

# Request for Proposal for selection of System Integrator to "Design, Supply, Implement, Commission, Operate & Manage the Command & Control Centre" as a part of Smart City Solutions for Chennai City.

Volume 1: Instruction to Bidders  
RFP No. S.P.D.C.No.B1/100/2016



L I V A B I L I T Y I N D E X



## Important Dates

#	Particulars	Planned Date
1	Release of RfP	22-02-2018
2	Pre-bid Meeting date and time	07-03-2018 at 11:00 AM
3	Date and Time for submission of Bids	28-03-2018 at 3: 00 PM
4	Date and Time of opening of Technical bid	28-03-2018 at 3:30 PM
5	Date of opening of Commercial bids	To be notified later after technical Evaluation.

## Table of Contents

<b>1</b>	<b>Introduction.....</b>	<b>1</b>
1.1	About the Chennai Smart City Limited .....	1
1.2	Introduction to Greater Chennai Smart city Project .....	1
1.3	RfP Format.....	2
1.4	RfP Fact Sheet.....	3
1.5	Definitions/Acronyms.....	4
<b>2</b>	<b>Instruction to Bidders.....</b>	<b>5</b>
2.1	General .....	5
2.2	Bidders.....	7
2.3	Compliant Bids/Completeness of Response .....	8
2.4	Bidder to Inform.....	8
2.5	Bid Preparation costs .....	8
2.6	Pre-bid Meeting & Clarification .....	8
2.6.1	<i>Bidders Queries.....</i>	<i>8</i>
2.6.2	<i>Responses to Pre-Bid Queries and Issue of Corrigendum.....</i>	<i>9</i>
2.7	RfP Document Fee.....	9
2.8	Earnest Money Deposit (EMD) .....	9
2.9	Bid Validity Period.....	10
2.10	Contents of Bid.....	10
2.11	Bid Formats.....	12
2.11.1	<i>Pre-Qualification Bid Format.....</i>	<i>12</i>
2.11.2	<i>Technical Bid Format.....</i>	<i>13</i>
2.12	Commercial Bid Format.....	14
2.13	Language .....	15
2.14	Authentication of Bids.....	15
2.15	Amendment of Request for Proposal .....	15
2.16	Price .....	16
2.17	Deviations and Exclusions.....	16
2.18	Total Responsibility .....	16
2.19	Late Bids.....	16
2.20	Right to Terminate the Process .....	16
2.21	Non-Conforming bids .....	17
2.22	Acceptance/Rejection of Bids .....	17
2.23	Confidentiality .....	18
2.24	Disqualification.....	18
2.25	Key Personnel.....	18
2.25.1	<i>Initial Composition; Full Time Obligation; Continuity of Personnel.....</i>	<i>19</i>

2.25.2	<i>Evaluations</i> .....	19
2.25.3	<i>Replacement</i> .....	19
2.25.4	<i>High Attrition</i> .....	20
2.26	Fraud and Corrupt Practices.....	20
2.27	Conflict of Interest.....	22
2.28	Sub-Contracting.....	22
2.29	Inclusion of MSMEs in Project Delivery.....	22
2.30	Choice of Original Equipment Manufacturer (OEM):.....	23
2.31	Right to vary quantity.....	23
2.32	Withdrawal, Substitution, and Modification of Bids.....	23
2.33	Site Visit.....	23
<b>3</b>	<b>Selection Process for Bidder</b> .....	<b>24</b>
3.1	Opening of Bids.....	24
3.2	Preliminary Examination of Bids.....	24
3.3	Clarification on Bids.....	25
3.4	Evaluation Process.....	25
3.4.1	<i>Stage 1: Pre-Qualification</i> .....	25
3.4.2	<i>Stage 2: Technical Evaluation</i> .....	26
3.4.3	<i>Stage 3: Commercial Evaluation</i> .....	26
3.4.4	<i>Stage 4: Total Bid Evaluation</i> .....	27
3.5	Evaluation Process.....	28
3.5.1	<i>Stage 1: Pre-Qualification</i> .....	28
3.5.2	<i>Stage 2: Technical Evaluation</i> .....	28
3.5.3	<i>Stage 3: Commercial Evaluation</i> .....	29
3.5.4	<i>Stage 4: Total Bid Evaluation</i> .....	30
3.6	Pre-Qualification Criteria.....	31
3.7	Technical Evaluation Criteria.....	34
3.7.1	<i>Key Personnel Criteria</i> .....	41
<b>4</b>	<b>Award of Contract</b> .....	<b>42</b>
4.1	Notification of Award.....	42
4.2	Signing of Contract.....	42
4.3	Performance Bank Guarantee (PBG).....	42
4.4	Warranty & Maintenance.....	43
4.5	Failure to agree with the Terms & Conditions of the RFP.....	44
<b>5</b>	<b>Annexure 1 – Template for Pre-Bid Queries</b> .....	<b>45</b>
<b>6</b>	<b>Annexure 2 – Formats for Submission of the Pre-Qualification Bid</b> .....	<b>46</b>
6.1	Pre-qualification bid checklist.....	46
6.2	Pre-Qualification Bid Covering Letter.....	49
6.3	Company profile.....	51



6.4	Declaration of Non-Blacklisting .....	52
6.5	No Deviation Certificate .....	54
6.6	Total Responsibility Certificate.....	55
6.7	Self-certificate for Project execution experience (In Bidding Entity’s Letter Head).....	56
<b>7</b>	<b>Annexure 3 – Formats for Submission of the Technical Bid .....</b>	<b>57</b>
7.1	Technical Bid Check-List .....	57
7.2	Technical Bid Covering Letter.....	58
7.3	Credential Summary.....	60
7.4	Bidder’s Experience - Client Citations.....	61
7.5	Overview of Proposed Solution.....	62
7.5.1	<i>Structure of Proposed Solution .....</i>	<i>62</i>
7.5.2	<i>Project Plan.....</i>	<i>63</i>
7.5.3	<i>Manpower Plan.....</i>	<i>65</i>
7.6	Details of Resources proposed.....	67
7.6.1	<i>Summary of Resources proposed.....</i>	<i>67</i>
7.7	Curriculum Vitae (CV) of Team Members .....	68
7.8	Compliance to Requirement (Technical / Functional Specifications).....	70
7.9	Proposed Bill of Material (Technical Bid).....	71
7.10	Manufacturers'/Producers’ Authorization Form.....	77
7.11	Anti-Collusion Certificate .....	78
<b>8</b>	<b>Annexure 4 – Formats for Submission of the Commercial Bid (will be given in online portal)79</b>	
8.1	Section 1: CAPITAL EXPENDITURE (CAPEX).....	80
8.2	Section 1: OPERATIONAL EXPENDITURE (OPEX).....	86
8.3	Section 1: Sub-Total.....	87
8.4	Section 2: Unit Price for Upgradation – CAPEX .....	88
8.5	Section 2: Unit Price for Upgradation – OPEX .....	92
8.6	Section 2: Sub-Total.....	94
8.7	Section 3: Value of Price Bid .....	95
<b>9</b>	<b>Annexure 5 (a) – Performance Bank Guarantee .....</b>	<b>96</b>
<b>10</b>	<b>Annexure 5 (b) – Bank Guarantee for Earnest Money Deposit .....</b>	<b>98</b>
<b>11</b>	<b>Annexure 6 – Non-Disclosure Agreement .....</b>	<b>100</b>
<b>12</b>	<b>Annexure 7 - Consortium Agreement .....</b>	<b>103</b>
<b>13</b>	<b>Annexure 8 - Format for Power of Attorney to Authorize Signatory .....</b>	<b>105</b>
<b>14</b>	<b>Annexure 9 - Format for Power of Attorney for Lead bidder of Consortium.....</b>	<b>107</b>

# **1 Introduction**

## **1.1 About the Chennai Smart City Limited**

Chennai is the state capital of Tamil Nadu, and India's fourth largest city, by economy and population. The city has a diverse array of economic sectors and is known for its automobile industry historically and rich IT sector.

The municipal affairs of the city are managed by the Greater Chennai Corporation, which deals exclusively with the city jurisdiction and the Chennai Metropolitan Development GCC / CSCL (CMDA), which also deals with the wider Chennai Metropolitan Area (CMA).

The city of Chennai participated in the Smart City Challenge (Phase 1) and is one among the 20 shortlisted cities by MoUD for implementing Smart City projects in round 1.

Special Purpose Vehicle (SPV) was incorporated in the name "*Chennai Smart City Limited*" (CSCL) on 15<sup>th</sup> July 2016.

## **1.2 Introduction to Greater Chennai Smart city Project**

The Government of India launched the Smart Cities Mission on 25 June 2015. The objective is to promote sustainable and inclusive cities that provide core infrastructure and give a decent quality of life to its citizens, a clean and sustainable environment and application of 'Smart' Solutions. The focus is on sustainable and inclusive development and the idea is to look at compact areas, create a replicable model which will act like a lighthouse to other aspiring cities. The Smart Cities Mission is meant to set examples that can be replicated both within and outside the Smart City, catalyzing the creation of similar Smart Cities in various regions and parts of the country.

Some of the core infrastructure elements in Chennai Smart City would include adequate water supply, assured electricity supply, sanitation, including solid waste management, efficient urban mobility and public transport, affordable housing, especially for the poor, robust IT connectivity and digitalization, good governance, especially e-Governance and citizen participation, sustainable environment, safety and security of citizens, particularly women, children and the elderly.

The strategic components of the Chennai smart city are city improvement, city renewal and city extension plus a Pan-city initiative in which Smart Solutions are applied covering larger parts of the city.

Area-based development will transform existing infrastructure thereby improving livability of the whole city. Application of Smart Solutions will enable the city to use technology to improve infrastructure and services.

Comprehensive development in this way will improve quality of life, create employment and enhance incomes for all, especially the poor and the disadvantaged, leading to inclusive cities.

### **1.3 RfP Format**

The intent of this RfP is to invite bids from the Bidders for implementation of an integrated solution for the GCC / CSCL.

The Request for Proposal (RfP) consists of three volumes viz.

#### **1. RfP Volume 1: Instruction to Bidders**

Volume 1 details the instructions with respect to the bid process management, technical evaluation framework, and the technical & financial forms.

#### **2. RfP Volume 2: Scope of work including Functional & Technical Specifications**

Volume 2 of the RfP provides information regarding the Project Implementation Plan, business requirements/applications to be covered and corresponding process related documentation, scope of work for the selected bidder and functional requirements.

#### **3. RfP Volume 3: Master Service Agreement**

Volume 3 contains the contractual, legal terms & conditions applicable for the proposed engagement.

#### 1.4 RfPFactSheet

#	Item	Description
1.	Method of Selection	The method of selection is QCBS – Quality cum Cost based Selection. The Contract will be awarded to the bidder with highest Total Score.
2.	Availability of RfP Documents	Download from <a href="http://www.tntenders.gov.in">www.tntenders.gov.in</a>
3.	Date of RfP Issuance	22-Feb-2018 Notice Inviting Tender
4.	Tender document fee	To be downloaded from online Procurement website at free of cost.
5.	Earnest Money Deposit (EMD)	INR 1.5 Crore only by Bank Guarantee (as per format attached in Annexure 5(b))
6.	Pre-bid Meeting date and time, Venue	07-03-2018 at 11:00AM, at O/O Superintending Engineer, Special Projects Department, 5th Floor, Amma Malligai, Ripon Building Complex, Chennai -600003.
7.	Date and Time for submission of Bids	28-03-2018 at 3:00 PM, at O/O Superintending Engineer, Special Projects Department, 5th Floor, Amma Malligai, Ripon Building Complex, Chennai -600003.
8.	Bid Validity	Bid must remain valid up to 180 (One Hundred & Eighty) days from the date of submission of the Bid.
9.	Name and Address of the Tender Inviting GCC / CSCL for correspondence	Superintending Engineer, Special Projects Department, 5th Floor, Amma Malligai, Ripon Building Complex, Chennai -600003.

-

## 1.5 Definitions/Acronyms

Terms	Meaning
BOM	Bill of Material
BEC	Bidders Evaluation Committee
CC	Capital Cost
CCTV	Closed Circuit Television
CEO	Chief Executive Officer
DD	Demand Draft
EMD	Earnest Money Deposit
GIS	Geographical Information Systems
GPS	Global Positioning System
HOD	Head of Department
ICT	Information and Communication Technology
INR	Indian National Rupee
LoA	Letter of Acceptance
NPV	Net Present Value
OEM	Original Equipment Manufacture
PBG	Performance Bank Guarantee
PDD	Proposal Due Date
PoC	Proof of Concept
PQC	Pre-Qualification Criteria
RfP	Request for Proposal
PV	Present Value
SI	System Integrator
SLA	Service Level Agreement
SOP	Standard Operating Procedures
TQ	Technical Qualification
UAT	User Acceptance Testing
VM	Virtual Machine
WSP	Wi-Fi Service Provider
TRV	Total Revenue
GCC	Greater Chennai Corporation
CCTNS	Crime & Criminal Tracking Network & Systems
CSCCL	Chennai Smart City Limited
O&M	Operations & Maintenance

## 2 Instruction to Bidders

### 2.1 General

- a. While every effort has been made to provide comprehensive and accurate background information, requirements and envisaged solution(s) specifications, Bidders must form their own conclusions about the solution(s) needed to meet the GCC / CSCL's requirements. Bidders and recipients of this RfP may wish to consult their own legal advisers in relation to this RfP.
- b. All information supplied by Bidders as part of their bids in response to this RfP, may be treated as contractually binding on the Bidders, on successful award of the assignment by the GCC / CSCL on the basis of this RfP.
- c. No commitment of any kind, contractual or otherwise shall exist unless and until a formal written contract has been executed by or on behalf of GCC / CSCL. Any notification of preferred bidder status by GCC / CSCL shall not give rise to any enforceable rights by the Bidder. GCC / CSCL may cancel this public procurement at any time prior to a formal written contract being executed by or on behalf of GCC / CSCL.
- d. Sealed bids shall be received by the GCC / CSCL on the e-Procurement portal [www.tntenders.gov.in](http://www.tntenders.gov.in) before the time and date specified in the schedule of the tender notice. In the event of the specified date for the submission of tender offers being declared a public holiday by the Government of Tamil Nadu, the offers will be received up to the appointed time on the next working day. The GCC / CSCL may, at its discretion, extend this deadline for submission of offers by issuing corrigendum and uploading the same on e-Procurement portal.
- e. In addition to the online submission mentioned above, the bidder shall submit one hard copy of the complete proposal (excluding Commercial bid) in the hard copy format duly signed **ON ALL PAGES** by the authorized signatory of bidding organization (lead bidder in case of consortium). **The commercial bid shall uploaded Online Portal& also in HARDCOPY SUBMISSION OF COMMERCIAL BID separately sealed cover as per section 2.10.1 of this RFP.** The bidder shall ensure that content uploaded in the soft copy in the online portal shall be same as the content in the hardcopy bid proposal being submitted by the bidder. The bidder shall ensure hard copy of bid / proposal shall be neatly bound, covered in sealed envelope any loose sheets in the hard copy document submission should be avoided.

- f. Any other form of bid submission through email, FAX, Telephone etc. offers shall not be accepted.



## 2.2 Bidders

Bidder	<ul style="list-style-type: none"> <li>• Bidders can submit as a sole Bidder or as consortium</li> <li>• Both Sole Bidder / Consortium shall would be scrutinized through the prescribed Pre-Qualifications, Technical Evaluation &amp; final techno-commercial Stage. Only upon successfully complying with all the stages the bids would scrutinized for next stage of evaluation.</li> </ul>
	<p>Incase of Consortium Bids</p> <ul style="list-style-type: none"> <li>• Maximum of 3 entities are allowed for form a consortium bid. Out the 3 entities one of them would act as Lead Bidder and remaining entities would act as consortium members.</li> <li>• Consortium bid needs to submit Consortium agreement which shall articulate the terms of agreement laid among the entities of the consortium.</li> <li>• the list of entities in the consortium need to be declared, Consortium members cannot be changed during the project period.</li> <li>• Any bidder (Sole/Prime/Consortium member) shall be allowed to be part of only one bid (either as Prime / consortium partner). If any bidder / Prime bidder / consortium partner is found to be part of another bid, then both such bids would be summarily rejected.</li> <li>• The Lead bidder shall be responsible and jointly &amp; severally liable under this RfP for             <ul style="list-style-type: none"> <li>○ The delivery of products &amp; services</li> <li>○ Meeting the SLAs</li> <li>○ Successful completion of this entire Project</li> </ul> </li> <li>• The Consortium members are responsible for scope agreed as per the roles and responsibilities defined as consortium Agreement.s</li> <li>• The Lead Bidder shall be authorized by the consortium members for             <ul style="list-style-type: none"> <li>○ <i>The management of all consortium members</i></li> <li>○ <i>To incur liabilities and receive instructions for and on behalf of any and all consortium members.</i></li> <li>○ <i>Entire execution of the Contract, receipt of payments etc. on behalf of consortium</i></li> </ul> </li> </ul> <p><i>Ensuring that all the bid compliance are met by the consortium members (mentioned in the bid, failing which bid can be disqualified).</i></p>

## **2.3 Compliant Bids/Completeness of Response**

- a. Bidders are advised to study all instructions, forms, terms, requirements and other information in the RfP documents carefully. Submission of the bid shall be deemed to have been done after careful study and examination of the RfP document with full understanding of its implications.
- b. Failure to comply with the requirements of this paragraph may render the bid non-compliant and the Bid may be rejected. Bidders must:
  - i. Include all documentation specified in this RfP, in the bid.
  - ii. Follow the format of this RfP while preparing the bid and respond to each element in the order as set out in this RfP.
  - iii. Comply with all requirements as set out within this RfP.

## **2.4 Bidder to Inform**

The Bidder shall be deemed to have carefully examined the Terms & Conditions, Scope, Service Levels, Specifications, and Schedules of this RfP. If bidder has any doubts/clarifications as to the meaning of any portion of the Conditions or the specifications they shall, before the last date for Submission of Pre-Bid Queries, set forth the particulars thereof and submit them to GCC / CSCL in writing in order that such doubt may be removed or clarifications are provided.

## **2.5 Bid Preparation costs**

The Bidder shall bear all costs associated with the preparation and submission of its bid, for the purposes of clarification of the bid, if so desired by the GCC / CSCL.

## **2.6 Pre-bid Meeting & Clarification**

### **2.6.1 Bidders Queries**

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

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

Bidders must submit their queries as per the format mentioned in Section5Annexure 1 – Template for Pre-Bid Queries

## **2.6.2 Responses to Pre-Bid Queries and Issue of Corrigendum**

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

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

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

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

## **2.7 RfP Document Fee**

RfP can be downloaded free from the website URL mentioned in the fact sheet.

## **2.8 Earnest Money Deposit (EMD)**

EMD of **INR 1,50,00,000/-** (Indian Rupees one Crore & fifty lakhs only) shall be through a Bank Guarantee from a scheduled bank in India. No exemption for submitting the EMD will be given to any agency. Bid security in any other form will not be entertained.

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

*For Successful bidders:* The bid security, for the amount mentioned above, of successful bidder would be returned without interest upon submission of Performance Bank Guarantee by the successful bidder.

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

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

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

## **2.9 Bid Validity Period**

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

On completion of the validity period, unless the Bidder withdraws his bid in writing, it will be deemed to be valid until such time that the Bidder formally (in writing) withdraws his bid.

## **2.10 Contents of Bid**

The two bids system shall be followed. Technical and Commercial Offers shall be uploaded separately through the online portal.

- a. Please note that Prices should NOT be indicated in the Technical Bid but should only be indicated in the Commercial Bid in the online portal. In case of any commercial figures are mentioned in other than commercial bid document then such bid is subject to rejection.
- b. All the pages of the bid must be sequentially numbered. The bid documents must contain in the beginning of the document, a list of contents with page numbers. Any deficiency in the documentation may result in the rejection of the Bid.
- c. The original bid shall be prepared in indelible ink. It shall contain no interlineations or overwriting, except as necessary to correct errors made by the Bidder itself. Any such corrections must be initialed by the person (or persons) who sign(s) the bids.
- d. All pages of the bid shall be initialed and stamped by the person (or persons) who sign the bid.
- e. Failure to submit the bid before the submission deadline specified in the Fact Sheet would cause a bid to be rejected.
- f. GCC / CSCL will not accept delivery of bid by fax, e-mail or in person.

### **2.10.1 Bid Submission Details**

#### *2.10.1.1 Two Cover Bid System*

Bidders should examine all Instructions, Scope of Work and Terms and Conditions as given in the Tender document. The tender should be submitted in two parts viz Technical Bid and Price Bid.

**2.10.1.2 Technical Proposal (Cover A)**

- a) Technical Proposal shall include both Prequalification & Technical Qualifications
- b) The Technical proposal as per the format given in the Tender document shall be typed, signed and stamped in all pages by the bidder or Authorised Signatory of the bidder. Any alterations, deletions or overwriting shall be attested with full signature of the bidder or Authorised Signatory of the bidder.
- c) The supporting documents and other documents as given in the Pre-Qualification & Technical Evaluation Criteria should be submitted in the Technical Proposal.
- d) The Technical Proposal shall not contain any indications of the Price whether directly or indirectly otherwise the Bid will be summarily rejected.
- e) Scanned copies of the same shall be uploaded in the tender portal – Bid Schedule
- f) Scanned copy of EMD should be submitted in the Online Portal and original shall be submitted in the Cover A

**2.10.1.3 Price Bid (Cover -B)**

- a) All the Price items as per the format given in this Rfp document shall be neatly typed, signed and stamped in all the pages by the bidder or Authorised Signatory of the bidder. Any alterations, deletions or overwriting shall be attested with full signature of the bidder or Authorised Signatory. Only a single price should be quoted for each Price Bid item. The Bid is liable for rejection if Price Bid contains variation clause or conditional offers or partial offers.
- b) The Price Bid shall be placed in a separate cover and sealed appropriately. The Price Bid cover (Envelope-B) shall be superscribed as “*name of RFP*”. The “FROM” address and “TO” address shall be written legibly.
- c) Summary of Cost shall be entered template given in Price Bid of the online portal

**2.10.1.4 Outer Cover (Cover C)**

Both the Technical Bid cover (Cover -A) and Price Bid cover (Cover -B) shall then be put in a single outer cover and sealed appropriately. The outer cover shall be superscribed as “<name of RFP>The “FROM” address and “TO” address shall be written legibly.

