitoring feature of database activity on the network and should have reporting mechanism to restrict or allow the traffic based on defined policies.

10.6.4 Infrastructure Security

The following focused initiatives to discover and remedy security vulnerabilities of the IT systems of BSCDCL Smart City should be considered to proactively prevent percolation of any threat vectors -

- Deploy anti-virus software to all workstations and servers to reduce the likelihood of security threats;
- Deploy perimeter security technologies e.g. enterprise firewalls to reduce the likelihood of any security threat;
- Deploy web content filtering solutions to prevent threats from compromised websites to help identify and block potentially risky web pages;
- Install enterprise-level e-mail anti-security software to reduce vulnerability to phishing and other e-mail security spams. This would check both incoming and outgoing messages to ensure that spam messages are not being transmitted if a system becomes compromised.
- Perform periodic scanning of the network to identify system level vulnerabilities
- Establish processes for viewing logs and alerts which are critical to identify and track threats and compromises to the environment. The granularity and level of logging must be configured to meet the security management requirements.
- Deploy technology to actively monitor and manage perimeter and internal information security.
- Deploy network Intrusion Detection System (IDS) on the perimeter and key points of the network and host IDS to critical systems. Establish process to tune, update, and monitor IDS information.
- In case of cloud deployment, cloud services can be disrupted by DDoS attacks or misconfiguration errors which have the potential to cascade across the cloud and disrupt the network, systems and storage hosting the cloud application.
- Deploy security automation techniques like automatic provisioning of firewall policies, privileged accounts, DNS, application identity etc.

Physical Security of ICCC Premises

- MSI will be required to do the physical security arrangements for the ICCC premises during contract period.

- MSI will be required to manage the access cards and access control for ICCC premises during contract period.

- MSI will be required to provide security guards at the ICCC premises during contract period.

- Physical security arrangements should be 24*7, as the operations of ICCC is conceived to be 24*7.

Network Security for Smart Devices

The core principles of security for any smart device network rest on the three most important data security concerns of confidentiality, integrity and authentication. Hence the security for smart device networks should primarily focus on the protection of the data itself and network connections between the nodes. From a network perspective, following are to be considered for designing the smart devices network -

- Protection of fair access to communication channels (i.e. media access control)
- Concealing of physical location of the nodes
- Defence against malicious resource consumption, denial of service, node capturing and node injection
- Provision for secure routing to guard the network from the effects of bad nodes
- Protection of the mobile code

Smart devices have a triple role in most networks - data collectors, processors and traffic forwarders for other devices in the network. The typical attacks for which countermeasures are to be defined and implemented are: Radio Jamming, Nodes Reporting Wrong Data, Data Aggregation Attacks and Battery Attacks.

The following guidelines need to be considered for security enhancement of smart devices and their networks:

- Use of IP-based network for smart devices
- Use of Link Layer Security for password-based access control and encryption
- Protection of smart devices nodes behind a firewall for carrying out SSL-based application data transfer and mechanism to avoid distributed DoS attacks
- Public-key-based authentication of individual devices to the network and provisioning them for secure communications
- Conformance of the security solution to the standards of IETF, IEC and IEEE to ensure maximum security and interoperability, with support for the following commonly used protocols at a minimum - IPSec/IKE, SSH and SSL/TLS

Software Defined Security at Application End Points

- Deploy Software Defined Security Architecture at the Virtualization layer at the Host level to guarantee that each and every Application gets its security policy and enforcements at the point closest to its existence.
- The Software Defined Security (SDS) architecture should be able to enforce the Security Policy at the Virtual NIC level of the Application VM thus offering highest and closest level of security.
- The SDS should allow the Firewall Policy to be tied to each Virtual Machine and the policy should automatically move with the movement of the Virtual Machine, thus bringing Security Policy Portability.
- The Software Defined Security Architecture offers the integration of Industry leading solutions around Antivirus, Anti Malware, IPS, Next Generation Firewall etc. to be integrated in the Security Policy template through Service Insertion or Service Chaining.
- The SDS Framework to be deployed which should create virtual / logical Application or Service isolation from each other, dynamically controlled through template or blueprint, thus creating an environment or architecture of Risk or Breach Containment, post any successful security breach.
- The SDS should be able to instantaneously provision security policy through templates or by creating unique Security Groups of the VMs based on Operating Systems, Workload Type (Web, App or DB), Machine Name, Services running, Regulatory requirement etc. and apply Automated and Centralised Security Policy based on this context or grouping.

10.7 Software Development Lifecycle

Continuous Build and Deployment

The Bhopal Smart City system should be highly modular and parallel development should be carried out for faster execution using industry's best Software Development Lifecycle practices. All application modules within the same technology platform should follow a standardized build and deployment process.

At its core, Continuous Delivery is all about releasing high-quality software to the market faster and with less effort—a simple goal, but one that requires new thinking around the people, processes and technologies driving your application delivery efforts.

A set of practices and principles in software engineering aimed at, building, testing and releasing software, faster and more frequently. These principles help reduce the cost, time and risk of delivering changes, and ultimately value, to customers by allowing for more incremental changes to applications in production.

With an application release automation, teams can easily plan and create a comprehensive release plan that incorporates tasks performed by third party tools and orchestrates the promotion from one environment to the next, streamlining the entire process to eliminate hand-offs.

Simplifying build and configuration of new environment instances means testing can occur early and often. Defects and errors are found sooner in the cycle to significantly reduce re-work. Teams have easy access to the test data they need to create real-world 'production-like' environments that enable more thorough testing and yield more accurate results, so errors or defects are discovered long before an app is deployed to production, so there's no negative impact to customer experience.