## 2.11 Bid Formats

### 2.11.1 Pre-Qualification Bid Format

#	Section Heading	Details
1.	Pre-qualification checklist	As per format provided in section 6.1
2.	Pre-Qualification Bid Covering Letter	As per format provided in section 6.2
3.	Company Profile	Details as per Section 66.36.3.3
4.	No Deviation Certificate	As per format provided in section 6.5
5.	Total responsibility certificate	As per format in 6.6
6.	Non-Disclosure Agreement	NDA as per Annexure Annexure 6 – Non-Disclosure Agreement
7.	Consortium Agreement (if applicable)	As per format provided in Annexure 7 - Consortium Agreement
8.	About Bidder (Company Profile)	As per format provided in section 6.3 Company profile of this Volume of the RfP
9.	Bidder/Consortium Registration	<ul style="list-style-type: none"> <li>• Certificate of Incorporation / Registration under companies Act, 1956/2013 or any suitable Act abroad</li> <li>• Consortium agreement clearly stating the roles and responsibilities of each member</li> </ul> <i>As per Pre-qualification criteria – SI # 3 in section 6.1</i>
10.	Annual Turnover	<p>Certificate from the Statutory auditor / CA clearly specifying the annual turnover for the specified years</p> <i>As per Pre-qualification criteria – SI # 4 in section 6.1</i>
11.	Positive Net worth	<p>Certificate from the Statutory auditor/ CA clearly specifying the net worth of the firm</p> <i>As per Pre-qualification criteria – SI # 5 in section 6.1</i>
12.	Prior Project Experience Bidder/Consortium from relevant scope of the RfP	<p>Work Order / Copy of Contract &amp; Client Certificate as Proof of the projects undertaken</p> <i>As per Pre-qualification criteria – SI # 6 in section 6.1</i>
13.	Undertaking for non-blacklisting clause	<p>Undertaking by the authorized signatory as per format</p> <i>As per Pre-qualification criteria – SI # 5 in section 6.1 &amp; Sec 6.4</i>

#	Section Heading	Details
14.	Bidder Certifications	Copies of valid certificates in the name of the sole bidder or the Lead bidder in case of a Consortium <i>As per Pre-qualification criteria – SI # 8 in section 6.1</i>
15.	EMD	Bank Guarantee as per Annexure 5 (b) – Bank Guarantee for Earnest Money Deposit
16.	Power of Attorney	Documentary evidence as per format provided in Annexure 8 - Format for Power of Attorney to Authorize Signatory and Annexure 9 - Format for Power of Attorney for Lead bidder of Consortium
17.	Project Experience	Citation details of projects as per format in Section Bidder's Experience - Client Citations 7.4 and Self-certificate for Project execution experience (In Bidding Entity's Letter Head) 6.7 as applicable.
18.	Online Submission Technical Bid	Yes
19.	Hard Submission	Yes

### 2.11.2 Technical Bid Format

#	Section Heading	Details
1.	Technical Bid Checklist	As per format provided in section 7.1 Technical Bid Check-List
2.	Technical Bid Covering Letter	As per format provided in Section 7.2 Technical Bid Covering Letter
3.	About Bidder	<ul style="list-style-type: none"> <li>• Details about bidder (whether sole bidder or Consortium)</li> <li>• Bidder's General Information as required in Technical Evaluation Criteria 3.7 &amp; 3.7.1</li> </ul>
4.	Approach & Methodology	Details as required in Technical Evaluation Criteria 3.7 & 3.7.1
5.	Solution Proposal	Details as required in Technical Evaluation Criteria 3.7 & 3.7.1 Please refer to Structure of Proposed Solution 7.5.1
6.	Project/credential summary	As per format provided in Credential Summary in Section 7.3
7.	Bidder's Experience	Project citation as per format provided in Bidder's Experience - Client Citations in section 7.4 and supporting documentary evidences and Self-



		certifications as per format in section 6.7as Applicable.
8.	Project Plan and Resources	<ul style="list-style-type: none"> <li>• Project plan as per format provided in Project Plan in Section 7.5.2</li> <li>• Manpower Plan as per format provided in Manpower Plan in Section 7.5.3 I &amp; II</li> <li>• Summary of resources as per format provided in Summary of Resources proposed in Section 7.6.1</li> <li>• CV of resources as per format provided in Curriculum Vitae (CV) of Team Members in Section 7.7</li> </ul>
9.	Manufacturers'/Producers' Authorization Form	As per format provided in section 7.10
10.	Anti-Collusion Certificate	As per format provided in section 7.11
11.	Non-disclosure agreement	As per format provided in section 11 (Annexure 6 – Non-Disclosure Agreement)
12.	Online Submission Technical Bid along with copy of EMD	Yes
13.	Hardcopy Submission Technical Bid along with Original EMD	Yes
14.	Annual Turnover from e-governance /ERP Solution to State /Central/ Quasi Government/ULB	Certificate from the Statutory auditor / CA clearly specifying the annual turnover for the specified years

## 2.12 Commercial Bid Format

The Bidder must submit the Commercial Bid in the formats specified in Online Portal. The Price Bid has three sections, the first section captures the commercials for the envisaged CCC in the form of CAPEX and OPEX heads. This summation of these two heads shall constitute to the actual expenditure to the CCC Project. **In order to have control on reasonability of the CAPEX and OPEX costing, it has been envisaged to have CAPEX:OPEX ratio i.e. the total cost of CAPEX in section I of the Price BID shall not exceed 50% of the total of CAPEX & OPEX cost in Section I. BIDDERS SHALL ENSURE THE QUOTED PRICE BID IN SECTION 1 ABIDES BY THIS RATIO. Only commercial bids which comply to this ratio would be considered for further course of evaluation.**

The envisaged CCC is growing solution therefore it is anticipated for vertical and horizontal growth of CCC solution in the future. Therefore in order to facilitate the procurement of this upgradation the likely upgraded line items in the CCC have been identified and their prices are being discovered in the Section 2 of the Price Bid. The prices discovered in this section shall be valid till the end of contract period of System Integrator so that authority may use it as rate card for procurement as per the actual demands in future. The line items envisaged for upgradation The cost of such upgradation items are sought against arbitrary quantities which is used only for evaluation purposes. The GCC / CSCL shall evaluate and may place an order to actual demanded quantity based on unit rates discovered in this section.

**For the purpose of bid evaluation for the selection of the successful bidder, the figures under Grand Total i.e. “Value of Price Bid” shall be used for ascertaining commercial score & there hence the successful bidder.**

### **2.13 Language**

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

### **2.14 Authentication of Bids**

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

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

### **2.15 Amendment of Request for Proposal**

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

It shall be the responsibility of the prospective bidder(s) to check the GCC / CSCL's website from time to time for any amendment in the RfP document. In case of failure to get the amendments, if any, GCC / CSCL shall not be responsible.

In order to allow prospective bidders a reasonable time to take the amendment into account in preparing their bids, GCC / CSCL, at its discretion, may extend the deadline for submission of bids. Such extensions shall be uploaded on website of the GCC / CSCL.

## **2.16 Price**

Bidders shall give the required details of all applicable GST, duties, other levies and charges etc. in respect of direct transaction between GCC / CSCL and the Bidder.

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

Prices quoted by the Bidder shall remain firm during the entire contract period and not subject to variation on any account. A bid submitted with an adjustable price quotation shall be treated as non-responsive and rejected. **Commercial Prices should NOT be part of Pre-qualification or Technical Bid, if any commercial details are found other than the Commercial Bid then the such bids are treated as Non-responsive & rejected.**

## **2.17 Deviations and Exclusions**

Bids shall be submitted strictly in accordance with the requirements and terms & conditions of the RfP. The Bidder shall submit a No Deviation Certificate as per the format mentioned in Section 6.5. The bids with deviation(s) are liable for rejection.

## **2.18 Total Responsibility**

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

## **2.19 Late Bids**

Late submission will not be entertained and will not be permitted by the Online Portal. Authorities shall does not be responsible for delay in submission of any online submission related or website related issues and date of submission cannot be extended for such reasons GCC / CSCL reserves the right to modify and amend any of the above-stipulated condition/criterion.

## **2.20 Right to Terminate the Process**

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

### **2.21 Non-Conforming bids**

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

- a. If it does not comply with the requirements of this RfP.
- b. If a bid does not follow the format requested in this RfP or does not appear to address the particular requirements of the solution.

### **2.22 Acceptance/Rejection of Bids**

- a. GCC / CSCL reserves the right to reject in full or part, any or all bids without assigning any reason thereof. GCC / CSCL reserves the right to assess the Bidder's capabilities and capacity. The decision of GCC / CSCL shall be final and binding.
- b. Bid should be free of over writing. All erasures, correction or addition must be clearly written both in words and figures and attested.

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

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

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

## **2.23 Confidentiality**

All the material/information shared with the Bidder during the course of this procurement process as well as the subsequent resulting engagement following this process with the successful bidder, shall be treated as confidential and should not be disclosed in any manner to any unauthorized person under any circumstances. The employees of the successful Lead bidder and Consortium members who are proposed to be deployed on the project need to comply to information security as per Master Service Agreement in RfP Volume III.

## **2.24 Disqualification**

The bid is liable to be disqualified in the following cases, but not limited to,

- a. In-case bidder fails to meet the bidding requirements / terms & conditions as prescribed in this RfP
- b. During validity of the bid, or its extended period, if any, the bidder changes its quoted prices.
- c. The bidder's bid is conditional and has deviations from the terms and conditions of RfP.
- d. Bid is received in incomplete form.
- e. Bid is not accompanied by all the requisite documents.
- f. Information submitted in technical bid is found to be misrepresented, incorrect or false, accidentally, unwittingly or otherwise, at any time during the processing of the contract (no matter at what stage) or during the tenure of the contract including the extension period if any.
- g. Financial bid is enclosed with the same document as technical bid.
- h. Bidder tries to influence the bid evaluation process by unlawful/corrupt/fraudulent means at any point of time during the bid process.
- i. In case any one party submits multiple bids or if common interests are found in two or more bidders, the bidders are likely to be disqualified, unless additional bids/bidders are withdrawn upon notice immediately
- i. If any of the Lead Bidderis also partner in any other bid, then all the affected bids shall be disqualified.
- j. Bids without EMD will be disqualified

## **2.25 Key Personnel**

GCC / CSCL has identified certain key positions and minimum qualifications for each of the positions that should be part of project team of the bidder (hereby referred to as "key

personnel"). Details of these key positions are provided in Section **Error! Reference source not found.**

### **2.25.1 Initial Composition; Full Time Obligation; Continuity of Personnel**

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

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

In any such case, the GCC / CSCL's prior written consent would be mandatory.

### **2.25.2 Evaluations**

Bidder shall carry out an evaluation of the performance of each member of the Key Personnel in connection with the Services at least once in each Contract Year. Bidder shall provide reasonable written notice to GCC / CSCL of the date of each evaluation of each member of the Key Personnel. GCC / CSCL shall be entitled to provide inputs to the bidder for each such evaluation. Bidder shall promptly provide the results of each evaluation to GCC / CSCL, subject to Applicable Law.

### **2.25.3 Replacement**

In case any proposed resource resigns, then the Bidder has to inform GCC / CSCL within one week of such resignation.

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

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

A resume, curriculum vitae and any other information about the candidate that is reasonably requested by GCC / CSCL; and

An opportunity to interview the candidate.

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

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

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

#### **2.25.4 High Attrition**

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

- a) provide GCC / CSCL with a reasonably detailed explanation as to the reasons for such change, including, where applicable and permitted, notes from any exit interviews conducted by Bidder with any departing member of the Key Personnel; and
- b) if such change to Key Personnel has or is likely to have any material adverse impact on the provision of the Services or any substantial part thereof, undertake, at its own costs, such remediation acts as are reasonably necessary in order to improve the retention of the Key Personnel including making reasonable changes to the human resources policies and procedures applicable to the Key Personnel (including those related to compensation, benefits and other conditions so that they are competitive with the market) as may be necessary to ensure that such policies and procedures comply with Good Industry Practice.

#### **2.26 Fraud and Corrupt Practices**

- a. The Bidders and their respective officers, employees, agents and advisers shall observe the highest standard of ethics during the Selection Process. Notwithstanding anything to the contrary contained in this RfP, GCC / CSCL shall reject a Bid without being liable in any manner whatsoever to the Bidder, if it determines that the Bidder has, directly or indirectly or through an agent, engaged in corrupt practice, fraudulent practice, coercive practice, undesirable practice or restrictive practice (collectively the "Prohibited



Practices”) in the Selection Process. In such an event, GCC / CSCL shall, without prejudice to its any other rights or remedies, forfeit and appropriate the EMD or PBG, as the case may be, as mutually agreed genuine pre-estimated compensation and damages payable to GCC / CSCL for, inter alia, time, cost and effort of GCC / CSCL, in regard to the RfP, including consideration and evaluation of such Bidder’s Bid.

- b. Without prejudice to the rights of GCC / CSCL under Clause above and the rights and remedies which GCC / CSCL may have under the LOA or the Agreement, if a Bidder is found by GCC / CSCL to have directly or indirectly or through an agent, engaged or indulged in any corrupt practice, fraudulent practice, coercive practice, undesirable practice or restrictive practice during the Selection Process, or after the issue of the LOA or the execution of the Agreement, such Bidder shall not be eligible to participate in any tender or RfP issued by GCC / CSCL during a period of 3 years from the date such Bidder is found by GCC / CSCL to have directly or through an agent, engaged or indulged in any Prohibited Practices.
- c. For the purposes of this Section, the following terms shall have the meaning hereinafter respectively assigned to them:
- d. “corrupt practice” means (i) the offering, giving, receiving, or soliciting, directly or indirectly, of anything of value to influence the action of any person connected with the Selection Process (for avoidance of doubt, offering of employment to or employing or engaging in any manner whatsoever, directly or indirectly, any official of GCC / CSCL who is or has been associated in any manner, directly or indirectly with the Selection Process or the LOA or has dealt with matters concerning the Agreement or arising there from, before or after the execution thereof, at any time prior to the expiry of one year from the date such official resigns or retires from or otherwise ceases to be in the service of GCC / CSCL, shall be deemed to constitute influencing the actions of a person connected with the Selection Process); or (ii) save as provided herein, engaging in any manner whatsoever, whether during the Selection Process or after the issue of the LOA or after the execution of the Agreement, as the case may be, any person in respect of any matter relating to the Project or the Award or the Agreement, who at any time has been or is a legal, financial or technical consultant/adviser of GCC / CSCL in relation to any matter concerning the Project;
- e. “fraudulent practice” means a misrepresentation or omission of facts or disclosure of incomplete facts, in order to influence the Selection Process;
- f. “coercive practice” means impairing or harming or threatening to impair or harm, directly or indirectly, any persons or property to influence any person’s participation or action in the Selection Process;
- g. “undesirable practice” means (i) establishing contact with any person connected with or employed or engaged by GCC / CSCL with the objective of canvassing, lobbying or in

any manner influencing or attempting to influence the Selection Process; or (ii) having a Conflict of Interest; and

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

## **2.27 Conflict of Interest**

- a. A bidder shall not have a conflict of interest that may affect the Selection Process or the Solution delivery (the “Conflict of Interest”). Any Bidder found to have a Conflict of Interest shall be disqualified. In the event of disqualification, GCC / CSCL shall forfeit and appropriate the EMD, if available, as mutually agreed genuine pre-estimated compensation and damages payable to GCC / CSCL for, inter alia, the time, cost and effort of GCC / CSCL including consideration of such Bidder’s Bid, without prejudice to any other right or remedy that may be available to GCC / CSCL hereunder or otherwise.
- b. GCC / CSCL requires that the bidder provides solutions which at all times hold GCC / CSCL’s interest’s paramount, avoid conflicts with other assignments or its own interests, and act without any consideration for future work. The bidder shall not accept or engage in any assignment that would be in conflict with its prior or current obligations to other clients, or that may place it in a position of not being able to carry out the assignment in the best interests of GCC / CSCL.

## **2.28 Sub-Contracting**

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

- Cabling and fixtures work, and all civil work during implementation.
- Facility Management Staff at Command & Communications Center.

Sub-contracting shall be allowed only with prior written approval of GCC / CSCL. However, even if the work is sub-contracted, the sole responsibility of the work shall lie with the lead bidder. The lead bidder shall be held responsible for any delay/error/non-compliance etc. of its sub-contracted vendor. The details of the sub-contracting agreements (if any) between both the parties would be required to be submitted to GCC / CSCL.

## **2.29 Inclusion of MSMEs in Project Delivery**

Bidders are encouraged to include Micro, Small and Medium Enterprises (MSMEs) in the delivery of the project. Bidders may earmark some proportion of the total contract for procuring goods and services from MSEs. Activities that can be sub-contracted to

MSME/MSE partners are restricted to those defined under Sub-Contracting Clause 2.28 above.

### **2.30 Choice of Original Equipment Manufacturer (OEM):**

The bidder shall apply high standards of diligence in choosing an optimal OEM who complies with the tender conditions, specifications & SLAs. The bidder may evaluate products being proposed are not end of life and also there is guarantee of OEM support for minimum period of 6 years. The same may be formally secured through the Manufacturer's Authorizing form Prescribed in Section 7.10

### **2.31 Right to vary quantity**

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

### **2.32 Withdrawal, Substitution, and Modification of Bids**

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

### **2.33 Site Visit**

- a. The Bidder may wish to visit and examine the site or sites and obtain for itself, at its own responsibility and risk, all information that may be necessary for preparing the bid and entering into the Contract. The costs of visiting the site or sites shall be at the Bidder's own expense.
- b. The GCC / CSCL upon request from any bidder will arrange for site visit of its personnel or agents to gain access to the relevant site or sites, provided that the Bidder gives the GCC / CSCL adequate notice of a proposed visit of at least 7 (seven) days. Failure of a Bidder to make a site visit will not be a cause for its disqualification.

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

### **3 Selection Process for Bidder**

#### **3.1 Opening of Bids**

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

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

There will be bid-opening for the following

- a. EMD with Pre-Qualification bid**
- b. Technical bid**
- c. Commercial bid**

The venue, date and time for opening the Pre-qualification bid are mentioned in the Fact sheet. The date and time for remaining bid process would be communicated to the respective bidders who qualify the respective stage of evaluation.

#### **3.2 Preliminary Examination of Bids**

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

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

- a. Not submitted in format as specified in the RfP document
- b. Received without the Letter of Authorization (Power of Attorney)
- c. Found with suppression of details
- d. With incomplete information, subjective, conditional offers and partial offers submitted
- e. Submitted without the documents requested

- f. Non-compliant to any of the clauses mentioned in the RfP
- g. With lesser validity period
- h. Signature of Authorized personnel on all pages both on Hard & Copy of the bid.

### **3.3 Clarification on Bids**

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

### **3.4 Evaluation Process**

GCC / CSCL shall constitute a Tender Evaluation Committee to evaluate the responses of the bidders. The Tender Evaluation Committee shall evaluate the responses to the RfP and all supporting documents/documentary evidence. Inability to submit requisite supporting documents/documentary evidence by bidders may lead to rejection of their bids.

The decision of the Tender Evaluation Committee in the evaluation of bids shall be final. No correspondence will be entertained outside the process of evaluation with the Committee. The Tender Evaluation Committee may ask for meetings or presentation with the Bidders to seek clarifications or conformations on their bids. GCC / CSCL reserves the right to validate the authenticity of the information provided in the Pre-qualification and Technical Evaluation criteria and the requisite support must be provided by the respective bidder.

The Tender Evaluation Committee reserves the right to reject any or all bids. Each of the responses shall be evaluated as per the criteria and requirements specified in this RfP.

The steps for evaluation are as follows:

#### **3.4.1 Stage 1: Pre-Qualification**

- a. GCC / CSCL shall validate the “Earnest Money Deposit (EMD)”.
- b. If the contents are as per requirements, GCC / CSCL shall open the “Pre-Qualification Bid”. **Each of the Pre-Qualification condition mentioned in Section 3.5 is MANDATORY.** In case, the Bidder does not meet any one of the conditions, the bidders shall be disqualified.

Bidders who comply to the pre-qualification criteria along with other RfP terms & conditions would be termed as “Qualified Bidders” and such bidders shall be informed

of their successfully meeting Pre-Qualifications Criteria & other associated RfP Terms & Conditions. Their Technical Bids alone would be opened for next stage of evaluation.

- c. Technical and Financial bids for those bidders who don't pre-qualify will not be opened.

### **3.4.2 Stage 2: Technical Evaluation**

- a. "Technical bid" will be evaluated only for the bidders who succeed in Stage 1.
- b. GCC / CSCL will review the technical bids of the short-listed bidders to determine whether the technical bids are substantially responsive. Bids that are not substantially responsive are liable to be disqualified at GCC / CSCL's discretion.
- c. The bidders' technical solutions proposed in the bid document shall be evaluated as per the requirements specified in the RfP and technical evaluation framework as mentioned in Technical Evaluation Criteria and details in Section 3.6 & 3.6.1
- d. Bidders shall be earmarked an exclusive open space where the bidder shall install smart envisaged components and demonstrate the "Proof-of-Concept" to the Technical Evaluation Committee appointed by the GCC / CSCL. The place for showing demonstration would be provided by GCC / CSCL and bidder may setup sample smart components and showcase live demonstrations to Technical Evaluation Committee
- e. Bidders should submit detailed – "**Approach & Methodology & Solutions proposed**"
- f. Each Technical Bid will be assigned a Technical Score out of a maximum of 100points. Only the bidders who get **Technical Score of more than or equal to 60%in Technical Evaluation** will qualify for Commercial Evaluation stage.

### **3.4.3 Stage 3: Commercial Evaluation**

- a. All the technically qualified bidders will be notified to participate in Commercial Bid opening process.
- b. The commercial bids for the technically qualified bidders shall then be opened on the notified date and time and reviewed to determine whether the commercial bids are substantially responsive. Bids that are not substantially responsive are liable to be disqualified at GCC / CSCL's discretion.
- c. The bid price shall include all GST and levies and shall be in Indian Rupees and mentioned separately.
- d. Each of the Commercial bids shall be evaluated on a score of 100 points. The Commercial Score of the bidder shall be calculated with respect the lowest Total Price by any bidder. The methodology of Commercial Score shall be as follows.
- e. Commercial Score of the bidder under consideration = (Lowest Total Price from all Commercial Bids / Total Price quoted in Commercial bid by the bidder under consideration) X 100

#### **3.4.4 Stage 4: Total Bid Evaluation**

- a. The Total Score shall be based on Quality and Cost based Evaluation (QCBS). Technical Score shall have 70 % weightage and Commercial Score shall have 30% weightage.
- b. The Total Score of the bidder =  $0.7 \times (\text{Technical Score}) + 0.3 \times (\text{Commercial Score})$
- c. *The bidder achieving the highest Total Score shall be invited for negotiations for awarding the contract. In case of a tie where two or more bidders achieve the same highest Total Score, the bidder with the higher Technical Score will be invited first for negotiations for awarding the contract.*



### **3.5 Evaluation Process**

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

The decision of the Tender Evaluation Committee in the evaluation of bids shall be final. No correspondence will be entertained outside the process of evaluation with the Committee. The Tender Evaluation Committee may ask for meetings or presentation with the Bidders to seek clarifications or conformation on their bids. Authority reserves the right to validate the authenticity of the information provided in the Pre-qualification and Technical Evaluation criteria and the requisite support must be provided by the respective bidder.

The Tender Evaluation Committee reserves the right to reject any or all bids. Each of the responses shall be evaluated as per the criteria and requirements specified in this RfP.

The steps for evaluation are as follows:

#### **3.5.1 Stage 1: Pre-Qualification**

- a. Authority shall validate the “Earnest Money Deposit (EMD)”.
- b. If the contents are as per requirements, Authority shall open the “Pre-Qualification Bid”. **Each of the Pre-Qualification condition mentioned in Section 3.5 is MANDATORY.** In case, the Bidder does not meet any one of the conditions, the bidder shall be disqualified.
- c. Bidders who comply to the pre-qualification criteria along with other RfP terms & conditions would be termed as “Qualified Bidders” and such bidders shall be informed of their successfully meeting Pre-Qualifications Criteria & other associated RfP Terms & Conditions. Their Technical Bids alone would be opened for next stage of evaluation.
- d. Technical and Financial bids for those bidders who don't pre-qualify will not be opened.

#### **3.5.2 Stage 2: Technical Evaluation**

- a. “Technical bid” will be evaluated only for the bidders who succeed in Stage 1.

- b. Authority will review the technical bids of the short-listed bidders to determine whether the technical bids are substantially responsive. Bids that are not substantially responsive are liable to be disqualified at Authority's discretion.
- c. The bidders' technical solutions proposed in the bid document shall be evaluated as per the requirements specified in the RfP and technical evaluation framework as mentioned in Technical Evaluation Criteria and details in Section 3.6 & 3.6.1
- d. Bidders shall be earmark an exclusive open space for where the bidder shall install smart envisaged components and demonstrate the "Proof-of-Concept" to the Technical Evaluation Committee appointed by the Authority. The place for showing demonstration would be provided by Authority and bidder may setup sample smart components and showcase live demonstrations to Technical Evaluation Committee
- e. Bidders should submit detailed – "***Approach & Methodology & Solutions proposed***"
- f. Each Technical Bid will be assigned a Technical Score out of a maximum of 100 points. Only the bidders who get **Technical Score of more than or equal to 60% in Technical Evaluation** will qualify for Commercial Evaluation stage.

### **3.5.3 Stage 3: Commercial Evaluation**

- a. All the technically qualified bidders will be notified to participate in Commercial Bid opening process.
- b. The commercial bids for the technically qualified bidders shall then be opened on the notified date and time and reviewed to determine whether the commercial bids are substantially responsive. Bids that are not substantially responsive are liable to be disqualified at Authority's discretion.
- c. Commercial bids shall be submitted in separate sealed cover in hard copy as per the format provided in Section 8 (Annexure 4), any deviation in template shall be liable for rejection. The summary of commercial bid alone shall be submitted online in the prescribed template given in the online tender portal.
- d. The bid price shall include all GST and levies and shall be in Indian Rupees and mentioned separately.
- e. Total Price shall be calculated based on the format provided in Section 8 (Annexure 4). Each of the Commercial bids shall be evaluated on a score of 100 points. The Commercial Score of the bidder shall be calculated with respect the lowest Total Price by any bidder. The methodology of Commercial Score shall be as follows.

f. Commercial Score of the bidder under consideration  
= (Lowest Total Price from all Commercial Bids / Total Price quoted in Commercial bid by the bidder under consideration) X 100

#### **3.5.4 Stage 4: Total Bid Evaluation**

a. The Total Score shall be based on Quality and Cost based Evaluation (QCBS). Technical Score shall have 50 % weightage and Commercial Score shall have 50% weightage.

b. The Total Score of the bidder =  $0.5 \times (\text{Technical Score}) + 0.5 \times (\text{Commercial Score})$

c. *The bidder achieving the highest Total Score shall be invited for negotiations for awarding the contract. In case of a tie where two or more bidders achieve the same highest Total Score, the bidder with the higher Technical Score will be invited first for negotiations for awarding the contract.*

### 3.6 Pre-Qualification Criteria

#	Eligibility Criteria	Document Proof	Supporting Document Reference
1	<p>The bidder shall either submit the bid as Sole Bidder or as consortium. Incase of Consortium bid, one of the entities of the consortium shall be a termed as Lead bidder and other(s) would be termed as consortium members.</p> <p>The Bidder (Sole / Lead member incase of Consortium) shall be a registered entity under relevant Act in India. The other consortium members of the consortium-bid shall be registered under relevant act in their country of incorporation (India / abroad)</p> <p>Note: Incase of Consortium : Max 3 companies (including the lead bidder) are allowed in a consortium. For mode details please refer section 2.2 of this volume in the RfP</p>	<ul style="list-style-type: none"> <li>• Incorporation Certificate                             <ul style="list-style-type: none"> <li>○ Sole / Lead Bidder : Copy of Certificate of Incorporation / Registration under Companies Act in India</li> <li>○ Other member in the Consortium shall be Registered under suitable Act respective country of incorporation</li> </ul> </li> <li>• For Consortium bids : Consortium Agreement clearly stating the                             <ul style="list-style-type: none"> <li>○ roles and responsibilities of each member. The Lead Bidder shall have maximum Stake in the consortium</li> <li>○ All the consortium members are equally responsible and jointly &amp; severally liable under this RfP for                                     <ul style="list-style-type: none"> <li>a.The delivery of products &amp; services</li> <li>b.Successful completion of this entire Project</li> <li>c.Compliance the SLAs</li> </ul> </li> <li>○ Authorization by authorized signatories of Consortium members authorizing the Lead Bidder to bid on their behalf for this RfP</li> </ul> </li> </ul>	PQ_1

#	Eligibility Criteria	Document Proof	Supporting Document Reference
2	<p>The Average Annual Turnover (TO) in Indian Rupees for last 3 audited financial years.</p> <ul style="list-style-type: none"> <li>• For Sole Bidder – Min INR 150 Cr</li> <li>• For Consortium Bid                             <ul style="list-style-type: none"> <li>○ Turnover of all members together should have Min. INR 150 Cr</li> <li>○ Lead Bidder should have minimum Turnover of INR 75 Cr</li> <li>○ Other members should have minimum Turnover of INR 5 Cr</li> </ul> </li> </ul>	<ul style="list-style-type: none"> <li>• Certificate from the Statutory auditor clearly specifying the annual turnover for the specified years</li> </ul>	PQ_2
3	<p>The Positive Net Worth in Indian Rupees for FY 2016-2017</p> <ul style="list-style-type: none"> <li>• For Sole Bidder – INR 30 Cr</li> <li>• For Consortium                             <ul style="list-style-type: none"> <li>○ All members put together should have min. INR 30 Cr PNW requirement</li> <li>○ Lead Bidder should have minimum INR 15Cr. PNW</li> <li>○ Other members should have minimum INR 1 Cr. PNW</li> </ul> </li> </ul>	<ul style="list-style-type: none"> <li>• Certificate from the Statutory auditor clearly specifying the net worth of the firm                             <ul style="list-style-type: none"> <li>○ Incase of consortium every entity within consortium (Lead &amp; consortium member) should produce this certificate from the respective Statutory auditor</li> </ul> </li> </ul>	PQ_3
4	<p>Prior Project Experience Implementing any of the 2 smart components for any smart city projects and other Project of Government Department /agencies in India Smart Components includes,</p> <ol style="list-style-type: none"> <li>1. Command &amp; Control Centre</li> <li>2. Disaster Management / City Surveillance System/Safe City,</li> <li>3. Smart Poles /Environmental Sensors /Public Address System/Emergency</li> </ol>	<ul style="list-style-type: none"> <li>• Work Order / Copy of Contract for the project highlighting the scope of work undertaken</li> <li>• Client Certificate for Completion / work in-progress</li> </ul>	PQ_4

#	Eligibility Criteria	Document Proof	Supporting Document Reference
	<p>Box/Variable Messaging Displays,</p> <p>4. Smart Cloud based Data Center/Disaster Recovery Center Projects,</p> <p>5. Integration of utilities such /as water supply /Power/Sewerage/Drainage etc.</p> <p>6. ERP/eGovernance solution for Government / Quasi Government / PSU at scale of min. INR 25 crores</p>		
5	<p>The Sole bidder or all member (lead bidder +all consortium members) should not have been blacklisted by any Central / State Government / Government Undertaking / ULB in India as on the bid submission date</p>	<ul style="list-style-type: none"> <li>• Undertaking by the authorized signatory of bidder (In case of Consortium to be provided by each member) as per format given in Annexure 2, section 6.4</li> </ul>	PQ_5
6	<p>The Sole Bidder or the Lead Bidder in case of a Consortium, should possess any three of the below Certifications which are valid at the time of bid submission:</p> <ul style="list-style-type: none"> <li>• ISO 9001:2008 or above – for Quality Process</li> <li>• ISO 20000:2011 for IT Service Management</li> <li>• ISO 27001:2005 for Information Security Management System</li> <li>• CMMI III or above – for IT maturity</li> </ul>	<ul style="list-style-type: none"> <li>• Copies of valid certificates in the name of the sole bidder or the Lead bidder in case of a Consortium</li> </ul>	PQ_6

### 3.7 Technical Evaluation Criteria

#### A. Technical Evaluation Framework

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

Category	Evaluation Framework	Weightage
A	Organizational Capability	30
B	Prior Experience in Smart Components	35
C	Proof of Concept	35
<b>Technical Score</b>		<b>100</b>

#### B. Technical Evaluation Parameters

#	Technical Evaluation Criteria	Technical Evaluation parameter	Points	Supporting Forms												
<b>A. Bidders Organization Capability</b>																
A1	<b>Average Annual Turnover of last 3 audited financial years.</b> In case of consortium, the Turn Over of all the members will be taken together	<table border="1"> <thead> <tr> <th>Turnover (in INR)</th> <th>Marks</th> </tr> </thead> <tbody> <tr> <td>&gt;500 Cr.</td> <td>10</td> </tr> <tr> <td>&gt;= 375 Cr. and &lt;500 Cr.</td> <td>8</td> </tr> <tr> <td>&gt;= 300 Cr. and &lt;375 Cr.</td> <td>6</td> </tr> <tr> <td>&gt;= 225 Cr. and &lt;300 Cr.</td> <td>4</td> </tr> <tr> <td>&gt;150 Cr. and &lt; 225 Cr.</td> <td>2</td> </tr> </tbody> </table>	Turnover (in INR)	Marks	>500 Cr.	10	>= 375 Cr. and <500 Cr.	8	>= 300 Cr. and <375 Cr.	6	>= 225 Cr. and <300 Cr.	4	>150 Cr. and < 225 Cr.	2	<b>10</b>	<i>Certificate from Statutory Auditor from the respective organization</i>
Turnover (in INR)	Marks															
>500 Cr.	10															
>= 375 Cr. and <500 Cr.	8															
>= 300 Cr. and <375 Cr.	6															
>= 225 Cr. and <300 Cr.	4															
>150 Cr. and < 225 Cr.	2															
A2	<b>Average Annual Turnover from eGovernance / ERP Solution to State / Central / Government / Quasi Government/ULB at of last 3 audited financial years.</b> In case of consortium, the Turn Over of all the members will be taken together	<table border="1"> <thead> <tr> <th>eGovernance based Turnover (in INR)</th> <th>Marks</th> </tr> </thead> <tbody> <tr> <td>&gt;= 65 Cr.</td> <td>10</td> </tr> <tr> <td>&gt;= 55 Cr. and &lt;65 Cr.</td> <td>8</td> </tr> <tr> <td>&gt;= 45 Cr. and &lt;55 Cr.</td> <td>6</td> </tr> <tr> <td>&gt;= 35 Cr. and &lt;45 Cr.</td> <td>4</td> </tr> <tr> <td>&gt;= 25 Cr. and &lt;35 Cr.</td> <td>2</td> </tr> </tbody> </table>	eGovernance based Turnover (in INR)	Marks	>= 65 Cr.	10	>= 55 Cr. and <65 Cr.	8	>= 45 Cr. and <55 Cr.	6	>= 35 Cr. and <45 Cr.	4	>= 25 Cr. and <35 Cr.	2	<b>10</b>	<i>Certificate from Statutory Auditor from the respective organization</i>
eGovernance based Turnover (in INR)	Marks															
>= 65 Cr.	10															
>= 55 Cr. and <65 Cr.	8															
>= 45 Cr. and <55 Cr.	6															
>= 35 Cr. and <45 Cr.	4															
>= 25 Cr. and <35 Cr.	2															

#	Technical Evaluation Criteria	Technical Evaluation parameter	Points	Supporting Forms								
A3	<p><b>Net worth as on 2016-17 financial year end</b> In case of consortium, the Net worth of all the members will be taken together</p>	<table border="1"> <thead> <tr> <th>Net Worth (in INR)</th> <th>Marks</th> </tr> </thead> <tbody> <tr> <td>&gt;= 50 Cr.</td> <td>5</td> </tr> <tr> <td>&gt;= 40 Cr. and &lt; 50 Cr.</td> <td>3.5</td> </tr> <tr> <td>&gt;= 30 Cr. and &lt; 40 Cr.</td> <td>2</td> </tr> </tbody> </table>	Net Worth (in INR)	Marks	>= 50 Cr.	5	>= 40 Cr. and < 50 Cr.	3.5	>= 30 Cr. and < 40 Cr.	2	5	Certificate from Statutory Auditor
Net Worth (in INR)	Marks											
>= 50 Cr.	5											
>= 40 Cr. and < 50 Cr.	3.5											
>= 30 Cr. and < 40 Cr.	2											
A4	<p><b>CMMi Certification</b></p>	<table border="1"> <thead> <tr> <th>Certification</th> <th>Marks</th> </tr> </thead> <tbody> <tr> <td>CMMI level V</td> <td>2</td> </tr> </tbody> </table>	Certification	Marks	CMMI level V	2	2	Copy of valid certificate as on date of bid				
Certification	Marks											
CMMI level V	2											
A5	<p><b>Resource Strength (Full time Employees (FTE) in who are Professionally Qualified in ICT related fields)</b> In case of consortium, the FTE Professionally Qualified in ICT related fields of all members of Consortium Members</p>	<table border="1"> <thead> <tr> <th>Number of FTE</th> <th>Marks</th> </tr> </thead> <tbody> <tr> <td>&gt; 500 FTE</td> <td>3</td> </tr> <tr> <td>&gt; 400 FTE to =&lt;500 FTE</td> <td>2</td> </tr> <tr> <td>&gt; 300 FTE to =&lt;400 FTE</td> <td>1</td> </tr> </tbody> </table>	Number of FTE	Marks	> 500 FTE	3	> 400 FTE to =<500 FTE	2	> 300 FTE to =<400 FTE	1	3	Copy of certificate of HR department
Number of FTE	Marks											
> 500 FTE	3											
> 400 FTE to =<500 FTE	2											
> 300 FTE to =<400 FTE	1											
<p><b>B. Project Experience of Bidder</b></p>												
B1	<p><b>Command and Control Center /Integrated eGovernance /Integrated ERP solution</b></p>	<p>The Bidder (Sole Bidder / Consortium bidder) should have experience in this domain <b>Command and Control Center / Integrated eGovernance / Integrated ERP solution</b> with min. INR value of INR 25 crores in a project.</p> <p>Marks are allocated based on number of projects executed</p> <table border="1"> <thead> <tr> <th>No. of Projects</th> <th>Marks</th> </tr> </thead> <tbody> <tr> <td>&gt;=3</td> <td>5</td> </tr> <tr> <td>= 2</td> <td>3.5</td> </tr> <tr> <td>= 1</td> <td>2</td> </tr> </tbody> </table>	No. of Projects	Marks	>=3	5	= 2	3.5	= 1	2	5	<p>&gt; Copy of Work Order and</p> <p>&gt; Client certificate of Work in Progress / completed</p>
No. of Projects	Marks											
>=3	5											
= 2	3.5											
= 1	2											



#	Technical Evaluation Criteria	Technical Evaluation parameter	Points	Supporting Forms								
B2	<b>Disaster Management</b>	<p>The bidder (either lead or any member of consortium) should have experience in executing Disaster Management Project</p> <p>Each project for city of minimum 5 lakh population is considered as one unit for integration with Disaster Management solutions, is considered as one project.</p> <p>Marks are allocated based on number of projects executed</p> <table border="1"> <thead> <tr> <th>No. of Projects</th> <th>Marks</th> </tr> </thead> <tbody> <tr> <td>&gt;=3</td> <td>5</td> </tr> <tr> <td>= 2</td> <td>3.5</td> </tr> <tr> <td>= 1</td> <td>2</td> </tr> </tbody> </table>	No. of Projects	Marks	>=3	5	= 2	3.5	= 1	2	5	<p>&gt; Copy of Work Order and</p> <p>&gt; Client certificate of Work in Progress / completed</p>
No. of Projects	Marks											
>=3	5											
= 2	3.5											
= 1	2											
B3	<b>City Surveillance Projects with required network infrastructure.</b>	<p>The bidder (either lead or any member of consortium) should have experience in executing Disaster and City surveillance projects.</p> <p>Each City Surveillance project with minimum of 300 cameras or more (in a single work order) in outdoor or public area is considered as one Project. Marks are allocated based on number of projects executed</p> <table border="1"> <thead> <tr> <th>No. of Projects</th> <th>Marks</th> </tr> </thead> <tbody> <tr> <td>&gt;=3</td> <td>5</td> </tr> <tr> <td>= 2</td> <td>3.5</td> </tr> <tr> <td>= 1</td> <td>2</td> </tr> </tbody> </table>	No. of Projects	Marks	>=3	5	= 2	3.5	= 1	2	5	<p>&gt; Copy of Work Order and</p> <p>&gt; Client certificate of Work in Progress / completed</p>
No. of Projects	Marks											
>=3	5											
= 2	3.5											
= 1	2											
B4	<b>Cloud Hosted Smart Data Center</b>	<p>The bidder (either lead or any member of consortium) should have experience in executing cloud hosted projects.</p> <p>Each project with cloud hosted e-governance project worth more than Rs 2 Cr is considered as one project. Marks are allocated based on number of projects executed</p>	5	<p>&gt; Copy of Work Order and</p> <p>&gt; Client certificate of Work in Progress / completed</p>								

#	Technical Evaluation Criteria	Technical Evaluation parameter		Points	Supporting Forms								
		No. of Projects	Marks										
		>=3	5										
		= 2	3.5										
		= 1	2										
B5	<p><b>Smart Poles/ Smart Sensors/ VMD/PA/ECB.</b></p>	<p>The bidder (either lead or any member of consortium) should have experience in executing Smart Poles/ Sensors/ Digital Signboards / Public Address Systems/ Variable Messaging Display projects/ Emergency Call Button.</p> <p>Each project of min. of 10 'unit quantities' of any of the smart components such as Smart Poles, Digital Signboards, Variable Messaging Displays, Sensors, Public Address System, Emergency Call Button shall be considered as a project.</p> <p>Marks are allocated based on number of projects executed</p> <table border="1"> <thead> <tr> <th>No. of Projects</th> <th>Marks</th> </tr> </thead> <tbody> <tr> <td>&gt;=3</td> <td>5</td> </tr> <tr> <td>= 2</td> <td>3.5</td> </tr> <tr> <td>= 1</td> <td>2</td> </tr> </tbody> </table>		No. of Projects	Marks	>=3	5	= 2	3.5	= 1	2	5	<p>&gt; Copy of Work Order and</p> <p>&gt; Client certificate of Work in Progress / completed</p>
No. of Projects	Marks												
>=3	5												
= 2	3.5												
= 1	2												
B6	<p><b>Integration with Smart Utility Solutions such as SCADA- Water, Power, GIS, ITMS</b></p>	<p>The bidder should have experience in projects of integration with Smart Utility Solutions such as SCADA- Water / Power / GIS / ITMS / Smart Sewerage/ Drainage</p> <p>Each project of Indian Rupees 2 Cr. Or more for integration with Smart Utility solutions will be considered as one project.</p> <p>Marks are allocated based on number of projects executed</p> <table border="1"> <thead> <tr> <th>No. of Projects</th> <th>Marks</th> </tr> </thead> <tbody> <tr> <td>&gt;=3</td> <td>5</td> </tr> <tr> <td>= 2</td> <td>3.5</td> </tr> <tr> <td>= 1</td> <td>2</td> </tr> </tbody> </table>		No. of Projects	Marks	>=3	5	= 2	3.5	= 1	2	5	<p>&gt; Copy of Work Order and</p> <p>&gt; Client certificate of Work in Progress / completed</p>
No. of Projects	Marks												
>=3	5												
= 2	3.5												
= 1	2												

#	Technical Evaluation Criteria	Technical Evaluation parameter	Points	Supporting Forms								
B7	<b>Network Connectivity</b>	<p>The bidder (either lead or any member of consortium) should have experience in executing Network Bandwidth/ Connectivity with Different smart components in city projects.</p> <p>Each project of Indian Rupees 1 Cr. or more for integration with Smart Utility solutions will be considered as one project.</p> <p>Marks are allocated based on number of projects executed</p> <table border="1"> <thead> <tr> <th>No. of Projects</th> <th>Marks</th> </tr> </thead> <tbody> <tr> <td>&gt;=3</td> <td>5</td> </tr> <tr> <td>= 2</td> <td>3.5</td> </tr> <tr> <td>= 1</td> <td>2</td> </tr> </tbody> </table>	No. of Projects	Marks	>=3	5	= 2	3.5	= 1	2	5	<p>&gt; Copy of Work Order and</p> <p>&gt; Client certificate of Work in Progress / completed</p>
No. of Projects	Marks											
>=3	5											
= 2	3.5											
= 1	2											
<b>C. Proof of Concept</b>												
C1	<b>Chennai City Requirements</b>	<ul style="list-style-type: none"> <li>Understanding of the Chennai city Requirements</li> </ul>	2	<i>Detailed in Approach &amp; Methodology</i>								
C2	<b>Dove-tailed Solution</b>	<p>Points are allocated based on the Proposed Solution for below criteria</p> <table border="1"> <thead> <tr> <th>Parameter</th> <th>Marks</th> </tr> </thead> <tbody> <tr> <td>Solution fitment Mapping</td> <td>2</td> </tr> <tr> <td>Unique Selling Proposition</td> <td>2</td> </tr> </tbody> </table>	Parameter	Marks	Solution fitment Mapping	2	Unique Selling Proposition	2	5	<i>Detailed in Approach &amp; Methodology</i>		
Parameter	Marks											
Solution fitment Mapping	2											
Unique Selling Proposition	2											

#	Technical Evaluation Criteria	Technical Evaluation parameter	Points	Supporting Forms																						
C3	<b>Architecture Soundness</b>	<p>Each of the following criteria for proposed solution by the bidder will be evaluated:</p> <table border="1"> <thead> <tr> <th>Parameter</th> <th>Marks</th> </tr> </thead> <tbody> <tr> <td>Redundancy</td> <td>1</td> </tr> <tr> <td>High Availability</td> <td>1</td> </tr> <tr> <td>Interoperability/Integration capability</td> <td>1</td> </tr> <tr> <td>Machine Learning based + AI</td> <td>1</td> </tr> <tr> <td>Programming of SOP</td> <td>1</td> </tr> <tr> <td>IoT layer</td> <td>1</td> </tr> <tr> <td>Dashboard Data Analytics</td> <td>1</td> </tr> <tr> <td>Scalability</td> <td>1</td> </tr> <tr> <td>Network Connectivity</td> <td>1</td> </tr> <tr> <td>Ease of Business</td> <td>1</td> </tr> </tbody> </table>	Parameter	Marks	Redundancy	1	High Availability	1	Interoperability/Integration capability	1	Machine Learning based + AI	1	Programming of SOP	1	IoT layer	1	Dashboard Data Analytics	1	Scalability	1	Network Connectivity	1	Ease of Business	1	<b>10</b>	<i>Detailed in Approach &amp; Methodology</i>
Parameter	Marks																									
Redundancy	1																									
High Availability	1																									
Interoperability/Integration capability	1																									
Machine Learning based + AI	1																									
Programming of SOP	1																									
IoT layer	1																									
Dashboard Data Analytics	1																									
Scalability	1																									
Network Connectivity	1																									
Ease of Business	1																									
C4	<b>Project Plan</b>	Implementation plan (with Gantt week-wise Resource Loading)	<b>2</b>	<i>Detailed in Approach &amp; Methodology</i>																						
C5	<b>Project Team</b>	<p>Each of the following 3 profiles meeting the qualifications in the following section Marks would be awarded based on the profiles compliance to the minimum requirement specified</p> <table border="1"> <thead> <tr> <th>Profile</th> <th>Marks</th> </tr> </thead> <tbody> <tr> <td>Project Director with experience of minimum 15 years</td> <td>2</td> </tr> <tr> <td>Project Manager with experience of minimum 10 years</td> <td>2</td> </tr> <tr> <td>Command &amp; Communications/ Control Center Expert with experience of minimum 10 years</td> <td>2</td> </tr> </tbody> </table>	Profile	Marks	Project Director with experience of minimum 15 years	2	Project Manager with experience of minimum 10 years	2	Command & Communications/ Control Center Expert with experience of minimum 10 years	2	<b>6</b>	<i>Detailed in Approach &amp; Methodology</i>														
Profile	Marks																									
Project Director with experience of minimum 15 years	2																									
Project Manager with experience of minimum 10 years	2																									
Command & Communications/ Control Center Expert with experience of minimum 10 years	2																									
C6	<b>Live Prototype Demonstration</b>	Each of the following components of the solution demonstrated by the bidder will be evaluated:	<b>10</b>	<i>Detailed in Approach &amp; Methodology</i>																						

#	Technical Evaluation Criteria	Technical Evaluation parameter		Points	Supporting Forms
		Parameter	Marks		
		Disaster Management	2		
		Surveillance	2		
		City Dashboard Integration	2		
		IoT + Data Analytics	2		
		Smart Sensors	2		

### 3.7.1 Key Personnel Criteria

SI shall provide adequate number of personnel, each responsible for a specific role within the project. SI shall provide clear definition of the role and responsibility of each individual personnel. SI shall have a defined hierarchy and reporting structure for various teams that shall be part of the project. SI has to provide the list of proposed Resources for the Project. Any changes in Resource deployment will have to be approved by the Authority.

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

All the below mentioned Positions shall be Onsite throughout the entire project implementation phase.

#	Position	Minimum Qualifications & Experience
1.	Project Director	a) Education: BE/B.Tech & MCA/M. Tech/MBA from a recognized educational institution b) Experience: Minimum 10 years in IT sector. Should have more than 10 years of experience of handling such large projects
2.	Project Manager	a) Education: MBA/MCA/M. Tech & B. Tech/B.E. from a recognized educational institution b) Experience: Minimum 10 years in IT sector. Should have more than 5 years of experience of handling such large projects as a project manager c) Should preferably have PMP or Prince2 certification
3.	Command & Communications/Control Center Expert	a) B.Tech / M.Tech/Post Graduate from a recognized educational institution d) Experience: Minimum 10 years. Should have experience in designing & implementing Command Center for minimum 2 projects of similar nature.
4.	Solution Architect	a) Education: MCA/M. Tech/B. Tech/B.E. from a recognized educational institution b) Experience: Minimum 10 years in IT sector. Should have experience of more than 3 years as a Solution Architect in large projects of similar nature
5.	IOT Expert	a) B.Tech / M.Tech/Post Graduate from a recognized educational institution b) Experience: Minimum 10 years. Should have experience in designing & implementing IOT for minimum 2 projects of similar nature.
6.	QA Manager	a) B.Tech / M.Tech/MBA/MCA from a recognized educational institution b) Experience: Should have a minimum 5 years of experience

-		a) B.Tech / M.Tech/MBA/MCA from recognized educational institution
7.	Master Trainer	b) Experience: Should have a minimum 4 years of experience in conducting trainings for similar applications & solutions

Note: Profiles No 1 to 3 are (shaded rows in above table) chosen for Technical evaluation criteria. The Resource (manpower) plan for Implementation Phase to be provided as per format provided in 7.5.3 (I)

Apart from the above –mentioned resources, the Bidder shall also propose manpower to be deployed during the Operation & Maintenance phase of the Project as provided in the format 7.5.3 II.