A dedicated 'development / customization' environment should be proposed and setup. The MSI must provision separate development and testing environment for application development and testing to simplifying build and configuration of new environment instances means testing can occur early and often. Defects and errors are found sooner in the cycle to significantly reduce re-work. Teams have easy access to the test data they need to create real-world 'production-like' environments that enable more thorough testing and yield more accurate results, so errors or defects are discovered long before an app is deployed to production, so there's no negative impact to customer experience. Any change, modifications in any module must follow industry standard processes like change management, version control and release management in large and complex application development environment.

Application source code could be maintained in source control and could be broken up into a number of projects. Source control projects are created to abstract related set of modules or feature that can be independently included in another application.

It is a mandatory to create, update and maintain all relevant documentation throughout the contract duration. Also it should be ensured that a bug tracking toll is maintained for proper tracking of all bugs fixes as per various tests conducted on the application.

10.8 Quality Assurance & Audit

A thorough quality check is proposed for the Bhopal Smart City system and its modules, as per standard Software Development Life Cycle (SDLC). MSI is expected to lay down a robust Quality Assurance program for testing of the developed application for its functionality, performance and security before putting in production environment. The program must include an overall plan for testing and acceptance of system, in which specific methods and steps should be clearly indicated and approved by BSCDCL. MSI is required to incorporate all suggestions / feedback provided after the elaborate testing of the system, within a pre-defined, mutually agreed timeline. MSI must undertake the following:

- Outline the methodology that will be used for testing the system.
- Define the various levels or types of testing that will be performed for system.
- Provide necessary checklist/documentation that will be required for testing the system.
- Describe any technique that will be used for testing the system.
- Describe how the testing methodology will conform to the requirements of each of the functionalities and expected outcome.
- Using simulated test environment in order to find the defects and bugs in much earlier SDLC so that they do not escape into next phase/environment.
- Indicate / demonstrate to BSCDCL that all applications installed in the system have been tested.

10.8.1 Automated Testing

MSI is expected to perform automated testing with following features:

- Should support multi-layer test scenarios with a single solution.
- Should support and execute testing on GUI and UI-Less (standard Web Services, non-SOAP Web Services, such as REST, etc.) Components.
- Should allow version control of tests and test assets providing ability to compare versions and identify changes.

- Should allow centralized storage and management of tests and test assets including external resources used by tests.
- Should have an IDE environment for QA engineers which should be configurable.
- Should provide local system monitoring to test and validate performance issues including memory leakage, CPU overload and network overload to determine if specific business scenarios exceed desired performance thresholds.
- Should provide Auto-documentation while creating of automated tests.
- Should generate reports that can diagnose defects and can be exported to (PDF, XML , Html) (mandatory) and doc (optional) formats.
- Report with summary data, pie charts and statistics for both the current and previous runs needs to be provided.
- Should enable thorough validation of applications through a full complement of checkpoints such as GUI object, database, XML, XPath, etc.
- Should provide Unicode support for multilingual application testing.
- Should be able to record the test Execution into a video file for viewing later.
- Should provide facility to parameterize tests to generate/assign test case output values automatically during runtime.

10.8.2 Performance and Load Testing

MSI is expected to implement performance and load testing with following features:

- Testing workload profiles and test scenarios based on the various functional requirements should be defined. Application as well as system resource utilization parameters that need to be monitored and captured for each run also needs to be defined.
- Should support application testing and API testing including HTTP(s), web services, mobile applications and different web 2.0 frameworks such as Ajax/Flex/HTML5.
- MSI should perform the load testing of Bhopal Smart City system for multiple workload profiles, multiple scenarios, and user loads to handle the envisaged users of the system.
- Different activities before load testing i.e. identification of work load profiles, scenarios, information capturing report formats, creation of testing scripts, infrastructure detailing and workload profile should be prepared before the start of actual load testing exercise.
- Solution parameters needs to be tuned based on the analysis of the load testing reports. The tuning process could be iterative until the issues are closed. Multiple load runs needs to be executed for users to simulate different scenarios, such as peak load (year end, quarter end, etc.), load generation within the LAN, Load generation across WAN or mobile network simulator while introducing configurable latency/jitter/packet loss etc.
- Should eliminate manual data manipulation and enable ease of creating data-driven tests.
- Should provide capability to emulate true concurrent transactions.
- Should identify root cause of performance issues at application or code level. Include code performance analysis to quickly pinpoint component-level bottlenecks: Slowest classes and methods, most frequently called methods, most costly (aggregate time spent for each method), response time variance etc.
- Should allow selection of different network bandwidth such as analog modems, ISDN, DSL, or custom bandwidth.
- Should be able to monitor various system components e.g. Server (OS, Web, Application & Database) Monitoring, Network (between Client & Server) Delay Monitoring, Network

Devices (Firewall, Switch & Router) Monitoring during the load test without having to install any data capturing agents on the monitored servers/components

- Should correlate response times and system performance metrics to provide quick insights in to root cause of performance issues.
- Reports on following parameters (but not limited to) such as transaction response time, transaction per second (Passed), user interface rendering time, transaction per second (Failed), web transaction breakdown graphs, hits per second, throughput, HTTP responses per Second, pages downloaded per second, system infrastructure performance metrics etc.
- Should provide End-to-End system performance analysis based on defined SLAs. Should monitor resource utilization including memory leakage, CPU overload and network overload. Should have the ability to split end-to-end response time for Network & Server(s) and provide drill-down capability to identify and isolate bottlenecks.

10.8.3 Audits & Inspections

MSI is expected to perform the following activities for overall ICCC Audits & Inspections organized by BSCDCL or its authorized agency:

- Should provide necessary information at the time of such activities
- Should provide necessary environment and access to the authorized personal for conducting such activities
- Should provide necessary evidences for Audits (if asked by the auditor / inspector) at the time of such activities.

END OF THE DOCUMENT