Any additional or support manpower shall be estimated and should be accounted for in the Commercial proposal by the selected bidder, so that, the project as per the scope defined and agreement are fulfilled, and the project objectives are met.

#### **4 Award of Contract**

##### **4.1 Notification of Award**

GCC / CSCL will notify the successful Bidder by e-mail/post/in person. To be confirmed by the Bidder in writing by post/in person.

The bidder achieving the highest Total Score in QCBS evaluation as per section 3.6 shall be invited for negotiations for awarding the contract. In case of a tie where two or more bidders achieve the same highest Total Score, the bidder with the higher Technical Score will be invited first for negotiations for awarding the contract.

##### **4.2 Signing of Contract**

After the notification of award, GCC / CSCL will issue Letter of Acceptance (LoA). On receipt of the Performance Bank Guarantee, a contract agreement shall be signed between the successful bidder and GCC / CSCL. The Master Service Agreement is provided in RfP Volume III.

##### **4.3 Performance Bank Guarantee (PBG)**

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

This **Performance Bank Guarantee** shall be for an amount equivalent to **5%** of total contract value. PBG shall be invoked by GCC / CSCL, in the event the Bidder:

- a. fails to meet the overall penalty condition as mentioned in RfP Volume II or any changes agreed between the parties,
- b. fails to perform the responsibilities and obligations as set out in the RfP to the complete satisfaction of GCC / CSCL,
- c. Misrepresents facts/information submitted to GCC / CSCL.

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

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

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

In case the project is delayed beyond the project schedule as mentioned in RfP Vol 2, the performance bank guarantee shall be accordingly extended by the Bidder till completion of scope of work as mentioned in RfP Volume II.

This Performance Bank Guarantee shall be valid up to the completion of the period of 'Go- Live' + 60 months for the Solution.

On satisfactory performance and completion of the order in all respects and duly certified to this effect by the GCC /CSCL, the PBG would be returned to the Bidder.

#### **4.4 Warranty & Maintenance**

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

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



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

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

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

The successful bidder hereby warrants GCC / CSCL that:

- i. The implemented integrated solution represents a complete, integrated solution meeting all the requirements as outlined in the RfP and further amendments if any and provides the functionality and performance, as per the terms and conditions specified in the contract.
- ii. The proposed integrated solution shall achieve parameters delineated in the technical specification/requirement.
- iii. The successful bidder shall be responsible for warranty services from licensors of products and services included in the systems till the complete cycle of this contract.
- iv. The successful bidder undertakes to ensure the maintenance of the acceptance criterion/standards in respect of the systems during the warranty period.

#### **4.5 Failure to agree with the Terms & Conditions of the RfP**

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

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

**5 Annexure 1 – Template for Pre-Bid Queries**

Bidder shall submit all pre-bid queries in excel in the following format.

#	Vol. No	Sec. No	Clause No	Page No	Content in the RfP	Clarification sought

## 6 Annexure 2 – Formats for Submission of the Pre-Qualification Bid

## 6.1 Pre-qualification bid checklist

#	Compliance Criteria	Document Proof	Compliance (Yes or No)	Ref. in bid
1.	Earnest Money Deposit	Bank Guarantee		NA
2.	Pre-Qualification Covering letter	Covering Letter		
3.	<p>The bidder shall either submit the bid as Sole Bidder or as consortium. In case of Consortium bid, one of the entities of the consortium shall be termed as Lead bidder and other(s) would be termed as consortium members.</p> <p>The Bidder (Sole / Lead member in case of Consortium) shall be a registered entity under relevant Act in India. The other consortium members of the consortium-bid shall be registered under relevant act in their country of incorporation (India / abroad)</p> <p>Note: In case of Consortium : Max 3 companies (including the lead bidder) are allowed in a consortium. For more details please refer section 2.2 of this volume in the RfP</p>	<ul style="list-style-type: none"> <li>• Incorporation Certificate <ul style="list-style-type: none"> <li>○ Sole / Lead Bidder : Copy of Certificate of Incorporation / Registration under Companies Act in India</li> <li>○ Other member in the Consortium shall be Registered under suitable Act respective country of incorporation</li> </ul> </li> <li>• For Consortium bids : Consortium Agreement clearly stating the <ul style="list-style-type: none"> <li>○ roles and responsibilities of each member. The Lead Bidder shall have maximum Stake in the consortium</li> <li>○ All the consortium members are equally responsible and jointly &amp; severally liable under this RfP for <ul style="list-style-type: none"> <li>a. The delivery of products &amp; services</li> <li>b. Successful completion of this entire Project</li> <li>c. Compliance the SLAs</li> </ul> </li> <li>○ Authorization by authorized signatories of Consortium members authorizing the</li> </ul> </li> </ul>		

		<i>Lead Bidder to bid on their behalf for this RfP</i>		
4.	<p>The Average Annual Turnover (TO) in Indian Rupees for last 3 audited financial years.</p> <ul style="list-style-type: none"> <li>• For Sole Bidder – Min INR 150 Cr</li> <li>• For Consortium Bid <ul style="list-style-type: none"> <li>○ Turnover of all members together should have Min. INR 150 Cr</li> <li>○ Lead Bidder should have minimum Turnover of INR 75 Cr</li> <li>○ Other members should have minimum Turnover of INR 5 Cr</li> </ul> </li> </ul>	<ul style="list-style-type: none"> <li>• Certificate from the Statutory auditor clearly specifying the annual turnover for the specified years</li> </ul>		
5.	<p>The Positive Net Worth in Indian Rupees for FY 2016-2017</p> <ul style="list-style-type: none"> <li>• For Sole Bidder – INR 30 Cr</li> <li>• For Consortium <ul style="list-style-type: none"> <li>○ All members put together should have min. INR 30 Cr PNW requirement</li> <li>○ Lead Bidder should have minimum INR 15Cr. PNW</li> <li>○ Other members should have minimum INR 1 Cr. PNW</li> </ul> </li> </ul>	<ul style="list-style-type: none"> <li>• Certificate from the Statutory auditor clearly specifying the net worth of the firm <ul style="list-style-type: none"> <li>○ In case of consortium every entity within consortium (Lead &amp; consortium member) should produce this certificate from the respective Statutory auditor</li> </ul> </li> </ul>		
6.	<p>Prior Project Experience Implementing any of the 2 smart components for any smart city projects and other Project of Government Department /agencies in India</p> <p>Smart Components includes,</p> <ol style="list-style-type: none"> <li>7. Command &amp; Control Centre</li> <li>8. Disaster Management / City Surveillance System/Safe City,</li> <li>9. Smart Poles /Environmental Sensors /Public Address System/Emergency Box/Variable Messaging Displays,</li> <li>10. Smart Cloud based Data Center/Disaster Recovery Center Projects,</li> <li>11. Integration of utilities such /as water supply /Power/Sewerage/Drainage etc.</li> </ol>	<ul style="list-style-type: none"> <li>• Work Order / Copy of Contract for the project highlighting the scope of work undertaken</li> <li>• Client Certificate for Completion / work in-progress</li> </ul>		

	12. ERP/eGovernance solution for Government / Quasi Government / PSU at scale of min. INR 25 crores			
7.	The Sole bidder or all member (lead bidder +all consortium members) should not have been blacklisted by any Central / State Government / Government Undertaking / ULB in India as on the bid submission date	<ul style="list-style-type: none"> <li>Undertaking by the authorized signatory of bidder (In case of Consortium to be provided by each member) as per format given in Annexure 2, section 6.4</li> </ul>		
8.	<p>The Sole Bidder or the Lead Bidder in case of a Consortium, should possess any three of the below Certifications which are valid at the time of bid submission:</p> <ul style="list-style-type: none"> <li>ISO 9001:2008 or above – for Quality Process</li> <li>ISO 20000:2011 for IT Service Management</li> <li>ISO 27001:2005 for Information Security Management System</li> <li>CMMI III or above – for IT maturity</li> </ul>	<ul style="list-style-type: none"> <li>Copies of valid certificates in the name of the sole bidder or the Lead bidder in case of a Consortium</li> </ul>		

## 6.2 Pre-Qualification Bid Covering Letter

Date: dd/ mm / yyyy

To,

[            ]

Sub: **Cover Letter for Bid Submission**

Ref: RfP No. <<.....>> dated << .....>>

Dear Sir,

With reference to your “**Request for Proposal for Selection of System Integrator for Design, Supply, Implement, Commission, Operate & Manage the Command & Control Centre for Chennai Smart City**”, we hereby submit our Prequalification bid, Technical Bid and Commercial Bid for the same.

We hereby declare that:

- a. We hereby acknowledge and unconditionally accept that the GCC / CSCL can at its absolute discretion apply whatever criteria it deems appropriate, not just limiting to those criteria set out in the RfP and related documents, in short listing of Agency for providing services.
- b. We have submitted EMD of Indian Rupees[    ] Crores and Tender fee of Indian Rupees[    ] through Bank Guarantee in the <<Account details>>.
- c. We hereby declare that all information and details furnished by us in the Bid are true and correct, and all documents accompanying such application are true copies of their respective originals.
- d. We agree to abide by our offer for a period of 180 days from the date of opening of pre-qualification bid prescribed by **GCC / CSCL** and that we shall remain bound by a communication of acceptance within that time.
- e. We have carefully read and understood the terms and conditions of the RfP and the conditions of the contract applicable to the RfP. We do hereby undertake to provision as per these terms and conditions.
- f. In the event of acceptance of our bid, we do hereby undertake:
  - i. To supply the products and commence services as stipulated in the RfP document
  - ii. To undertake the project services for entire contract period from the date of signing of the contract as mentioned in the RfP document.
  - iii. We affirm that the prices quoted are inclusive of design, development, delivery, installation, commissioning, training, providing facility management and handholding support, and inclusive of all out of pocket expenses, GST, levies discounts etc.
- g. We do hereby undertake, that, until a formal contract is prepared and executed, this bid, together with your written acceptance thereof and notification of award of contract, shall constitute a binding contract between us.

- h. We understand that the **GCC / CSCL** may cancel the bidding process at any time and that **GCC / CSCL** is not bound to accept any bid that it may receive without incurring any liability towards the bidder.
  
- i. We fully understand and agree to comply that on verification, if any of the information provided in our bid is found to be misleading the selection process, we are liable to be dismissed from the selection process or termination of the contract during the project, if selected to do so

In case of any clarifications please contact \_\_\_\_\_ email at \_\_\_\_\_

Thanking you,

Yours sincerely,

(Signature of the Lead bidder)

Printed Name

Designation

**Seal**

Date:

Place:

Business Address:

### 6.3 Company profile

**A. Brief company profile** (Incase of consortium bid this same table details to be filled for the Lead & Consortium Members as well)

Sl. No.	Particulars	Description or details
1.	Name of Bidder	
2.	Legal status of Bidder (company, Pvt. Ltd., LLP etc.)	
3.	Main business of the Bidder	
4.	Registered office address	
5.	Incorporation/Registration date and number	
6.	GST number	
7.	PAN details	
8.	Primary Contact Person (Name, Designation, address, mobile number, fax, email)	
9.	Secondary Contact Person (Name, Designation, address, mobile number, fax, email)	
10.	EMD details	
11.	Role in Consortium (if applicable)	Brief scope of work in the consortium

**B. Certificate of Incorporation/Registration (required for both bidder and Consortium members)**

#### C. Financial Turnover

The financial turnover of the company is provided as follows:

	2016 – 17	2015 – 16	2014 – 15
Annual Turnover			

Copy of audited financial statements or declaration from the appointed statutory auditor to be provided as proof of the financial turnover

Positive net worth, as on the last date of latest audited financial year. Copy of self-certified statutory auditor certificate to be submitted along with the bid



**6.4 Declaration of Non-Blacklisting**

*(To be provided on the Company letter head)*

**Declaration for Lead Bidder:**

Place

Date

To,

[       ]

Subject: Self Declaration of not been blacklisted in response to the **Request for Proposal for Selection of System Integrator for Design, Supply, Implement, Commission, Operate & Manage the Command & Control Centre for Chennai Smart City**

Ref: RfP No. <<.....>> dated << .....>>

Dear Sir,

We confirm that our company or firm, \_\_\_\_\_, is currently not blacklisted in any manner whatsoever by any of the State or UT and or Central Government in India on any ground including but not limited to indulgence in corrupt practice, fraudulent practice, coercive practice, undesirable practice or restrictive practice.

(Signature of the Lead Bidder)

Printed Name

Designation

**Seal**

Date:

Place:

Business Address:

**Declaration for Consortium Member:**

*(To be provided on the Company letter head)*

{Place}

{Date}

To,

[                    ]

Subject: Self Declaration of not been blacklisted in response to the **Request for Proposal for Selection of System Integrator for Design, Supply, Implement, Commission, Operate & Manage the Command & Control Centre for Chennai Smart City**

Ref: RfP No. <<.....>> dated << .....>>

Dear Sir,

We confirm that our company or firm, \_\_\_\_\_, is currently not blacklisted in any manner whatsoever by any of the State or UT and or Central Government in India on any ground including but not limited to indulgence in corrupt practice, fraudulent practice, coercive practice, undesirable practice or restrictive practice.

(Signature of the Consortium Member)

Printed Name

Designation

**Seal Date:**

Place: Business Address:

## 6.5 No Deviation Certificate

*(To be provided on the Company letter head)*

{Place}

{Date}

To,

[                    ]

This is to certify that our offer is exactly in line with your tender enquiry/RfP (including amendments) no. \_\_\_\_\_ dated \_\_\_\_\_. This is to expressly certify that our offer contains no deviation either Technical (including but not limited to Scope of Work, Business Requirements Specification, Functional Requirements Specification, Hardware Specification and Technical Requirements Specification) or Commercial in either direct or indirect form.

(Authorized Signatory)

Signature:

Name:

Designation:

Address:

Seal:

Date:

## 6.6 Total Responsibility Certificate

*(To be provided on the Company letter head)*

{Place}

{Date}

To,

[                    ]

This is to certify that we undertake the total responsibility for the defect free operation of the proposed solutions as per the requirement of the RfP for the duration mentioned in all the volumes of the RfP.

(Authorized Signatory)

Signature:

Name:

Designation:

Address:

Seal:

Date:

**6.7 Self-certificate for Project execution experience (In Bidding Entity's Letter Head)**

This is to certify that <Name of the Bidding entity> has been awarded with < Name of theProject > as detailed under:

<b>Name of the Project</b>	
<b>Client's Name, Contact no. and Complete Address</b>	
<b>Contract Value for the bidder (in Indian Rupees)</b>	
<b>Current status of the project (Completed/Ongoing)</b>	
<b>Activities completed by bidding entity as on bid submission date</b> <i>(N.B Only relevant activities as sought in the Criteria to be included)</i>	
<b>Value of Work completed for which payment has been received from the client.</b>	
<b>Date of Start</b>	
<b>Date of Completion</b>	

(Authorized Signatory)

Signature:

Name:

Designation:

Bidding entity's name

Address:

Seal:

Date:

**7 Annexure 3 – Formats for Submission of the Technical Bid**

**7.1 Technical Bid Check-List**

SI #	Checklist Item	Compliance (Yes/No)	Page No. and Section No. in the Bid
1	Technical Bid Letter		
2	Credential summary		
3	Supporting Documents as Technical Evaluation Criteria prescribed in section 3.6 of this volume of this RfP		
4	Detailed proposed solution		
5	Project plan and manpower plan		
6	Proposed CVs of Project Team		
7	Compliance to Requirement (Technical / Functional Specifications)		
8	Proposed unpriced Bill of Material		
9	Manufacturers'/Producers' Authorization Form Anti-Collusion certificate		
10	Anti-Collusion Certificate		
11	Non-disclosure agreement		
12	EMD		

## 7.2 Technical Bid Covering Letter

Date:  
dd/mm/yyyy

To,

[                    ]

Subject: **Request for Proposal for Selection of System Integrator for Implementation of for Design, Supply, Implement, Commission, Operate & Manage the Command & Control Centre for Chennai Smart City**

Ref: RfP No. <<.....>> dated << .....>>

Dear Sir,

I (in case of single bidder) or We, <<name of the undersigned Bidder and consortium members>>, having read and examined in detail all the bidding documents in respect of **“Request for Proposal for Selection of System Integrator for Implementation of for Design, Supply, Implement, Commission, Operate & Manage the Command & Control Centre for Chennai Smart City”** do hereby propose to provide our services as specified in the bid submitted by us.

It is hereby confirmed that I / We are entitled to act on behalf of our company / corporation / firm / organization and empowered to sign this document as well as such other documents, which may be required in this connection.

We declare that all the services shall be performed strictly in accordance with the RfP documents.

We confirm that the information contained in this response or any part thereof, including its exhibits, and other documents and instruments delivered or to be delivered to GCC / CSCL, is true, accurate, verifiable and complete. This response includes all information necessary to ensure that the statements therein do not in whole or in part mislead the department in its evaluation process. We also confirm that we shall not attract conflict of interest in principle.

We hereby declare that in case the contract is awarded to us, we shall submit the contract Performance bank guarantee in the form prescribed at Annexure 5 (a) of Section 9 of the RfP Volume I.

We hereby declare that our bid is made in good faith, without collusion or fraud and the information contained in the bid is true and correct to the best of our knowledge and belief.

We understand that our bid is binding on us and that you are not bound to accept a Bid you receive. This bid is valid for 180 days after opening of technical bid. We shall extend the validity of the bid if required by GCC / CSCL.

Thanking you,

Yours sincerely,

(Signature of the Lead Bidder)

Printed Name

Designation

**Seal**

Date:

Place:

Business Address:



**7.3 Credential Summary**

Project #	Project Name	Client Name	Client Type	Project Value (in Indian Rupees)	Project Components	Documentary evidence provided	Project Status (Completed or
						(Yes or No)	Ongoing or Withheld)
1							
2							
3							
4							
5							
6							
7							

- *Client type – Indicate whether the client is Government or PSU or Private*
- *Project Components – Indicate the major project components like application development for security surveillance, command and control center, Maintenance, Hardware procurement and deployment, DC setup and maintenance, Facility management services, provisioning manpower, IT support and maintenance*
- *Documentary evidence provided – Indicate the documentary evidence provided with the detailed project credential like work order or purchase order or completion certificate or letter of appointment*
- *Project Status – Completed (date of project completion) or Ongoing (project start date)*

#### 7.4 Bidder’s Experience - Client Citations

Prime Bidder or Consortium member is requested to furnish the credentials in the following format for both Pre-qualification and Technical criterion. All credentials should be followed by relevant documentary proof.

Name of the Project & Location	
Client's Name and Complete Address	
Narrative description of project	
Contract Value for the bidder (in Indian Rupees)	
Date of Start	
Date of Completion	
Activities undertaken by prime bidder or consortium member	

*Note: If the project is ongoing, bidder must clearly specify which of the stages/phases/milestones are completed and which are ongoing and at what stage of completion and produce a self-certificate as per the format provided in Section 6.7.*

## 7.5 Overview of Proposed Solution

### 7.5.1 Structure of Proposed Solution

Bidders are required to provide a detailed approach & methodology to execute the entire project. Bidders shall articulate the response proposal addressing all pointers being evaluated in the Technical Evaluation Criteria. So that the same can translated in the form of presentation for showcasing to the Technical Evaluation Committee. The typical content under the technical proposal shall contain the following

#	Item
1.	<p><b>Understanding of requirement and Implementation approach</b></p> <ul style="list-style-type: none"> <li>· Understanding of requirements</li> <li>· Work Plan &amp; its adequacy</li> </ul>
2.	<p><b>Robustness and quality</b></p> <ul style="list-style-type: none"> <li>· End to end integrated solution proposed</li> <li>· Hardware deployment and integration approach encompassing all solutions</li> <li>· Timelines and modalities for implementation in a time bound manner</li> <li>· Project implementation approach or strategy and operations and maintenance plan including comprehensiveness of fallback strategy and planning during rollout</li> <li>· Any other area relevant to the scope of work and other requirements of the project</li> </ul>
3.	<p><b>Assessment of Manpower deployment, Training and Handholding plan</b></p> <ul style="list-style-type: none"> <li>· Deployment strategy of Manpower</li> <li>· Contingency management</li> <li>· Mobilization of existing resources and additional resources as required</li> <li>· Training and handholding strategy</li> </ul>

**7.5.2 Project Plan**

A **Detailed Project Plan** covering break-up of each phase into the key activities, along with the start and end dates must be provided as per format given below.

<b>Activity-wise Timelines</b>							
<b>Sl. No.</b>	<b>Detailed Work Break down structure</b>	<b>Month wise Program</b>					
		1	2	3	4	5	...
	Project Plan						
1	Activity 1						
1.1	Sub-Activity 1						
1.2	Sub-Activity 2						
2							
2.1							
2.2							
3							
3.1							
4							

**Activity-wise Timelines**

<b>Sl. No.</b>	<b>Item of Activity</b>	<b>Month wise Program</b>
----------------	-------------------------	---------------------------

*Note: The above activity chart is just for the purpose of illustration. Bidders are requested to provide detailed activity & phase wise timelines for executing the project with details of deliverables & milestones as per their bid.*

---

7.5.3 Manpower Plan

I. Till Go-Live (Implementation)

<b>Manpower distribution</b>										
S. No.	Role	Month wise time to be spent by each personnel (in days)						Total		
		Month 1	Month 2	Month 3	...	...	Go-Live			
1	Project Director								Onsite	
									Offsite	
2	Project Manager								Onsite	
3	Solution Architect (DC)								Onsite	
4	Command Center Expert								Onsite	
5	IOT Expert								Onsite	
6	QA Manager								Onsite	
7	Master Trainer								Onsite	
9	<Add more rows as required>								Onsite	
		<b>Total</b>								

**II. After Go-Live (Operation & Maintenance)**

<b>Manpower distribution</b>							
S. No.	Manpower Detailed Breakup	Years					Total
		Year 1	Year 2	Year 3	Year 4	Year 5	
1							Onsite/Offsite
2							Onsite/Offsite
3							Onsite/Offsite
4							Onsite/Offsite
5							Onsite/Offsite
6							Onsite/Offsite
7							Onsite/Offsite
8							Onsite/Offsite
9	<Add more rows as required>						Onsite/Offsite
		<b>Total</b>					

**7.6 Details of Resources proposed**

**7.6.1 Summary of Resources proposed**

Sr.No.	Name of the resource	Proposed Role	Highest Degree	Basic Qualification (e.g., B.Sc. or BE or MCA or Post Graduation)	Certifications (e.g., PMP or ITIL or TOGAF or CCNP etc.)	Total Experience (In Years)
1.						
2.						
3.						
4.						
5.						
6.						
7.						
8.						
9.						
10.						



7.7 Curriculum Vitae (CV) of Team Members

<b>1</b>	<b>Name:</b>				
<b>1.</b>	<b>Proposed position or role</b>	<i>(only one candidate shall be nominated for each position)</i>			
<b>2.</b>	<b>Date of Birth</b>		<b>Nationality</b>		
<b>3.</b>	<b>Education</b>	<b>Qualification</b>	<b>Name of School or College or University</b>	<b>Degree Obtained</b>	<b>Year of Passing</b>
<b>4.</b>	<b>Years of experience</b>	<i>(as required for the Profile)</i>			
<b>5.</b>	<b>Areas of Expertise and no. of years of experience in this area</b>				
<b>6.</b>	<b>Certifications and Trainings attended</b>				
<b>7.</b>	<b>Employment Record</b>	<b>Employer</b>	<b>Position</b>	<b>From</b>	<b>To</b>
		<i>[Starting with position and last 2 firms, list in reverse order, resent giving for each employment: dates of employment, name of employing organization, positions held.]</i>			

<p>8. <b>Detailed Tasks Assigned</b></p>	<p><i>(List all tasks to be performed under this project)</i></p>
--	---

**9. Relevant Work Undertaken that Best Illustrates the experience as required for the Role)**

Project 1	
Name of assignment	
Year	
Location	
Employer	
Main project features	
Position held	
Activities performed	
Project 2	
Name of assignment	
Year	
Location	
Employer	
Main project features	
Position held	
Activities performed	

## **7.8 Compliance to Requirement (Technical / Functional Specifications)**

*The bidder should provide compliance to the requirement specifications (both technical and functional) specified in the Annexures of the Volume II of this RfP. The same should be reproduced here, and compliance against each requirement line item should be marked. As part of this compliance to the line-by-line technical specifications from the respective OEM proposed for this solution. The bidders shall not have multiple OEMs for single product / infrastructure envisaged in the CCC.*

### 7.9 Proposed Bill of Material (Technical Bid)

The Bidder should provide the proposed Bill of Material (BoM) here. Bidders are required to mention the details of the make/brand and model against each line item, wherever applicable. The bid can be considered non-responsive in the absence of such details. Once the bidder provides this information in the submitted bid, the bidder cannot change it with any other component / equipment etc. of lower specifications / performance; it can only be upgraded at the time of actual deployment/installation.

Sl. #	Line Item	Unit of Measurement	Quantity Proposed	Make/Brand	Model Details	Full compliance with RFP Requirements (Yes/No)
<b>A</b>	<b>Command &amp; Communications Center (CCC)</b>					
1	Interior & Civil works for CCC as per scope & functional specifications of Non-IT	Sqft	2050			
2	Video Wall Solution- 50" DLP Smart GRID in a 12x2 arrangement with passive component to scale upto total of 14x3 cube arrangement	Nos	24			
3	War Room : Additional LED Smart Displays 55" (Min. 4 nos)	Nos	As Required			
4	Monitoring Desktops / Laptops for Line Department users (min 30), Live video and Playback from field camera (min 3), Helpdesk Operators (min. 4 Nos.)	Nos	As Required			
5	Network Multifunctional Devices with Colour Laser Printing (min. 4 nos)	Nos	As Required			
6	IP based Video Phones (min 60nos., monitoring workstations and war room)	Nos	As Required			
7	Indoor Fixed Dome Cameras for internal surveillance (design Qty as per standards)	Nos	As Required			

**Design, Supply, Implement, Commission, Operate & Manage the Command & Control Centre**

8	Edge Network Switches (L3) to connect Workstations (on HA)	LS	As Required			
9	Network Rack (on High Availability mode)	Lot	As Required			
10	ICT Networking (Passive Components)	Lot	As Required			
11	Electrical Cabling & Necessary Illumination Devices	Lot	As Required			
12	Public Address System connected to Building Management System	Set	As Required			
13	1st Layer Access Control System (RFID Or virtual) to CCC & War Room	Set	As Required			
14	2nd Layer Access Control System (Biometric based) to CCC & War Room	Set	As Required			
15	Digital Display Unit (40") for CCC & War Room and LCD Projector, including sealing mounting kit and motorized screen - 113"	Nos	As Required			
16	HVAC Air conditioners to humidifiers to suite 24x7 operations at CCC	Lot	As Required			
17	UPS with N+N configuration for critical load & Inverter for non-critical lighting load	Nos	As Required			
18	DG Sets (N + N Configuration)	Nos	As Required			
<b>B</b>	<b>Smart Data Center Solution on cloud model</b>					
1	DC Core Router	LS	As Required			
2	Internet Routers	LS	As Required			
3	DC Switches (Core, Application & rack)	LS	As Required			
4	Firewall (both Internal & External)	LS	As Required			
5	Intrusion Prevention System & Intrusion Detection System	LS	As Required			
6	Server load balancer	LS	As Required			
7	Enterprise Management System (with SLA Management HelpdeskManagement Network Management integrated BMS)	LS	As Required			
8	Anti-virus Software for Client & Servers	LS	As Required			
9	Backup & Archival Software	LS	As Required			

10	DC/DR cloud onsite monitoring workstation laptops for mgmt. staff	LS	As Required			
11	CCC's EPABX including two dedicated PRI lines at CCC premises	Nos	As Required			
12	CCC's centralised AAA Service, Wireless Controller for Wi-Fi based Services through Smart Pole	Nos	As Required			
13	CCC's Voice router for Help Desk Direct Voice calling, recording, Geo tagging & analysis at CCC premises	Nos	As Required			
14	Fire Proof Enclosure for Media offsite Storage at CCC premises	LS	As Required			
15	Servers on cloud model	LS	As Required			
16	Enterprise service Bus	LS	As Required			
17	Virtualisation software	LS	As Required			
18	RDBMS Licenses	LS	As Required			
19	Customisation/Integration of the existing systems of GCC / CSCL	LS	As Required			
20	Integration Services from various IOT, sensors, applications, social media, etc to CCC	LS	As Required			
21	IoT based analytics tool for Big Data Analytics & Dashboarding	LS	As Required			
22	Command and Communications Software (including Disaster Management)	LS	As Required			
23	Command & Communications Centre + Disaster Management Solution Implementation	LS	As Required			
24	Video Management Software licenses for different received from field cameras	Set	900			
25	GIS Map Engine, Integration of shape files on base map, crowdsourcing based data	Lot	As Required			
26	Viewing Software licenses for GIS services, Analytics, MIS, visualisations,	Lot	As Required			

27	Smart Governance Portal with customised dashboard, interfacing IOT, Social Media & other required integrations as per Scope of work defined	Lot	As Required			
<b>C</b>	<b>Smart Sensors</b>					
1	Environmental Sensors	Nos	18			
2	Rain-Gauge Sensors	Nos	30			
3	Flood Sensors	Nos	46			
4	Integration feeds on Fire alarm from various BMS systems of buildings to CCC	LS	As Required			
<b>D</b>	<b>Variable Messaging Board</b>					
1	3.8 X 1.9m Double side display VMS board including VMS controller as per specifications including mounting	Nos	17			
2	4.8 x 1.9m Double side display VMS board Including VMS controller as per specifications including mounting	Nos	33			
3	VMS Software licenses cost (bundled)	LS	As Required			
<b>E</b>	<b>CCTV Surveillance &amp; Disaster Management</b>					
1	Outdoor Box Cameras (Surveillance)	Nos	400			
2	Outdoor PTZ Cameras	Nos	100			
3	Poles for Cameras and equipment	LS	As Required			
4	Provisioning of Electrical Power	LS	As Required			
5	Industrial Grade Outdoor PoE Switches 16 Ports	LS	As Required			
6	Networking Cost (Passive Component: Junction Box, Patch Panel, LIU, OFC, Cat6 Cable, Patch Cords, Earthing, Lighting arrester)	LS	As Required			
7	UPS (Solar + Electric) with Batteries	LS	As Required			
8	Digging, Piping & Re-filling, including digging for electrical cabling	LS	As Required			
9	Flood Monitoring Cameras Fixed Cameras with Edge Analytics	Lot	68			
<b>F</b>	<b>Mobile Command &amp; Control Center</b>					
1	Pre-fabricated Vans	Nos	1			
2	Interoperable Communication Server with Software License	LS	As Required			

3	Desktop with Touch Panel Display	LS	As Required			
4	Outdoor PTZ Camera with mounting accessories	LS	As Required			
5	Outdoor Fixed Box Cameras with mounting accessories	LS	As Required			
6	Min. 64 GB SD card	LS	As Required			
7	Full HD Handycam (meeting all the basic parameters of Fix Box Camera) with wireless capability	LS	As Required			
8	Local server Storage for 7 days	LS	As Required			
9	Cost for fixtures and camera mounting charges Wireless Connectivity	LS	As Required			
10	Switch, Router, modem	LS	As Required			
11	LAN, GSM Modems, VSAT Setup for the Van, with capability to create a Wi-Fi / WiMAX network	LS	As Required			
12	GPRS SIM Module	LS	As Required			
13	GPS equipment with mobile terminal	LS	As Required			
14	Public Address System	LS	As Required			
15	Petrol Generator to support Mobile CCC	LS	As Required			
16	UPS backup for 1 hour	LS	As Required			
17	Fire Extinguisher	LS	As Required			
<b>H</b>	<b>Smart Poles</b>					
	<a href="#">Smart Poles</a>					
1	<a href="#">Smart Poles 16 mtrs</a>	LS	50			
	<a href="#">Smart Street Light</a>					
2	<i>LED Control Nodes</i>	LS	As Required			
3	<i>LED Luminaires</i>	LS	200			
4	<i>Feeder Panels</i>	LS	As Required			
5	<i>Necessary brackets for pole, cabling and other accessories required to install and make functional complete Smart LED solution</i>	LS	As Required			
	<a href="#">Public Authenticated Free Wi-Fi Internet Access</a>					
6	<i>Access Point for hotspots</i>	Nos	50			
7	<i>Field Switch</i>	LS	As Required			



8	<i>Junction Box</i>	LS	As Required			
9	<i>Field UPS</i>	LS	As Required			
	<a href="#">Centralised software for Smart Street Lights</a>					
10	Centralized Software for Smart Street Lights (Including Mobile Apps)	LS	As Required			
	<a href="#">Public Address System</a>					
11	Public Announcement (PA) System	Nos	50			
	<a href="#">Emergency Call Box</a>					
12	Emergency Call Box	Nos	50			
<b>I</b>	<b>ICT Based Smart Solid Waste/Bin Management System</b>					
1	Fixed Cameras for SWM monitoring with Edge Intelligence	Nos	100			
2	Centralised monitoring of SWM Monitoring Software	LS	As Required			
3	Software Integration of Weighbridge for solidwaste management	Lot	4			
<b>J</b>	<b>Smart Parking System</b>					
1	Smart Parking Management software for integration	Lot	As Required			
<b>K</b>	<b>Laying &amp; commissioning of Fibre network for Internet cable Bandwidth</b>					
1	Consolidated Internet Bandwidth Connectivity DC/DR including DC-DR interconnectivity	Lot	As Required			
2	Redundant bandwidth connectivity from Field Smart devices -Gateway -DC/DR_Cloud - MPLS Network	Lot	As Required			
K	Additional Infrastructure / Services (if any)					
	Additional Infrastructure / Services if any....					

**7.10 Manufacturers'/Producers' Authorization Form**

*(This form has to be provided by the OEMs of the hardware and software solutions proposed. This letter of authority should be on the letterhead of the manufacturer and should be signed by a person competent and having the power of attorney to bind the manufacturer.)*

Date:

To,

[                    ],

Subject: Manufacturer's Authorization Form

Ref: RfP No. <<.....>> dated << .....>>

Dear Sir,

We \_\_\_\_\_ (Name of the OEM) who are established and reputable manufacturers of \_\_\_\_\_ (List of Goods) having factories or product development centers at the locations \_\_\_\_\_ or as per list attached, do hereby authorize. \_\_\_\_\_ (Name and address of the Bidder) to bid, negotiate and conclude the contract with you against RfP No. \_\_\_\_\_ Dated \_\_\_\_\_ for the above goods manufactured or developed by us.

We hereby extend, our warranty for the hardware goods supplied by the bidder and or maintenance or support services for software products against this invitation for bid by \_\_\_\_\_ (Name of the Bidder) as per requirements and for the duration of contract as specified in thisRfP.

We also confirm that our offered product is not be end of life and the support for such offered product(s) will be available for minimum of 6 years from the date of submission of bid.

Thanking you,

Yours faithfully,

(Signature)

For and on behalf of: \_\_\_\_\_ (Name of the OEM)

Authorised Signatory

Name:

Designation:

Place:

Date:

**7.11 Anti-Collusion Certificate**

*[Certificate should be provided by Lead Bidder and on letter head]*

**Anti-Collusion Certificate**

We hereby certify and confirm that in the preparation and submission of our Bid for **Request for Proposal for Selection of System Integrator for Implementation of for Design, Supply, Implement, Commission, Operate & Manage the Command & Control Centre for Chennai Smart City** against the RfP issued by GCC / CSCL, We have not acted in concert or in collusion with any other Bidder or other person(s) and also not done any act, deed or thing, which is or could be regarded as anti-competitive. We further confirm that we have not offered nor will offer any illegal gratification in cash or kind to any person or organization in connection with the instant bid.

(Signature of the Lead Bidder)

Printed Name

Designation

**Seal**

Date:

Place:

Business Address:

## 8 Annexure 4 – Formats for Submission of the Commercial Bid (will be given in online portal)

### General Instructions

1. Bidder should provide all prices as per the prescribed format as per the RfP. Bidder should not leave any field blank. In case the field is not applicable, Bidder must indicate "0" (Zero) in all such fields.
2. All the prices are to be entered in Indian Rupees ONLY
3. All unit rates indicated in the schedules shall be inclusive of all taxes, GST levies, duties etc. The prices should also be inclusive of all costs till end of the contract period.
4. GCC / CSCL, reserves the right to ask the Bidder to submit proof of payment against any of the GST/taxes, duties, levies indicated.
5. The Bidder needs to account for all Out of Pocket expenses due to Boarding, Lodging and other related items.
6. The Unit Rate as mentioned in the following formats shall be used for the purpose of 'Change Order' for respective items, if any. However, based on the market trends, GCC / CSCL, retains the right to negotiate this rate for future requirement
7. Bidder shall be bound to give same or more % discount on the list price on the future purchases by GCC / CSCL. SI shall ensure that the future products supplied are of latest specifications as per the OEM roadmap.
8. For the purpose of evaluation of Commercial Bids, the GCC / CSCL, shall make appropriate assumptions to arrive at a common bid price for all the Bidders. This however may not direct co-relation with the Contract value or actual payment to be made to the Bidder.
9. The detailed commercial bid as per given templates below shall be submitted in separate sealed covers. The summary of the commercial bid should be indicated in as per prescribed template in the online portal.
10. Detailed Price bid template are given in 8.1 is only for illustrative purpose.

**Design, Supply, Implement, Commission, Operate & Manage the Command & Control Centre**

**8.1 Section 1: CAPITAL EXPENDITURE (CAPEX (A))**

c	Particulars	Unit	Quantity	Unit Rate	Price	Tax Amount (GST/Duties/etc) on 4	Amount(Incl. Tax)
		1	2	3	4 = (2 x 3)	5	6 = (4 + 5)
A	Command & Communications Center (CCC)						
1	Interior & Civil works for CCC as per scope & functional specifications of Non-IT	Sqft	2050				
2	Video Wall Solution- 50" DLP Smart GRID in a 12x2 arrangement with passive component to scale upto total of 14x3 cube arrangement	Nos	24				
3	War Room : Additional LED Smart Displays 55" (Min. 4 nos)	Nos	As Required				
4	Monitoring Desktops / Laptops for Line Department users (min 30), Live video and Playback from field camera (min 3), Helpdesk Operators (min. 4 Nos.)	Nos	As Required				
5	Network Multifunctional Devices with Colour Laser Printing (min. 4 nos)	Nos	As Required				
6	IP based Video Phones (min 60nos., monitoring workstations and war room)	Nos	As Required				
7	Indoor Fixed Dome Cameras for internal surveillance (design Qty as per standards)	Nos	As Required				
8	Edge Network Switches (L3) to connect Workstations (on HA)	LS	As Required				
9	Network Rack (on High Availability mode)	Lot	As Required				
10	ICT Networking (Passive Components)	Lot	As Required				
11	Electrical Cabling & Necessary Illumination Devices	Lot	As Required				
12	Public Address System connected to Building Management System	Set	As Required				
13	1st Layer Access Control System (RFID Or virtual) to CCC & War Room	Set	As Required				
14	2nd Layer Access Control System (Biometric based) to CCC & War Room	Set	As Required				
15	Digital Display Unit (40") for CCC & War Room and LCD Projector, including sealing mounting kit and motorized screen - 113"	Nos	As Required				
16	HVAC Air conditioners to humidifiers to suite 24x7 operations at CCC	Lot	As				

**Design, Supply, Implement, Commission, Operate & Manage the Command & Control Centre**

c	Particulars	Unit	Quantity	Unit Rate	Price	Tax Amount (GST/Duties/etc) on 4	Amount(Incl. Tax)
			Required				
17	UPS with N+N configuration for critical load & Inverter for non-critical lighting load	Nos	As Required				
18	DG Sets (N + N Configuration)	Nos	As Required				
B	Smart Data Center Solution on cloud model						
1	DC Core Router	LS	As Required				
2	Internet Routers	LS	As Required				
3	DC Switches (Core, Application & rack)	LS	As Required				
4	Firewall (both Internal & External)	LS	As Required				
5	Intrusion Prevention System & Intrusion Detection System	LS	As Required				
6	Server load balancer	LS	As Required				
7	Enterprise Management System (with SLA Management HelpdeskManagement Network Management integrated BMS)	LS	As Required				
8	Anti-virus Software for Client & Servers	LS	As Required				
9	Backup & Archival Software	LS	As Required				
10	DC/DR cloud onsite monitoring workstation laptops for mgmt. staff	LS	As Required				
11	CCC's EPABX including two dedicated PRI lines at CCC premises	Nos	As Required				
12	CCC's centralised AAA Service, Wireless Controller for Wi-Fi based Services through Smart Pole	Nos	As Required				
13	CCC's Voice router for Help Desk Direct Voice calling, recording, Geo tagging & analysis at CCC premises	Nos	As Required				
14	Fire Proof Enclosure for Media offsite Storage at CCC premises	LS	As Required				
15	Servers on cloud model	LS	As Required				
16	Enterprise service Bus	LS	As Required				

**Design, Supply, Implement, Commission, Operate & Manage the Command & Control Centre**

c	Particulars	Unit	Quantity	Unit Rate	Price	Tax Amount (GST/Duties/etc) on 4	Amount(Incl. Tax)
17	Virtualisation software	LS	As Required				
18	RDBMS Licenses	LS	As Required				
19	Customisation/Integration of the existing systems of GCC / CSCL	LS	As Required				
20	Integration Services from various IOT, sensors, applications, social media, etc to CCC	LS	As Required				
21	IoT based analytics tool for Big Data Analytics & Dashboarding	LS	As Required				
22	Command and Communications Software (including Disaster Management)	LS	As Required				
23	Command & Communications Centre + Disaster Management Solution Implementation	LS	As Required				
24	Video Management Software licenses for different received from field cameras	Set	900				
25	GIS Map Engine, Integration of shape files on base map, crowdsourcing based data	Lot	As Required				
26	Viewing Software licenses for GIS services, Analytics, MIS, visualisations,	Lot	As Required				
27	Smart Governance Portal with customised dashboard, interfacing IOT, Social Media & other required integrations as per Scope of work defined	Lot	As Required				
C	Smart Sensors						
1	Environmental Sensors	Nos	18				
2	Rain-Gauge Sensors	Nos	30				
3	Flood Sensors	Nos	46				
4	Integration feeds on Fire alarm from various BMS systems of buildings to CCC	LS	As Required				
D	Variable Messaging Board						
1	3.8 X 1.9m Double side display VMS board including VMS controller as per specifications including mounting	Nos	17				
2	4.8 x 1.9m Double side display VMS board Including VMS controller as per specifications including mounting	Nos	33				
3	VMS Software licenses cost (bundled)	LS	As Required				
E	CCTV Surveillance & Disaster Management						
1	Outdoor Box Cameras (Surveillance)	Nos	400				
2	Outdoor PTZ Cameras	Nos	100				

**Design, Supply, Implement, Commission, Operate & Manage the Command & Control Centre**

c	Particulars	Unit	Quantity	Unit Rate	Price	Tax Amount (GST/Duties/etc) on 4	Amount(Incl. Tax)
3	Poles for Cameras and equipment	LS	As Required				
4	Provisioning of Electrical Power	LS	As Required				
5	Industrial Grade Outdoor PoE Switches 16 Ports	LS	As Required				
6	Networking Cost (Passive Component : Junction Box, Patch Panel, LIU, OFC, Cat6 Cable, Patch Cords, Earthing, Lighting arrester)	LS	As Required				
7	UPS ( Solar + Electric) with Batteries	LS	As Required				
8	Digging, Piping & Re-filling, including digging for electrical cabling	LS	As Required				
9	Flood Monitoring Cameras Fixed Cameras with Edge Analytics	Lot	68				
F	Mobile Command & Control Center						
1	Pre-fabricated Vans	Nos	1				
2	Interoperable Communication Server with Software License	LS	As Required				
3	Desktop with Touch Panel Display	LS	As Required				
4	Outdoor PTZ Camera with mounting accessories	LS	As Required				
5	Outdoor Fixed Box Cameras with mounting accessories	LS	As Required				
6	Min. 64 GB SD card	LS	As Required				
7	Full HD Handycam (meeting all the basic parameters of Fix Box Camera) with wireless capability	LS	As Required				
8	Local server Storage for 7 days	LS	As Required				
9	Cost for fixtures and camera mounting charges Wireless Connectivity	LS	As Required				
10	Switch, Router, modem	LS	As Required				
11	LAN , GSM Modems , VSAT Setup for the Van, with capability to create a Wi-Fi / WiMAX network	LS	As Required				
12	GPRS SIM Module	LS	As Required				
13	GPS equipment with mobile terminal	LS	As				



**Design, Supply, Implement, Commission, Operate & Manage the Command & Control Centre**

c	Particulars	Unit	Quantity	Unit Rate	Price	Tax Amount (GST/Duties/etc) on 4	Amount(Incl. Tax)
			Required				
14	Public Address System	LS	As Required				
15	Petrol Generator to support Mobile CCC	LS	As Required				
16	UPS backup for 1 hour	LS	As Required				
17	Fire Extinguisher	LS	As Required				
G	Training and Overall Project Management						
	<i>Training Costs (per batch of 20)</i>						
1	Functional Training (batch of 20 trainees per batch)	LS	200				
2	Administrative Training batches	LS	10				
3	Sr. Management Training Batches	LS	10				
4	Project Management/Coordination during implementation	LS	12				
5	Security Audit Charges	LS	As Required				
6	Operational Expenses during implementation	LS	As Required				
H	Smart Poles						
	<a href="#">Smart Poles</a>						
1	<i>Smart Poles 16 mtrs</i>	LS	50				
	<a href="#">Smart Street Light</a>						
2	<i>LED Control Nodes</i>	LS	As Required				
3	<i>LED Luminaires</i>	LS	200				
4	<i>Feeder Panels</i>	LS	As Required				
5	<i>Necessary brackets for pole, cabling and other accessories required to install and make functional complete Smart LED solution</i>	LS	As Required				
	<a href="#">Public Authenticated Free Wi-Fi Internet Access</a>						
6	<i>Access Point for hotspots</i>	Nos	50				
7	<i>Field Switch</i>	LS	As Required				
8	<i>Junction Box</i>	LS	As Required				
9	<i>Field UPS</i>	LS	As				

**Design, Supply, Implement, Commission, Operate & Manage the Command & Control Centre**

c	Particulars	Unit	Quantity	Unit Rate	Price	Tax Amount (GST/Duties/etc) on 4	Amount(Incl. Tax)
			Required				
	<a href="#">Centralised software for Smart Street Lights</a>						
10	Centralized Software for Smart Street Lights (Including Mobile Apps)	LS	As Required				
	<a href="#">Public Address System</a>						
11	Public Announcement (PA) System	Nos	50				
	<a href="#">Emergency Call Box</a>						
12	Emergency Call Box	Nos	50				
I	ICT Based Smart Solid Waste/Bin Management System						
1	Fixed Cameras for SWM monitoring with Edge Intelligence	Nos	100				
2	Centralised monitoring of SWM Monitoring Software	LS	As Required				
3	Software Integration of Weighbridge for solidwaste management	Lot	4				
J	Smart Parking System						
1	Smart Parking Management software for integration	Lot	As Required				
K	Laying & commissioning of Fibre network for Internet cable Bandwidth						
1	Consolidated Internet Bandwidth Connectivity DC/DR including DC-DR interconnectivity	Lot	As Required				
2	Redundant bandwidth connectivity from Field Smart devices -Gateway - DC/DR_Cloud - MPLS Network	Lot	As Required				
K	Additional Infrastructure / Services (if any)						
	Additional Infrastructure / Services if any....						
	Sub-Total Section 1 : CAPEX (A)						

**Design, Supply, Implement, Commission, Operate & Manage the Command & Control Centre**

**8.2 Section 1: OPERATIONAL EXPENDITURE (OPEX (B))**

#	Particulars	Year_1	Year_2	Year_3	Year_4	Year_5	Amount for 5 years	Applicable Tax Amount on "6"	Amount for 5 years with Tax
		1	2	3	4	5	6 = sum(1,2,3,4,5)	7	8 = (6 + 7)
A	Command & Communications Center (CCC)								
B	Smart Data Center (DC) Infrastructure (On cloud hosted model)								
C	Smart Environmental Sensors								
D	Variable Messaging Board, Public Announcement (PA) and Emergency Call Box								
E	CCTV Surveillance								
F	Mobile Command & Control Center								
G	Re-Training and Overall Project Management during O&M period								
H	Smart Poles								
I	ICT Based Smart Solid Waste/Bin Management System								
J	Smart Parking System								
K	Annual Recurring Charge for consolidated Internet Bandwidth and Cloud								
L	Facility Management, Technical & Operational support by Technical/ Operational /Support personnel of SI								
M	Additional Infrastructure / Services (if any)								
	<b>Sub Total Section 1 : OPEX (B)</b>								

8.3 Section 1: Sub-Total

#	Particulars	Total Amount with Taxes
1	Sub Total Section I –CAPEX (A)	
2	Sub Total Section I –OPEX (B)	
	<b>Sub-Total Section-1 (Total Project Cost) T</b>	
	<b>CAPEX : OPEX Ratio [ capped to 50% i.e. is { (A / T) x 100} ]</b>	

**Note :**

- The above table total cost summaries the actual project cost & contract value for the bidder. The payments to the successful bidder would be made as per this value only.
- The bidders shall ensure that the CAPE:OPEX ratio does not exceed 50%. The CAPEX:OPEX ratio is calculated by dividing the CAPEX by Total project Cost in above table.

**Design, Supply, Implement, Commission, Operate & Manage the Command & Control Centre**

**8.4 Section 2: Unit Price for Upgradation – CAPEX (C)**

#	Particulars	Unit	Quantity	Unit Rate	Price	Tax Amount (GST/Duties/etc) on 4	Amount(Incl. Tax)
		1	2	3	4 = (2 x 3)	5	6 = (4 + 5)
A	Command & Communications Center (CCC)						
1	Interior & Civil works for CCC as per scope & functional specifications of Non-IT	Sqft	100				
2	Video Wall Solution- 50" DLP Smart GRID in a 12x2 cubes	Nos	24				
3	Smart LED 55" TVs	Nos	10				
4	Monitoring Desktops / Laptops	Nos	15				
5	Network Multifunctional Devices with Colour Laser Printing	Nos	5				
6	IP based Video Phones	Nos	10				
7	Indoor Fixed Dome Cameras for internal surveillance	Nos	10				
8	Edge Network Switches (L3) to connect Workstations (on HA)	Nos	10				
9	Network Rack (on High Availability mode)	Nos	10				
10	ICT Networking (Passive Components) for connecting 10 compute devices	LS	1				
11	Electrical Cabling & Necessary Illumination Devices for connecting 10 compute devices	LS	1				
12	Public Address System connected to Building Management System	Nos	10				
13	1st Layer Access Control System (RFID Or virtual) to CCC & War Room	Nos	50				
14	2nd Layer Access Control System (Biometric based) to CCC & War Room	Set	50				
B	Smart Data Center Solution on cloud model						
1	VM License	Nos	10				
2	1 TB Storage Space	Nos	10				
8	Anti-virus Software for Client licenses	Nos	10				
9	Backup Software Licenses	Nos	10				
10	Archival Software Licenses	Nos	10				
11	EPABX additional dedicated PRI lines at CCC premises	Nos	1				
12	CCC's centralised AAA Service, Wireless Controller for Wi-Fi based Services through Smart Pole	Nos	2				
13	CCC's Voice router for Help Desk Direct Voice calling, recording, Geo tagging & analysis at CCC premises	Nos	2				
14	Fire Proof Enclosure for Media offsite Storage at CCC premises	Nos	10				
15	Servers on cloud model	Nos	10				
18	RDBMS Additional Enterprise Licenses (Same RDBMS in CCC)	Nos	10				

**Design, Supply, Implement, Commission, Operate & Manage the Command & Control Centre**

#	Particulars	Unit	Quantity	Unit Rate	Price	Tax Amount (GST/Duties/etc) on 4	Amount(Inlc. Tax)
		1	2	3	4 = (2 x 3)	5	6 = (4 + 5)
19	Customisation/Integration of the existing systems of GCC / CSCL	Nos	10				
20	Integration Services from various Additional devises such IOT, sensors, applications, social media, etc to CCC (applicable only for device quantities over and above those factored in CAPEX under this project)	LS	As Required				
24	Video Management Software licenses for different received from field cameras	Nos	10				
26	Additional GIS Software licenses for 4 core process	Nos	1				
27	Person-Month cost customisation of Smart Governance Portal	Person-Month	10				
C	Smart Sensors						
1	Environmental Sensors	Nos	10				
2	Rain-Gauge Sensors	Nos	10				
3	Flood Sensors	Nos	10				
D	Variable Messaging Board						
1	3.8 X 1.9m Double side display VMS board including VMS controller as per specifications including mounting + bundled VMS software liceses	Nos	10				
2	4.8 x 1.9m Double side display VMS board Including VMS controller as per specifications including mounting + bundled VMS software liceses	Nos	10				
E	CCTV Surveillance & Disaster Management						
1	Outdoor Box Cameras (Surveillance)	Nos	100				
2	Outdoor PTZ Cameras	Nos	50				
3	Poles for Cameras and Equipments	LS	10				
4	Provisioning of Electrical Power	LS	10				
5	Industrial Grade Outdoor PoE Switches 16 Ports	LS	10				
6	Networking Cost (Passive Component : Junction Box, Patch Panel, LIU, OFC, Cat6 Cable, Patch Cords, Earthing, Lighting arrester)	LS	10				
7	UPS ( Solar + Electric) with Batteries	LS	10				
8	Digging, Piping & Re-filling, including digging for electrical cabling	LS	10				
9	Flood Monitoring Cameras Fixed Camers with Edge Analytics	Lot	10				
F	Mobile Command & Control Center						
1	Pre-fabricated Vans	Nos	1				
2	Interoperable Communication Server with Software License	Nos	1				
3	Desktop with Touch Panel Display	Nos	1				
4	Outdoor PTZ Camera with mounting accessories	Nos	1				

**Design, Supply, Implement, Commission, Operate & Manage the Command & Control Centre**

#	Particulars	Unit	Quantity	Unit Rate	Price	Tax Amount (GST/Duties/etc) on 4	Amount(Incl. Tax)
		1	2	3	4 = (2 x 3)	5	6 = (4 + 5)
5	Outdoor Fixed Box Cameras with mounting accessories	Nos	1				
7	Full HD Handycam (meeting all the basic parameters of Fix Box Camera) with wireless capability	Nos	1				
8	Local server Storage for 7 days	LS	1				
10	Switch, Router, modem	LS	1				
11	LAN , GSM Modems , VSAT Setup for the Van, with capability to create a Wi-Fi / WiMAX network	LS	1				
12	GPRS SIM Module	LS	1				
13	GPS Equipments with mobile terminal	LS	1				
14	Public Address System	Nos	10				
15	Petrol Generator to support Mobile CCC	LS	1				
16	UPS backup for 1 hour	Nos	1				
17	Fire Extinguisher	Nos	10				
G	Training and Overall Project Management						
	<i>Not applicable</i>						
H	Smart Poles						
	<a href="#">Smart Poles</a>						
1	<i>Smart Poles 16 mtrs</i>	LS	10				
	<a href="#">Smart Street Light</a>						
2	<i>LED Control Nodes</i>	LS	10				
3	<i>LED Luminaires</i>	LS	40				
4	<i>Feeder Panels</i>	LS	10				
5	<i>Necessary brackets for pole, cabling and other accessories required to install and make functional complete Smart LED solution - for single pole</i>	LS	10				
	<a href="#">Public Authenticated Free Wi-Fi Internet Access</a>						
6	<i>Access Point for hotspots</i>	Nos	10				
	<a href="#">Centralised software for Smart Street Lights</a>						
10	Centralized Software for Smart Street Lights (Including Mobile Apps)	LS	10				
	<a href="#">Public Address System</a>						
11	Public Announcement (PA) System	Nos	10				
	<a href="#">Emergency Call Box</a>						
12	Emergency Call Box	Nos	10				
I	ICT Based Smart Solid Waste/Bin Management System						

**Design, Supply, Implement, Commission, Operate & Manage the Command & Control Centre**

#	Particulars	Unit	Quantity	Unit Rate	Price	Tax Amount (GST/Duties/etc) on 4	Amount(Inlc. Tax)
		1	2	3	4 = (2 x 3)	5	6 = (4 + 5)
1	Fixed Cameras for SWM monitoring with Edge Intelligence	Nos	10				
2	additional Centralised monitoring of SWM Monitoring Software	LS	10				
J	Laying & commissioning of Fibre network for Internet cable Bandwidth						
1	per 100 GB Consolidated Internet Bandwidth Connectivity DC/DR including DC-DR interconnectivity	LS	1				
1	per 500 GB Consolidated Internet Bandwidth Connectivity DC/DR including DC-DR interconnectivity	LS	1				
2	per 750 GB Consolidated Internet Bandwidth Connectivity DC/DR including DC-DR interconnectivity	LS	1				
Sub-Total Section 2 CAPEX ( C )							

**Note:**

- The quantities mentioned here are for evaluation purpose only. The deployment will be actual need basis and same shall be decided by GCC / CSCL.
- The amount quoted above shall be valid till the end of contract period of the SI in this bid.



**Design, Supply, Implement, Commission, Operate & Manage the Command & Control Centre**

**8.5 Section 2: Unit Price for Upgradation – OPEX (D)**

#	Particulars	Per Unit Per Annum Amount	Applicable Tax Amount on "1"	Per Annum Amount with Tax
		1	2	3 = (1 + 2)
<b>A</b>	<b>Command &amp; Communications Center (CCC)</b>			
1	Video Wall Solution- 50" DLP Smart GRID in a 12x2 cubes			
2	Smart LED 55" TVs			
3	Monitoring Desktops / Laptops			
4	Network Multifunctional Devices with Colour Laser Printing			
5	IP based Video Phones			
6	Indoor Fixed Dome Cameras for internal surveillance			
7	Edge Network Switches (L3) to connect Workstations (on HA)			
8	Public Address System connected to Building Management System			
9	1st Layer Access Control System (RFID Or virtual) to CCC & War Room			
10	2nd Layer Access Control System (Biometric based) to CCC & War Room			
<b>B</b>	<b>Smart Data Center Solution on cloud model</b>			
1	CCC's centralised AAA Service, Wireless Controller for Wi-Fi based Services through Smart Pole			
2	CCC's Voice router for Help Desk Direct Voice calling, recording, Geo tagging & analysis at CCC premises			
3	Servers on cloud model			
4	RDBMS Additional Enterprise Licenses (Same RDBMS in CCC)			
<b>C</b>	<b>Smart Sensors</b>			
1	Environmental Sensors			
2	Rain-Gauge Sensors			
3	Flood Sensors			
<b>D</b>	<b>Variable Messaging Board</b>			
1	3.8 X 1.9m VMS board including VMS controller as per specifications including mounting + bundled VMS software licenses			
2	4.8 x 1.9m VMS board Including VMS controller as per specifications including mounting + bundled VMS software licenses			
<b>E</b>	<b>CCTV Surveillance &amp; Disaster Management</b>			
1	Outdoor Box Cameras (Surveillance)			
2	Outdoor PTZ Cameras			
3	Poles for Cameras and Equipment's			

**Design, Supply, Implement, Commission, Operate & Manage the Command & Control Centre**

#	Particulars	Per Unit Per Annum Amount	Applicable Tax Amount on "1"	Per Annum Amount with Tax
9	Flood Monitoring Cameras Fixed Cameras with Edge Analytics			
F	Mobile Command & Control Center			
1	Mobile CCC Van			
H	Smart Poles			
	<a href="#">Smart Poles</a>			
I	ICT Based Smart Solid Waste/Bin Management System			
1	Fixed Cameras for SWM monitoring with Edge Intelligence			
J	Laying & commissioning of Fibre network for Internet cable Bandwidth			
1	Annual Recurring Cost per 100 GB Consolidated Internet Bandwidth Connectivity			
1	Annual Recurring Cost per 500 GB Consolidated Internet Bandwidth Connectivity			
2	Annual Recurring Cost per 750 GB Consolidated Internet Bandwidth Connectivity			
	Sub-Total Section 2 : OPEX (D)			

**Note:**

- unit rate for Annual OPEX cost for upgraded items discovered above. The OPEX cost shall be paid from the date completion of commissioning (i.e. Go-Live of that respective component). In case the commissioning is not happening during the year then annual OPEX cost can be prorated proportional to actual residual months in the contract period and payment can be made along with ongoing periodic O&M payment.
- The amount quoted above shall be valid till the end of contract period of the SI.

8.6 Section 2: Sub-Total

#	Particulars	Total Amount with Taxes
1	Sub Total Section 2 - CAPEX (C)	
2	Sub Total Section 2 - OPEX (D)	
	<b>Sub-Total Section-2</b>	

**8.7 Section 3: Value of Price Bid**

#	Particulars	Total Amount with Taxes
1	Sub Total Section – 1 CAPEX (A)	
2	Sub Total Section – 1 OPEX (B)	
3	Sub Total Section – 2 CAPEX (C)	
4	Sub Total Section – 2OPEX (D)	
	<b>Grand Total - Value of Price Bid (A + B + C + D)</b>	

**Note :**

- The Price quoted should be inclusive of all expenses (including all incidental, travel, etc.) and inclusive of all taxes.
- Incase of any revision of statutory taxes the difference in Contract Amount would be modified as per prevailing tax structure. The same shall be made effect from applicable date given by the GCC / CSCL, during the contract period.
- This total cost “Value of Price Bid” would be considered for Evaluation of Bid for this RfP
- The bidders shall ensure that the CAPE:OPEX ratio does not exceed 50% i.e. ratio of [ Section 1 { CAPEX } :{ Sub-Total Section-1 (Total Project Cost) T} shall not be more than 50%.

## 9 Annexure 5 (a) – Performance Bank Guarantee

Ref: \_\_\_\_\_

Date \_\_\_\_\_

Bank Guarantee No. \_\_\_\_\_

<Name>  
<Designation>  
<Address><Phone  
Nos.><Fax  
Nos.><Email id>

Whereas, <<name of the supplier and address>> (hereinafter called “the System Integrator”) has undertaken, in pursuance of contract no. <Insert Contract No.> dated. <Date> to provide Implementation services for <<name of the assignment>> to Greater Chennai Corporation/Chennai Smart City Limited(hereinafter called “the GCC / CSCL”)

And whereas it has been stipulated by in the said contract that the bidder shall furnish you with a bank guarantee by a recognized bank for the sum specified therein as security for compliance with its obligations in accordance with the contract;

And whereas we, <Name of Bank> a banking company incorporated and having its head/registered office at <Address of Registered Office> and having one of its office at <Address of Local Office> have agreed to give the supplier such a bank guarantee.

Now, therefore, we hereby affirm that we are guarantors and responsible to you, on behalf of the supplier, up to a total of Indian Rupees<Insert Value> (Rupees <Insert Value in Words> only) and we undertake to pay you, upon your first written demand declaring the supplier to be in default under the contract and without cavil or argument, any sum or sums within the limits of Indian Rupees<Insert Value> (Rupees <Insert Value in Words> only) as aforesaid, without your needing to prove or to show grounds or reasons for your demand or the sum specified therein.

We hereby waive the necessity of your demanding the said debt from the bidder before presenting us with the demand.

We further agree that no change or addition to or other modification of the terms of the contract to be performed there under or of any of the contract documents which may be made between you and the System Integrator shall in any way release us from any liability under this guarantee and we hereby waive notice of any such change, addition or modification.

This Guarantee shall be valid until <<Insert Date>>)

Notwithstanding anything contained herein:

I. Our liability under this bank guarantee shall not exceed Indian Rupees<Insert Value> (Rupees <Insert Value in Words> only).

II. This bank guarantee shall be valid up to <Insert Expiry Date>)

III. It is condition of our liability for payment of the guaranteed amount or any part thereof arising under this bank guarantee that we receive a valid written claim or demand for

payment under this bank guarantee on or before <Insert Expiry Date>) failing which our liability under the guarantee will automatically cease.

Date \_\_\_\_\_

Place \_\_\_\_\_

Signature \_\_\_\_\_

Witness

\_\_\_\_\_

Printed name \_\_\_\_\_

**(Bank's common seal)**

## 10 Annexure 5 (b) – Bank Guarantee for Earnest Money Deposit

To,

<Name>

<Designation>

<Address>

<Phone Nos.>

<Fax Nos.>

<Email id>

Whereas <<Name of the bidder>> (hereinafter called 'the System Integrator') has submitted the bid for Submission of RfP<<RfP Number>> dated <<Date>> for <<Name of the assignment>> (hereinafter called "the Bid") to <<GCC / CSCL>>.

Know all Men by these presents that we <<... >> having our office at <<Address>> (hereinafter called "the Bank") are bound unto the <<GCC / CSCL>> (hereinafter called "the GCC / CSCL") in the sum of Indian Rupees<<Amount in figures>> (Rupees <<Amount in words>> only) for which payment well and truly to be made to the said GCC / CSCL, the Bank binds itself, its successors and assigns by these presents. Sealed with the Common Seal of the said Bank this <<Date>>.

The conditions of this obligation are:

1. If the Bidder having its bid withdrawn during the period of bid validity specified by the Bidder on the Bid Form; or
2. If the Bidder, having been notified of the acceptance of its bid by the GCC / CSCL during the period of validity of bid

- (a) Withdraws his participation from the bid during the period of validity of bid document; or
- (b) Fails or refuses to participate in the subsequent Tender process after having been short listed;

We undertake to pay to the GCC / CSCL up to the above amount upon receipt of its first written demand, without the GCC / CSCL having to substantiate its demand, provided that in its demand the GCC / CSCL will note that the amount claimed by it is due to it owing to the occurrence of one or both of the two conditions, specifying the occurred condition or conditions.

This guarantee will remain in force up to <<insert date>> and including <<extra time over and above mandated in the RfP>> from the last date of submission and any demand in respect thereof should reach the Bank not later than the above date.

NOTWITHSTANDING ANYTHING CONTAINED HEREIN:

- I. Our liability under this Bank Guarantee shall not exceed Indian Rupees<<Amount in figures>> (Rupees <<Amount in words>> only)
- II. This Bank Guarantee shall be valid up to <<insert date>>)
- III. It is condition of our liability for payment of the guaranteed amount or any part thereof arising under this Bank Guarantee that we receive a valid written claim or demand for payment under

this Bank Guarantee on or before <<insert date>>) failing which our liability under the guarantee will automatically cease.

(Authorized Signatory of the Bank)

Seal:

Date:



## 11 Annexure 6 – Non-Disclosure Agreement

WHEREAS, we the undersigned Bidder, \_\_\_\_\_, having our principal place of business or registered office at \_\_\_\_\_, are desirous of bidding for RfP No. <<>> dated <<DD-MM-2015>> **“Request for Proposal for Selection of System Integrator for Implementation of for Design, Supply, Implement, Commission, Operate & Manage the Command & Control Centre for Chennai Smart City”** (hereinafter called the said 'RfP') to the “Greater Chennai corporation /Chennai Smart City Limited”, hereinafter referred to as 'GCC / CSCL'

And,

WHEREAS, the Bidder is aware and confirms that the GCC / CSCL's business or operations, information, application or software, hardware, business data, architecture schematics, designs, storage media and other information or documents made available by the GCC / CSCL in the RfP documents during the bidding process and thereafter, or otherwise (confidential information for short) is privileged and strictly confidential and or proprietary to the GCC / CSCL,

NOW THEREFORE, in consideration of disclosure of confidential information, and in order to ensure the GCC / CSCL's grant to the Bidder of specific access to GCC / CSCL's confidential information, property, information systems, network, databases and other data, the Bidder agrees to all of the following conditions.

It is hereby agreed as under:

1. The confidential information to be disclosed by the GCC / CSCL under this Agreement (“Confidential Information”) shall include without limitation, any and all information in written, representational, electronic, verbal or other form relating directly or indirectly to processes, methodologies, algorithms, risk matrices, thresholds, parameters, reports, deliverables, work products, specifications, architecture, project information, security or zoning strategies & policies, related computer programs, systems, trend analysis, risk plans, strategies and information communicated or obtained through meetings, documents, correspondence or inspection of tangible items, facilities or inspection at any site to which access is permitted by the GCC / CSCL.
2. Confidential Information does not include information which:
  - a. the Bidder knew or had in its possession, prior to disclosure, without limitation on its confidentiality;
  - b. information in the public domain as a matter of law;
  - c. is obtained by the Bidder from a third party without any obligation of confidentiality;
  - d. the Bidder is required to disclose by order of a competent court or regulatory authority;
  - e. Is released from confidentiality with the written consent of the GCC / CSCL.

The Bidder shall have the burden of proving hereinabove are applicable to the information in the possession of the Bidder.

3. The Bidder agrees to hold in trust any Confidential Information received by the Bidder, as part of the Tendering process or otherwise, and the Bidder shall maintain strict confidentiality in respect of such Confidential Information, and in no event a degree of confidentiality less than the Bidder uses to protect its own confidential and proprietary information. The Bidder also agrees:
  - a. to maintain and use the Confidential Information only for the purposes of bidding for this RfP and thereafter only as expressly permitted herein;
  - b. to only make copies as specifically authorized by the prior written consent of the GCC / CSCL and with the same confidential or proprietary notices as may be printed or displayed on the original;
  - c. to restrict access and disclosure of Confidential Information to their employees, agents, consortium members and representatives strictly on a "need to know" basis, to maintain confidentiality of the Confidential Information disclosed to them in accordance with this clause; and
  - d. To treat Confidential Information as confidential unless and until GCC / CSCL expressly notifies the Bidder of release of its obligations in relation to the said Confidential Information.
  
4. Notwithstanding the foregoing, the Bidder acknowledges that the nature of activities to be performed as part of the Tendering process or thereafter may require the Bidder's personnel to be present on premises of the GCC / CSCL or may require the Bidder's personnel to have access to software, hardware, computer networks, databases, documents and storage media of the GCC / CSCL while on or off premises of the GCC / CSCL. It is understood that it would be impractical for the GCC / CSCL to monitor all information made available to the Bidder's personnel under such circumstances and to provide notice to the Bidder of the confidentiality of all such information.

Therefore, the Bidder shall disclose or allow access to the Confidential Information only to those personnel of the Bidder who need to know it for the proper performance of their duties in relation to this project, and then only to the extent reasonably necessary. The Bidder will take appropriate steps to ensure that all personnel to whom access to the Confidential Information is given are aware of the Bidder's confidentiality obligation. Further, the Bidder shall procure that all personnel of the Bidder are bound by confidentiality obligation in relation to all proprietary and Confidential Information received by them which is no less onerous than the confidentiality obligation under this agreement.

5. The Bidder shall establish and maintain appropriate security measures to provide for the safe custody of the Confidential Information and to prevent unauthorized access to it.
  
6. The Bidder agrees that upon termination or expiry of this Agreement or at any time during its currency, at the request of the GCC / CSCL, the Bidder shall promptly deliver to the GCC / CSCL the Confidential Information and copies thereof in its possession or under its direct or indirect control, and shall destroy all memoranda, notes and other writings prepared by the Bidder or its Affiliates or directors, officers, employees or advisors based on the Confidential Information and promptly certify such destruction.

7. Confidential Information shall at all times remain the sole and exclusive property of the GCC / CSCL. Upon completion of the Tendering process and or termination of the contract or at any time during its currency, at the request of the GCC / CSCL, the Bidder shall promptly deliver to the GCC / CSCL the Confidential Information and copies thereof in its possession or under its direct or indirect control, and shall destroy all memoranda, notes and other writings prepared by the Bidder or its Affiliates or directors, officers, employees or advisors based on the Confidential Information within a period of sixty days from the date of receipt of notice, or destroyed, if incapable of return. The destruction shall be witnessed and so recorded, in writing, by an authorized representative of the GCC / CSCL. Without prejudice to the above the Bidder shall promptly certify to the GCC / CSCL, due and complete destruction and return. Nothing contained herein shall in any manner impair rights of the GCC / CSCL in respect of the Confidential Information.
  
8. In the event that the Bidder hereto becomes legally compelled to disclose any Confidential Information, the Bidder shall give sufficient notice and render best effort assistance to the GCC / CSCL to enable the GCC / CSCL to prevent or minimize to the extent possible, such disclosure. Bidder shall not disclose to a third party any Confidential Information or the contents of this RfP without the prior written consent of the GCC / CSCL. The obligations of this Clause shall be satisfied by handling Confidential Information with the same degree of care, which the Bidder applies to its own similar Confidential Information but in no event less than reasonable care.

**For and on behalf of:**

(BIDDER)

Authorised Signatory  
Name:  
Designation:

Office Seal:  
Place:  
Date :

## 12 Annexure 7 - Consortium Agreement

### DRAFT MEMORANDUM OF UNDERSTANDING EXECUTED BY MEMBERS OF THE CONSORTIUM

*[On Non-judicial stamp paper of Indian Rupees 100 duly attested by notary public]*

This Memorandum of Understanding (MoU) entered into this day of [Date] [Month] 2015 at [Place] among \_\_\_\_\_ (hereinafter referred to as "\_\_\_\_\_") and having office at [Address], India, as Party of the First Part and \_\_\_\_\_ (hereinafter referred as "\_\_\_\_\_") and having office at [Address], as Party of the Second Part and \_\_\_\_\_ (hereinafter referred as "\_\_\_\_\_") and having office at [Address], as Party of the Third Part.

The parties are individually referred to as Party and collectively as Parties.

WHEREAS Chennai Smart City Limited has issued a Request for Proposal dated [Date] (RfP) from the Applicants interested in **Request for Proposal for Selection of System Integrator for Implementation of for Design, Supply, Implement, Commission, Operate & Manage the Command & Control Centre for Chennai Smart City:**

AND WHEREAS the Parties have had discussions for formation of a Consortium for bidding for the said Project and have reached an understanding on the following points with respect to the Parties' rights and obligations towards each other and their working relationship.

AS MUTUAL UNDERSTANDING OF THE PARTIES, IT IS HEREBY AGREED AND DECLARED AS FOLLOWS:

i. The purpose of this Agreement is to define the principles of collaboration among the Parties to:

Submit a response jointly to Bid for the **"Request for Proposal for Selection of System Integrator for Implementation of for Design, Supply, Implement, Commission, Operate & Manage the Command & Control Centre for Chennai Smart City"** as a Consortium.

- a. Sign Contract in case of award.
- b. Provide and perform the supplies and services which would be ordered by the GCC / CSCL pursuant to the Contract.

ii. This Agreement shall not be construed as establishing or giving effect to any legal entity such as, but not limited to, a company, a partnership, etc. It shall relate solely towards the GCC / CSCL for **"Request for Proposal for Selection of System Integrator for Implementation of for Design, Supply, Implement, Commission, Operate & Manage the Command & Control Centre for Chennai Smart City"** for and related execution works to be performed pursuant to the Contract and shall not extend to any other activities.

iii. The Parties shall be jointly and severally responsible and bound towards the GCC / CSCL for the performance of the works in accordance with the terms and conditions of the BID document, and Contract.

- iv. ----- (Name of Party) shall act as Lead Partner of the Consortium .  
As such, it shall act as the coordinator of the Party's combined activities and shall carry out the following functions:
  - a. To ensure the technical, commercial and administrative co-ordination of the work package
  - b. To lead the contract negotiations of the work package with the GCC / CSCL.
  - c. The Lead partner is authorized to receive instructions and incur liabilities for and on behalf of all Parties.
  - d. In case of an award, act as channel of communication between the GCC / CSCL and the Parties to execute the Contract
  
- v. That the Parties shall carry out all responsibilities as Developer in terms of the Project Agreement.
  
- vi. That the broad roles and the responsibilities of each Party at each stage of the Bidding shall be as below:  
  
Lead Bidder: \_\_\_\_\_  
  
First Consortium Member: \_\_\_\_\_  
  
Second Consortium Member: \_\_\_\_\_
  
- vii. That the Parties affirm that they shall implement the Project in good faith and shall take all necessary steps to see the Project through expeditiously.
  
- viii. That this MoU shall be governed in accordance with the laws of India and courts in Tamil Nadushall have exclusive jurisdiction to adjudicate disputes arising from the terms herein.

In witness whereof the Parties affirm that the information provided is accurate and true and have caused this MoU duly executed on the date and year above mentioned.

(Lead bidder) ( First Consortium Member)(Second Consortium Member)

Witness:

- i. \_\_\_\_\_
- ii. \_\_\_\_\_

**13 Annexure 8 - Format for Power of Attorney to Authorize Signatory**

POWER OF ATTORNEY

*[To be executed on non-judicial stamp paper of the appropriate value in accordance with relevant Stamp Act. The stamp paper to be in the name of the company who is issuing the power of attorney.]*

We, M/s. \_\_\_\_\_ (name of the firm or company with address of the registered office) hereby constitute, appoint and authorise Mr. or Ms. \_\_\_\_\_ (Name and residential address) who is presently employed with us and holding the position of \_\_\_\_\_, as our Attorney to do in our name and our behalf all or any of the acts, deeds or things necessary or incidental to our RfP for the Project \_\_\_\_\_ (name of the Project), including signing and submission of the RfP response, participating in the meetings, responding to queries, submission of information or documents and generally to represent us in all the dealings with Client or any other Government Agency or any person, in connection with the works until culmination of the process of bidding till the Project Agreement is entered into with \_\_\_\_\_ (Client) and thereafter till the expiry of the Project Agreement.

We hereby agree to ratify all acts, deeds and things lawfully done by our said Attorney pursuant to this power of attorney and that all acts, deeds and things done by our aforesaid Attorney shall and shall always be deemed to have been done by us.

(Add in the case of a Consortium)

Our firm is a Member or Lead bidder of the Consortium of \_\_\_\_\_, \_\_\_\_\_ and \_\_\_\_\_.

Dated this the \_\_\_\_\_ day of \_\_\_\_\_ 2015

(Signature and Name of authorized signatory)

\_\_\_\_\_

(Signature and Name in block letters of all the remaining partners of the firm Signatory for the Company)

Seal of firm Company

Witness 1:

Witness 2:

*Notes:*

- a. To be executed by all the members individually.*
- b. The Mode of execution of the power of attorney should be in accordance with the procedure, if any laid down by the applicable law and the charter documents of the executant(s) and when it is so required the same should be under common seal affixed in accordance with the required procedure.*

**14 Annexure 9 - Format for Power of Attorney for Lead bidder of Consortium**

*[To be executed on non-judicial stamp paper of the appropriate value in accordance with relevant Stamp Act. The stamp paper to be in the name of the company who is issuing the power of attorney]*

Whereas \_\_\_\_\_ has invited RfP response for \_\_\_\_\_ (Name of the Project)

Whereas, the Members of the Consortium comprising of M/s.\_\_\_\_\_, M/s.\_\_\_\_\_, M/s.\_\_\_\_\_ and M/s.\_\_\_\_\_ (the respective names and addresses of the registered offices to be given) are interested in bidding for the Project and implementing the same in accordance with the terms and conditions contained in the RfP Documents.

Whereas, it is necessary for the members of the Consortium to designate one of them as the lead member with all necessary power and authority to do, for and on behalf of the Consortium/Joint Venture, all acts, deeds and things as may be necessary in connection with the Consortium's/Joint Venture's RfP response for the Project.

NOW THIS POWER OF ATTORNEY WITNESSETH THAT

We, M/s.\_\_\_\_\_ and M/s \_\_\_\_\_ and M/s\_\_\_\_\_ hereby designate M/s. \_\_\_\_\_ being one of the members of the Consortium/Joint Venture, as the lead member of the Consortium/Joint Venture, to do on behalf of the Consortium/Joint Venture, all or any of the acts, deeds or things necessary or incidental to the Consortium's/Joint Venture's RfP response for the Project, including submission of the RfP response, participating in meetings, responding to queries, submission of information or documents and generally to represent the Consortium in all its dealings with Client or any other Government Agency or any person, in connection with the Project until culmination of the process of bidding till the Project Agreement is entered into with Client and thereafter till the expiry of the Project Agreement.

We hereby agree to ratify all acts, deeds and things lawfully done by our said Attorney pursuant to this power of attorney and that all acts, deeds and things done by our aforesaid Attorney shall and shall always be deemed to have been done by us or Consortium/Joint Venture.

Dated this the \_\_\_\_\_ day of \_\_\_\_\_ 2015

\_\_\_\_\_  
(Signature)

\_\_\_\_\_  
(Name in Block Letter of Executant) *[Seal of Company]*



Witness 1

Witness 2

*Notes:*

*To be executed by all the members individually, in case of a Consortium/Joint Venture.  
The Mode of execution of the power of attorney should be in accordance with the procedure, if any laid down by the applicable law and the charter documents of the executant(s) and when it is so required the same should be under common seal affixed in accordance with the required procedure.*

# Request for Proposal for selection of System Integrator to "Design, Supply, Implement, Commission, Operate & Manage the Command & Control Centre" as a part of Smart City Solutions for Chennai City.

Volume 2: Scope of Work  
RFP No. S.P.D.C.No.B1/100/2016



L I V A B I L I T Y I N D E X

## Table of Contents

1	Scope of Project Work .....	5
1.1	Overview.....	5
1.2	Brief Description of Scope .....	5
1.2.1	Command & Control Center .....	5
1.2.2	Smart Data Center Solution (H/w + S/w) - Hosted on cloud model .....	6
1.2.3	Smart Sensors.....	6
1.2.4	Variable Messaging Board .....	6
1.2.5	City Surveillance System & Disaster Management System .....	7
1.2.6	Mobile Command & Control Center.....	7
1.2.7	Smart Pole.....	8
1.2.8	ICT based Solid Waste Management System.....	9
1.2.9	Integration to Smart Parking management system .....	9
1.2.10	Network Connectivity.....	9
1.3	Scope Matrix.....	11
1.4	Solution Integration Matrix .....	14
2	Detailed Scope of Work and Considerations.....	16
2.1	Overview of Phase I.....	16
2.1.1	Section 1 – Project Planning .....	16
2.1.2	Section 1- Design of CCC solution .....	17
2.1.3	Section 1- Supply, Install, Test & Commission CCC solution.....	25
2.1.4	Section 1- Final Acceptance Testing of CCC solution.....	34
2.1.5	Section 1- Training & Capacity Building.....	37
2.1.6	Solution Stabilization & Go-Live.....	42
2.2	Overview of Phase II.....	43
2.2.1	Detailed Phase-II Requirements.....	43
2.2.2	Section 1- Operation & Maintenance Services .....	43
2.2.3	Section 2- Facility Management Services .....	44
2.2.4	Section 3- Knowledge Transfer & Exit Management.....	50
3	Section 3- Service Level Agreements.....	54
3.1.1	Implementation SLAs.....	55
3.1.2	Operation & Maintenance SLAs.....	55
4	Project Implementation Timelines .....	60
5	Functional & Technical Specifications.....	61
5.1	Command and Control Center (CCC).....	61
5.1.1	Objectives .....	61

5.1.2	Proposed Components of CCC Solution.....	61
5.1.3	Functional Specifications .....	62
5.1.4	Technical Specifications.....	135
5.2	Smart Data Centre -Hosted on Cloud.....	159
5.2.1	Cloud Service Specification .....	159
5.2.2	Typical Data Center Infrastructure – guidelines.....	164
5.3	Smart Sensors .....	197
5.3.1	Functional Specifications .....	197
5.3.2	Technical Specifications.....	198
5.4	Variable Messaging Display Board (VMD) .....	199
5.4.1	Functional Specifications .....	199
5.4.2	Technical Specifications.....	200
5.5	City Surveillance & Disaster Management .....	202
5.5.1	City Surveillance .....	202
5.5.2	Smart solutions with Artificial Intelligence at Edge Devices:.....	228
5.5.3	Disaster Management System .....	230
5.6	Mobile Command Centers.....	232
5.6.1	Vehicle Top Mounted Fixed Camera .....	233
5.6.2	Vehicle Top Mounted PTZ Camera .....	234
5.6.3	In-Vehicle Fixed Camera .....	235
5.6.4	NVR for Vehicle Mounted cameras .....	236
5.6.5	Mobile Vans & Related Equipment’s.....	238
5.7	Smart Pole .....	239
5.7.1	Specifications .....	239
5.7.2	LED based Smart Street light.....	241
5.7.3	Public Internet Access.....	251
5.7.4	Centralised software for Smart Street Lights.....	258
5.7.5	Public Address System.....	258
5.7.6	Emergency Call Box .....	260
5.8	ICT Enabled Smart Solid Waste/Bin Management.....	260
5.8.1	Overview .....	260
5.8.2	Scope of Work .....	261
5.9	Parking Management System.....	262
5.9.1	Project Objective.....	262
5.9.2	Detailed Scope of Work: .....	262
6	Common guidelines / comments regarding the compliance of IT / Non-IT Equipment / Systems to be procured .....	268
7	Payment Terms & Payment Schedule.....	270

8	Annexure 1 Matrix for Scope of Work .....	271
9	Annexure 2 – RACI (Responsible, Accountable, Consulted and Informed) Matrix.....	276
10	Annexure 3: Command & Control Center Layout.....	281
11	Annexure 5: List of Locations .....	282
11.1	List of 22 subways for surveillance .....	282
11.2	List of 100 locations for surveillance.....	282
11.3	Smart Pole Locations.....	285
11.4	Location for Flood Sensors .....	286
11.5	Tentative location for Variable Messaging Board.....	287

# 1 Scope of Project Work

## 1.1 Overview

The project scope entails design, development, installation, operation and maintenance of the following smart city components for **the Chennai Smart City**.

1. Command and Control Center (CCC)
2. Smart Data Center Solution – Hosted on Cloud.
3. Smart Sensors
4. Variable Messaging Board
5. City Surveillance System & Disaster Management System
6. Mobile Command & Control Center
7. Smart Poles
8. ICT based Smart Solid waste/bin Management system
9. Integration of Smart Parking system
10. Laying & Commissioning of Fiber Network for Internet cable Bandwidth.

## 1.2 Brief Description of Scope

### 1.2.1 Command & Control Center

The vision of the Command and Control Center (CCC) is to have an integrated view of all the smart initiatives undertaken by Authority with the focus to serve as a decision support engine for city administrators in day-to-day operations or during exigency situations. This dynamic response to situations, both proactive and re-active will truly make the city operations “SMART”. Managing the complete incident life cycle is a critical element in CCC solutions. It requires the ability to detect performance anomalies i.e. KPIs, current status, leading indicators etc. that often serve as a precursor to an incident and continues with Situational Awareness, Situation Management and investigation/learning. The investigation/learning phase facilitates continuous improvement that improves all aspects of the incident handling process.

Please refer **Section 5.1** for detailed functional and technical requirement of the system.

#### 1.2.1.1 Smart Governance Portal

ICT in governance has been experienced in the form of ERP, which redefined the way Governments work, share information, engage citizens and deliver services to external and internal clients for the benefit of both government and the clients that they serve. Governments harnesses information technologies such as Wide Area Networks (WAN), Internet, World Wide Web, and mobile computing reach out to citizens, business, and other arms of the government to: Improve delivery of services to citizens, businesses and employees Engage citizens in the process of governance through interaction Empower citizens through access to knowledge and information and Make the working of the government more efficient and effective Results in enhanced inclusiveness (people being

part of decision making – virtual participative governance) transparency, convenience and empowerment; revenue growth; and cost reduction.

Please refer **section 5.1.4.13** for detailed functional and technical requirement of the system.

#### **1.2.1.2 Integration of Existing Systems & Utility Systems**

Integrated Command & Communications Center should be able to integrate with various Utility systems such as IOT/ICT sensors, City smart elements like Water/SCADA, Power, GIS, ITMS, Sewerage/ Drainage system, City Bus Intelligent Transport System etc. (Please refer Integration matrix below). CCC requires the ability to detect performance anomalies i.e. leading indicators that often serve as a precursor to an incident and continues with Situational Awareness & Management and investigation/learning.

Please refer **section 1.4** for Integration Matrix provides list of the proposed systems being integrated.

#### **1.2.2 Smart Data Center Solution (H/w + S/w) - Hosted on cloud model**

All the smart city data center, Data recovery and CCC application will be hosted in the Cloud Environment Datacenter. Video and other sensor data will be stored centrally at the datacenter. The datacenter will have IT compute infrastructure, Storage, Network and security components. The DR setup will have the Data backup of all the data available in the Datacenter.

Please refer **section 5.2** for detailed functional and technical requirement of the system.

#### **1.2.3 Smart Sensors**

Smart environment sensors will gather data about pollution, temperature, rains, flood levels, in the city (pollution) on a daily basis. It is for information of citizens and administration to further take appropriate actions during the daily course / cause of any event.

The data should be collected in a software platform that allows third party software applications to read that data. Various environment sensors shall sense the prevailing environment conditions and send the data to the integrated control system where real time data resides and the same shall be made available to various other departments and applications for decision making.

Please refer **section 5.3** for detailed functional and technical requirement of the system.

#### **1.2.4 Variable Messaging Board**

VMD will be installed at identified strategic locations. The location of VMDs will be on the key junctions (mostly on the sides without obstructing the traffic) and other strategic

locations with large foot fall. The VMD software application will allow user to publish specific messages for managing traffic and also general informative messages.

Please refer **section 5.4** for detailed functional and technical requirement of the system.

## **1.2.5 City Surveillance System & Disaster Management System**

### **1.2.5.1 City Surveillance System**

The proposed video surveillance system will involve setting up of IP based outdoor security cameras across various locations in the Chennai City. The video surveillance data from various cameras deployed will be stored and monitored at Command and control centers and Viewing centers. The Surveillance system will also have video analytics with edge level analytics system, etc.

Please refer **section 5.5** for detailed functional and technical requirement of the system.

### **1.2.5.2 Disaster Management System**

In case of an eruption of disaster (both natural/man-made) in the Chennai City the Disaster Management System embedded with Command & Control Centre (ICCC) would come in handy for the necessary mitigation. Disaster management as the systematic process of using administrative decisions, organization, operational skills and capacities to implement policies, strategies and coping capacities of the society and communities to lessen the impacts of natural hazards and related environmental and technological disasters. The CCC should be able to implement Chennai City Disaster Management Standard Operating procedures (SOPs) so that the CCC operator can take control of the situation and act accordingly during such crisis. This comprises of all forms of activities, including structural and non-structural measures to avoid (prevention) or to limit (mitigation and preparedness) adverse effects of hazards.

Please refer **section 5.5.3** for detailed functional and technical requirement of the system.

## **1.2.6 Mobile Command & Control Center**

Mobile vans would be used as and when the situation demands to capture the real-time video feed of an incident. These will be built on 4x4 rugged vehicles and will house communications equipment that may be required to stream video feeds to Command and Control Centers.

Mobile vans shall have the appropriate wireless and 3G/4G connectivity to connect to the nearest Command Control Centers through the Data Centers, local storage for storing at least 24 hours video feed for 4 cameras (7 days), local computing and processing capabilities & a seating capability for minimum four people.

Please refer **section 5.6** for detailed functional and technical requirement of the system.



### **1.2.7 Smart Pole**

The smart poles combine the benefits of LED lighting and mobile connectivity in a "lighting as-a-service" model for cities. The mobile wireless 4G/LTE infrastructure deployment on smart pole can result in better coverage, improved data speeds, reduced radiation, reduced signal dropouts, etc. Smart pole can vastly improve the telecom infrastructure of the city.

The primary function of the smart poles will be to provide street lighting, mobile broadband infrastructure, Wi-Fi hotspot services, Active Geo location transponder for location based services and surveillance camera. These facilities will be connected to the central command and control Centre where it will be constantly monitored and managed. The SI may also use the smart pole for other commercial purposes, namely, smart bill board, electronic vehicle charging, environmental sensor etc. It should however be ensured that the primary functions are not hampered in any way while using the same for other commercial purposes.

Please refer **section 5.7** for detailed functional and technical requirement of the system.

#### **1.2.7.1 Smart Street Light Management**

Implementing an energy efficient Smart LED based Street Light System bundled with motion & ambient light sensors along with Smart controllers has the following advantages over the conventional systems;

- a) LED street lighting can generate energy savings of 50 to 70 percent, with savings reaching 80 percent when coupled with smart controls.
- b) Minimize energy usage based on the real time ambient and traffic movement at the night time
- c) Reduced maintenance cost using centralized real time monitoring and GIS mapping
- d) Asset Management with complete and accurate streetlight inventory

Please refer **section 5.7.25.7.5** for detailed functional and technical requirement of the system.

#### **1.2.7.2 Public Address System**

Public Address system shall be used at intersections, public places, market places or those critical locations to make important announcements for the public. It shall be able to broadcast messages across all PA systems or specific announcement could be made to a particular location supporting single zone / multi zone operations. The system shall also deliver pre-recorded messages to the loud speakers attached to them from CD/DVD Players & Pen drives for public announcements.

Please refer **section 5.7.5** for detailed functional and technical requirement of the system.

#### **1.2.7.3 Emergency Call Box**

The emergency box (or panic button) will enable citizens to establish a two way audio (microphone and speaker) & camera (video camera and a video screen) communication link

with Police (or / and with Authority's Disaster Management Cell or Command and Control Center) through a press of a button.

Emergency/ Panic buttons to be strategically located, suitably sized and identified/clearly labelled for "Emergency".

The emergency mobile app will enable the user to initiate a bidirectional audio call with Police/ Command and Control Center.

Please refer **section 5.7.6** for detailed functional and technical requirement of the system.

#### **1.2.7.4 Telecom BTS**

The necessary provision shall be made to mount Telcom Base Transmission station (BTS) on top of the smart pole in future.

### **1.2.8 ICT based Solid Waste Management System**

The ICT based Solid Waste Management (SWM) system will involve in setting up of cameras with edge analytics to monitor the Garbage bins at the most vulnerable locations (i.e. repeated complaints). Upon garbage likely to reach the threshold the alert to the SWM's central monitoring Station is created whereby the garbage vehicle gets re-directed to the respective SWM location. Secondly the Weighbridge at the dumpyard is also being integrated to the CCC such that the trucks that bring garbage are digitally measured and details are sent on real time basis. This would the municipal authorities to have complete control on the total tonnage waste dumped at the dump yard.

Please refer **section5.8** detailed functional and technical requirement of the system.

### **1.2.9 Integration to Smart Parking management system**

The integration of Parking system would involve of integration of Parking Management System which is being developed by Chennai Municipal Authority of the city. The solution should alerts residents where the open parking space is available and allows them to pay with mobile wallets or bank wallets or mobile wallets like payTM etc through their mobile phones.

Please refer **section5.9** for detailed functional and technical requirement of the system.

### **1.2.10 Network Connectivity**

The entire smart components envisaged above are to be connected through dedicated Network connectivity on High Availability mode. The field infrastructure shall be aggerated through on-field edge gateway which shall be integrated through IP protocol to the central DC/DR cloud. The Network cloud shall be designed to meet the minimum SLA prescribed in this tender.



### 1.3 Scope Matrix

In the current list of projects, the number of projects might increase, and these modifications shall be informed to the successful bidder for necessary action.

#	Project Name	Design	Supply	Test	Commission	Integrate with CCC	O&M	Scalability	PAN City Roll Out	Existing System Integration	Pilot	Facilitation	Migration
1.	Integrated Command & Communication Center	Y	Y	Y	Y	Y	Y	Y	Y		Y	Y	
2.	Disaster Management System	Y	Y	Y	Y	Y	Y	Y	Y		Y	Y	
3.	Smart Governance Portal	Y	Y	Y	Y	Y	Y	Y	Y		Y	Y	
4.	Smart Sensors (Environmental Sensors)	Y	Y	Y	Y	Y	Y	Y	Y		Y	Y	
5.	Traffic Management					Y			Y		Y	Y	
6.	CCTV Surveillance	Y	Y	Y	Y	Y				Y	Y		
7.	Smart Poles	Y	Y	Y	Y	Y	Y	Y	Y		Y	Y	
8.	ICT based SWM	Y	Y	Y	Y	Y	Y	Y	Y		Y	Y	
9.	Smart GPS based Buses and Bus					Y	Y	Y	Y		Y	Y	

#	Project Name	Design	Supply	Test	Commission	Integrate with CCC	O&M	Scalability	PAN City Roll Out	Existing System Integration	Pilot	Facilitation	Migration
	stops												
10.	24x7 drinking Water supply					Y			Y		Y	Y	
11.	Sewerage					Y			Y		Y	Y	
12.	Storm water Drainage					Y			Y		Y	Y	
13.	Smart Metering					Y			Y		Y	Y	
14.	Solar Roof Top								Y		Y	Y	
15.	Solar Paneled enabled LED Lighting								Y		Y	Y	
16.	Public Bike Sharing					Y			Y		Y	Y	
17.	Transportation (Smart Bus Stops cluster with amenities)					Y			Y		Y	Y	
18.	MLCP + Retail outlet					Y			Y		Y	Y	
19.	E-RICKSHAW					Y			Y		Y	Y	
20.	Vending Kiosks/Dedicated Hawker zones					Y			Y		Y	Y	

#	Project Name	Design	Supply	Test	Commission	Integrate with CCC	O&M	Scalability	PAN City Roll Out	Existing System Integration	Pilot	Facilitation	Migration
21.	Public Toilets + Community Toilets					Y			Y		Y	Y	
22.	Social Media Integration					Y			Y		Y	Y	
23.	Dial 100 /112 Integration					Y			Y		Y	Y	
24.	CCTNS					Y			Y		Y	Y	
25.	VAHAN					Y			Y		Y	Y	
26.	SARATHI					Y			Y		Y	Y	
27.	e-Challan Integration					Y			Y		Y	Y	
28.	Smart Street Light System					Y	Y	Y	Y		Y	Y	Y
29.	Existing Live Services					Y						Y	Y

## 1.4 Solution Integration Matrix

#	Name of the Components/ System	Input Data Format	Integration Point	Dash boarding Point
1.	Video Management Software	API/SDK	EMS & CCC	CCC
2.	Video Analytics	API/SDK	VMS & ESB	CCC
3.	Disaster Management System + Incident Management System	API/SDK	ESB	CCC
4.	ANPR/RLVD Software	API/SDK	CCC	CCC
5.	Facial Recognition Software	API/SDK	VMS	CCC
6.	Enterprise Management Software	API/SDK	ESB	EMS
7.	PUBLIC Address Software	API/SDK	CCC	CCC
8.	Variable Message Display System	API/SDK	CCC	CCC
9.	GIS Map data / Engine	API/SDK	ESB	CCC
10.	Wi-Fi Management Software	API/SDK	ESB	CCC
11.	Smart Lighting Software	API/SDK	ESB	CCC
12.	Adaptive Traffic Control System Application	API/SDK	ESB	CCC
13.	VTS, Fleet Management & PIS	API/SDK	ESB	CCC
14.	Solid Waste Management Software	API/SDK	ESB	CCC
15.	Parking Management	API/SDK	ESB	CCC
16.	Environmental Sensor Software	API/SDK	ESB	CCC
17.	2 – way Mobile Application	API/SDK	CCC	Mobile App
18.	Video Wall Application	API/SDK	CCC	CCC

#	Name of the Components/ System	Input Data Format	Integration Point	Dash boarding Point
19.	EPABX	API/SDK	CCC	CCC
20.	Mobile Van Surveillance	API/SDK	CCC	CCC
21.	Vending Kiosks/Dedicated Hawker zones	API/SDK	ESB	CCC
22.	Smart Poles	API/SDK	ESB	CCC
23.	24x7 drinking Water supply SCADA	API/SDK	ESB	CCC
24.	Sewerage SCADA	API/SDK	ESB	CCC
25.	Stormwater Drainage SCADA	API/SDK	ESB	CCC
26.	Smart Metering	API/SDK	ESB	CCC
27.	Solar Roof Top	API/SDK	ESB	CCC
28.	Public Bike Sharing	API/SDK	ESB	CCC
29.	E-RICKSHAW	API/SDK	ESB	CCC
30.	Public Toilets + Community Toilets	API/SDK	ESB	CCC
31.	Social Media Integration	API/SDK	ESB	CCC
32.	VAHAN	API/SDK	CCC	CCC
33.	SARATHI	API/SDK	CCC	CCC
34.	e-Challan Integration	API/SDK	CCC	CCC
35.	DIAL 100	API/SDK	CCC	CCC
36.	e-Governance Portal	API/SDK	ESB	CCC
37.	Enterprise Service Bus	API/SDK	CCC	CCC



## 2 Detailed Scope of Work and Considerations

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

### 2.1 Overview of Phase I

The phase-1 will cover the work of the SI from the date of issue of LOA till the date of issue of commissioning certificate for the successful roll out of the Smart City solution in Chennai.

#### 2.1.1 Section 1 – Project Planning

The success of the project depends on the proper project planning and management. At the onset, the Service Provider shall plan the project implementation in great details and should provide a micro level view of the tasks and activities required to be undertaken in consultation with Authority. An indicative list of planning related documentation that the Service Provider should make at the onset is as follows:

- **Project Schedule:** A detailed week-wise timeline indicating various activities to be performed along with completion dates and resources required for the same
- **Manpower Deployment List:** A list needs to provide with resources who will be deployed on the project along with the roles and responsibilities of each resource.
- **Resource Deployment List:** List and number of all resources (including but not limited to servers, storage, network components and software licenses) other than manpower that may be required.
- **Communication Plan:** Detailed communication plan indicating what form of communication will be utilized for what kinds of meeting along with recipients and frequency.
- **Progress Monitoring Plan:** Detailed Daily, Weekly, Monthly Progress Report formats along with issue escalation format. The format will be approved by Authority to the successful bidder before start of the project.
- **Standard Operating Procedures:** Detailed Standard Operating Procedures for all the events and incidents to be developed and customized based on the Project scope and the functional requirement of the RFP. The SOPs will be approved by Authority to the successful bidder before the project implementation.
- **Risk Mitigation Plan:** List of all possible risks and methods to mitigate them.
- **Escalation Matrix & Incident Management:** A detailed list of key contact persons with contact details with escalation hierarchy for resolution of issues and problems. This has to be via an Incident Management system.
- **Traceability Matrix:** chronological requirement matrix which capture the original requirements and subsequent changes with clear audit trail which shall used as reference during the for compliance checks in the Final Acceptance Testing.

## **2.1.2 Section 1- Design of CCC solution**

- The system Integrator should design, develop, implement, integrate and test the complete smart components as per the BOM provided in this RFP Vol I.
- Conducting site survey, obtaining necessary permissions, developing system requirements, standard operating procedures etc.
- 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 at all the field locations, DC and CCC.
- Formulation of solution architecture, detailed design of smart city solutions for the field location, DC and CCC, development of test cases (Unit, System Integration and User Acceptance), SOP documentation

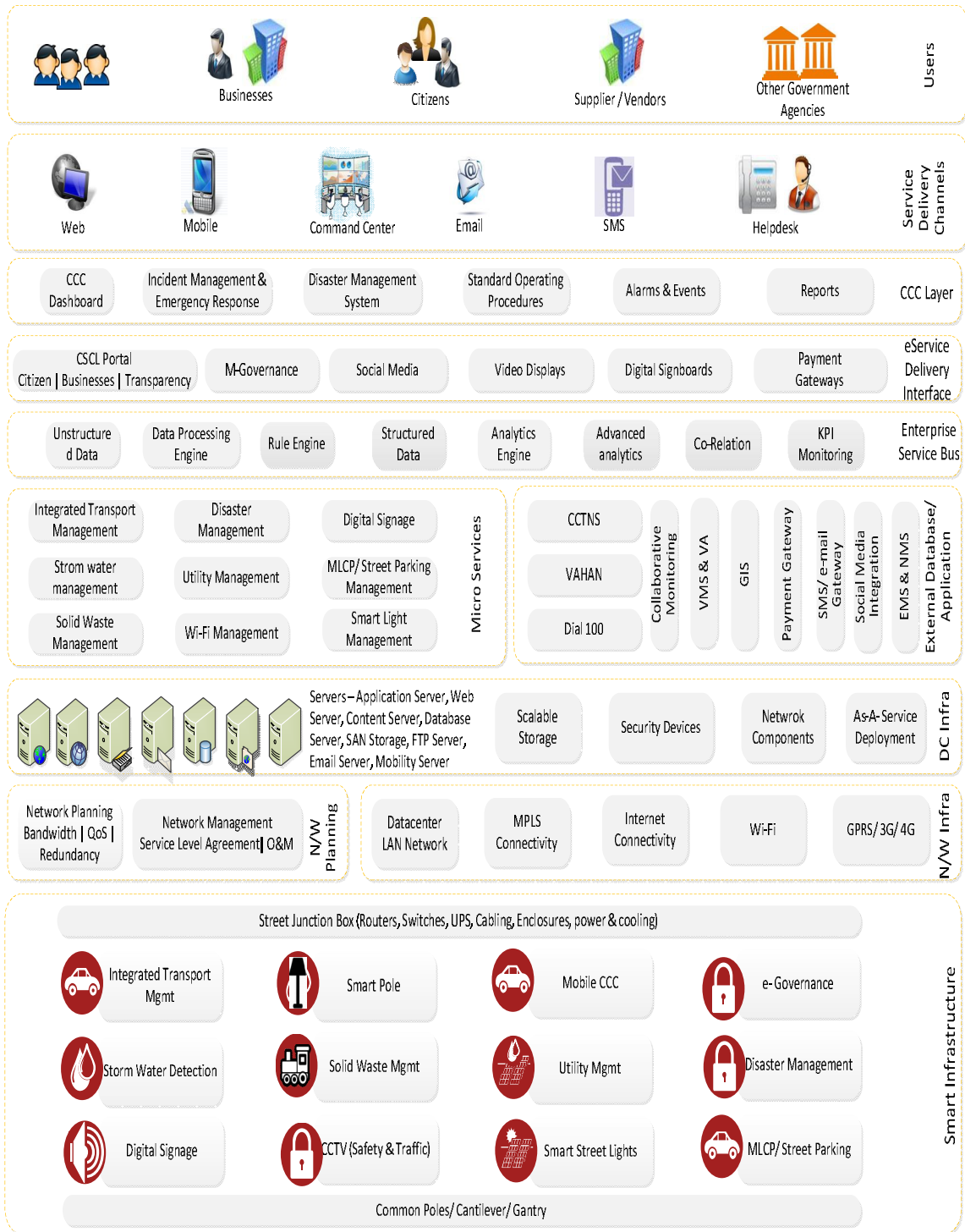
### **2.1.2.1 CCC Solution Design Functional Architecture**

Various components of the project, including expected system users, are as below and also depicted in the component architecture diagram below.

1. Street IT Infrastructure Layer
2. Network Layer
3. Data Center Layer
4. Application Layer
5. Integration Layer
6. Command and Communication Center Layer
7. Security Layer

All this component architecture is indicative in nature and is given in the RFP to bring clarity to prospective bidders on the overall scope of project and its intended use. The successful bidder shall carry out the detail requirement analysis and finalize the technical architecture in consultation with authority and its consultants. As per the figure below, the architecture of the complete network of smart elements is as follows.

### Functional Architecture of CCC :



- **Smart IT Infrastructure Layer** - The sensor layer will help the city administration gather information about the ambient city conditions or capture information from the edge level devices like environmental sensors, emergency

call boxes, cameras, etc. Authority is expected to deploy multiple environmental sensors across the city, to measure ambient conditions such as light intensity, temperature, water level (for chronic flood spots), air pollution, noise pollution and humidity. The output field devices layer will contain display devices or bi-directional (input & output) devices connected to the network which will be used by citizens to consume - and for administrators to provide - actionable information. Such field devices include digital messaging boards, environmental data displays, PA systems and emergency boxes.

- **Network Layer** - The secured network layer will serve as the backbone for the project and provide connectivity to gather data from sensors and communicate messages to display devices and actuators. The network bandwidth will be provided by Bidder; however, the selected bidder will have to size the bandwidth required for the overall solution, and supply and install the edge devices to utilize the network.
- **Data Center Layer** -The data center layer will house centralized computing power required to store, process and analyze the data to decipher actionable information. This layer includes servers, storage, ancillary network equipment elements, security devices and corresponding management tools. A disaster recovery site, which includes servers, storage, network equipment and security management systems will be used in case of fall back mechanism for the data center.
- **External Database / Application layer** – The database of various edge infrastructure such as sensors, surveillance camera, etc. based micro cameras coupled with data from eGovernance applications in the City/State gets routed from this layer
- **Enterprise Service Bus Layer** - The applications layer will include Command & Control center platform, Enterprise Service Bus, Disaster Management, Video Management System, smart Governance and smart components etc. applications that interface and control the street infrastructure, enterprise management system to monitor and manage all IT infrastructure and street infrastructure deployed in the city, and surveillance applications. While aspects of ambient conditions within the city will be gathered through various sensors deployed as a part of present RFP, some city specific data will come from other government and non-government agencies. It is through the integration layer – that data will be exchanged to and from the under lying architecture components and other data from system developed by government (such as police department, meteorological department, street lights department, water department, irrigation department, transport organizations within Chennai, etc.) and non-government agencies. This middleware shall take Publish-subscribe based framework.

- **eService Delivery Interface Layer:** Multiple 3<sup>rd</sup> Party and local service delivery gateways such as Payment gateway, CSC, Digital Signboards, mobility-based services, etc. gets interfaced at this layer.
- **CCC Layer:** IOT based analytics, Big Data analysis, Dashboarding, SOP and EMS, etc. enable citizens and administrators alike to get a holistic view of city conditions, and make informed decisions.
- **User Layer :**All the stakeholders of this solution including direct & indirect beneficiaries would be part of this layer. They interact with CCC solution through layer with proper authentication.
- **Cross-Functional Vertical Security Layer** - As ambient conditions, actuators and display devices are now connected through a network, security of the entire system becomes of paramount significance and the system integrator will have to provide: Infrastructure security, Network security, Identity and Access Management, and Application security.
- **Scalability** - Important technical components of the architecture must support scalability to provide continuous growth to meet the growing demand of Authority. The system should also support vertical and horizontal scalability so that depending on changing requirements from time to time, the system may be scaled upwards. There must not be any system-imposed restrictions on the upward scalability in number of cameras or other edge devices. Main technology components requiring scalability are storage, bandwidth, computing performance (IT Infrastructure), Software/application performance and advancement in camera features. In quantitative terms, there may not be major change in number of Command and Control Center.
- **Availability** - The architecture components should be redundant and ensure that there are no single points of failure in the key solution components. Considering the high sensitivity of the system, design should be in such a way as to be resilient to technology sabotage. To take care of remote failure, the systems need to be configured to mask and recover with minimum outage. The Bidder shall make the provision for high availability for all the services of the system. Redundancy has to be considered at the core / data center components level.
- **Security** - The architecture must adopt an end-to-end security model that protects data and the infrastructure from malicious attacks, theft, natural disasters etc. Successful Bidder must make provisions for security of field equipment as well as protection of the software system from hackers and other threats. Using Firewalls and Intrusion Prevention Systems such attacks and theft should be controlled and well supported (and implemented) with the security policy. The virus and worm attacks should be well defended with gateway level Anti-virus system, along with workstation level Anti-virus mechanism. There should also be an endeavor to make use of the SSL/VPN technologies to have secured communication between Applications and its end users.

Furthermore, all the system logs should be properly stored & archived for future analysis and forensics whenever desired. Authority would carry out the security audit of the entire system in approx. 3 months of Acceptance / operationalization through a Third-Party Auditor (TPA). The following guidelines need to be observed for security:

- Build a complete audit trail of all activities and operations using log reports, so that errors in system – intentional or otherwise – can be traced and corrected.
- The most appropriate level of security commensurate with the value to that function for which it is deployed must be chosen
- Access Controls must be provided to ensure that the system is not tampered or modified by the system operators or unauthorized persons.
- Implement data security to allow for changes in technology and business needs.

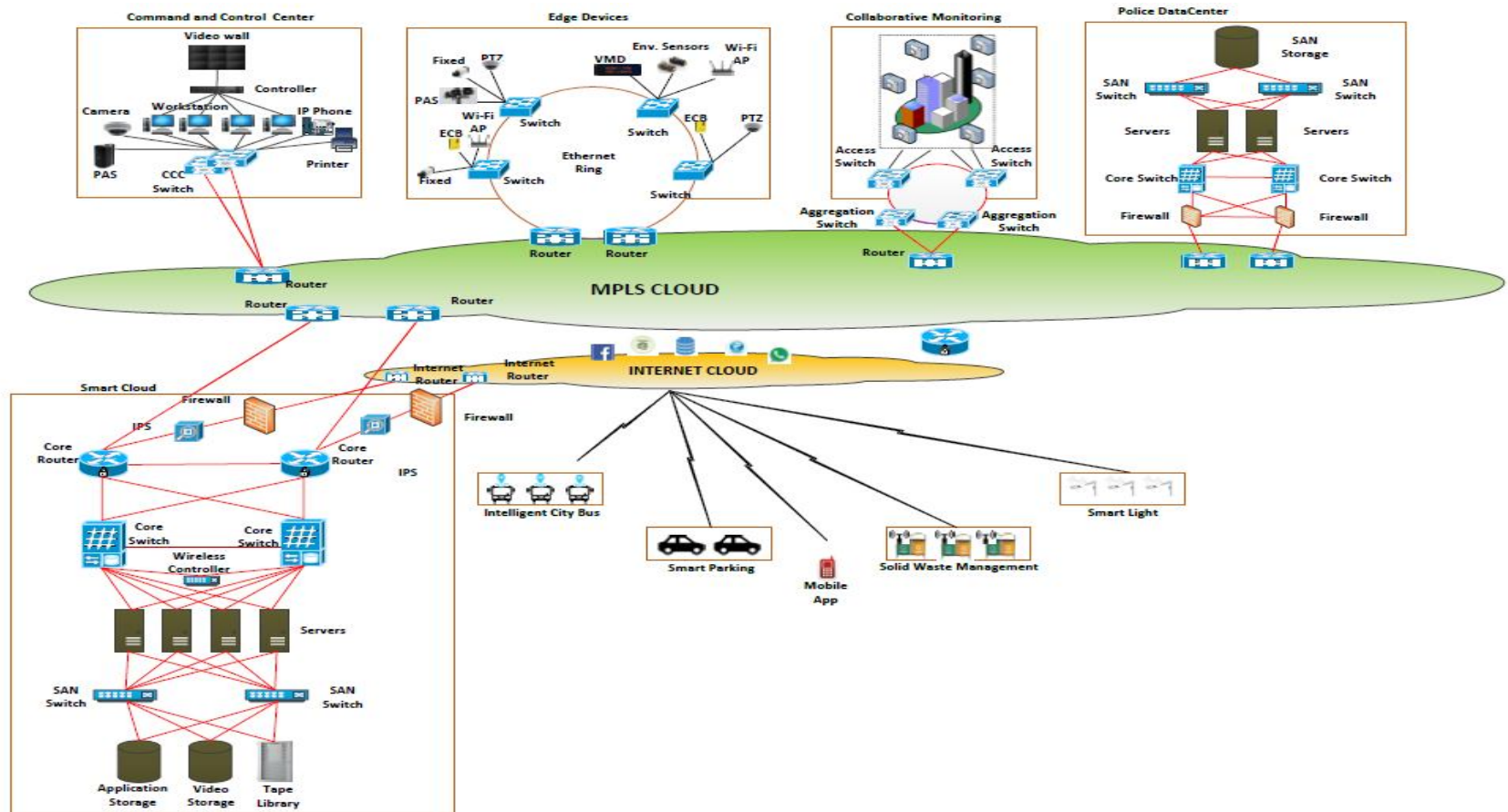
Field equipment installed through this Project would become an important public asset. During the implementation phase of the Project the SI shall be required to repair / replace any equipment if stolen/damaged. Appropriate insurance cover must be provided to all such field equipment.

- **Manageability** - Ease of configuration, ongoing health monitoring, and failure detection are vital to the goals of scalability, availability, and security and must be able to match the growth of the environment.
- **Interoperability** - The system should have capability to take feed from cameras installed by private / Govt. at public places, digitize (if required) & compress (if required) this feed & store as per requirements. Also system should have integration capabilities between various IT systems of the Authority as indicated in scope of work. The system can integrate with social media platforms for social media monitoring. It may be noted that most of the systems deployed by these large private / public/community establishments use open standards. Bidder may carry out further study on the same. Authority shall facilitate to get cooperation from the private / public establishments for community monitoring.
- **Open Standards** - Systems should use open standards and protocols to the extent possible.
  - ✓ The Successful Bidder will be required to review the Technical Architecture suggested in the Tender and finalize the detailed architecture for the overall system, incorporating findings of site survey exercise. The network so envisaged should be able to provide real time sensor data to the smart city Command Centers and video stream to the police control center and from police control center to the Smart City Datacenter, Tablets for select officials through Data Centers. All the components of the Technical Architecture should be of best industry standards.



### 2.1.2.2 CCC Solution Design Network Architecture

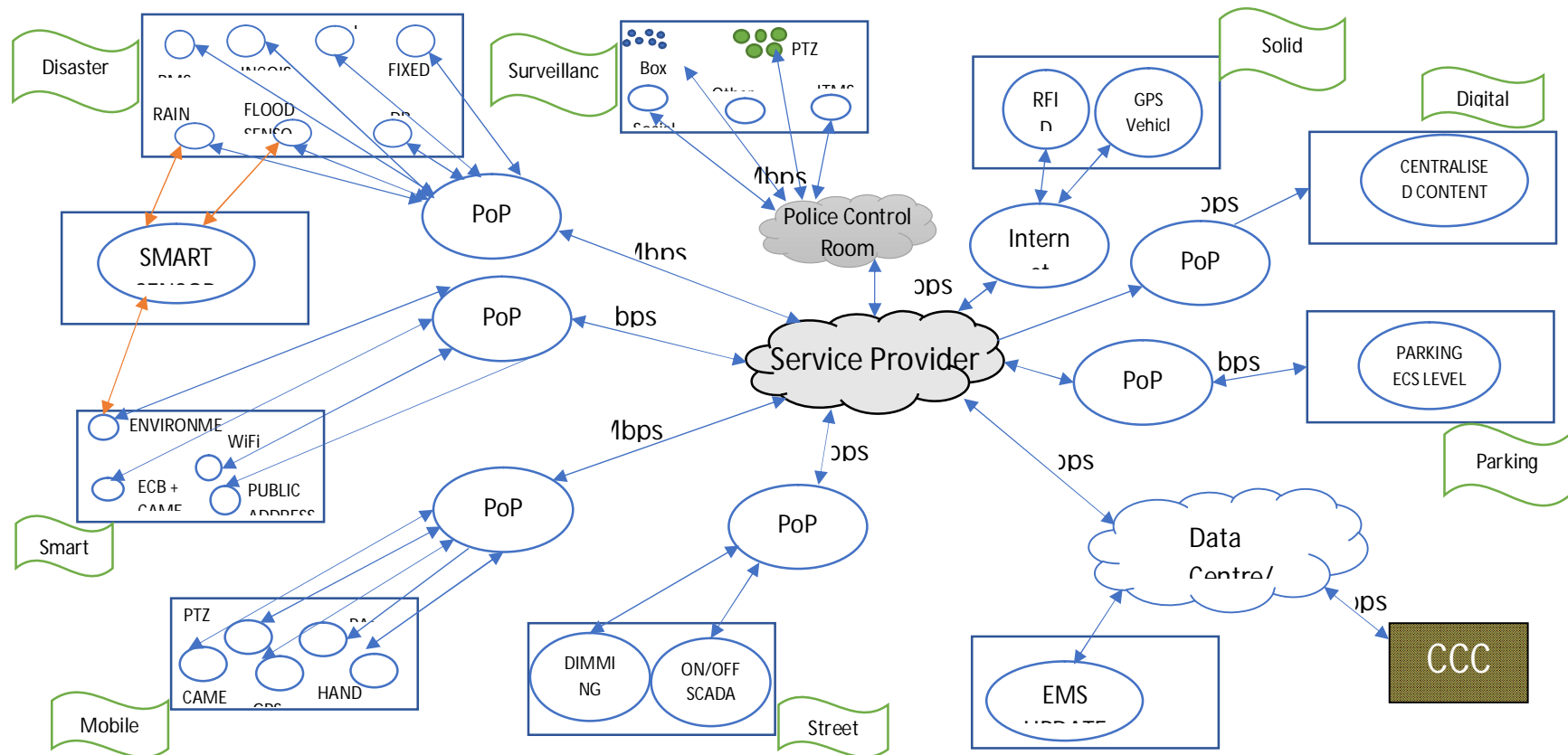
The typical CCC Network solution architecture is given below,





### 2.1.2.1 CCC Solution Design Entity-wise Bandwidth Sizing

The typical CCC bandwidth sizing planned, bidder is use this a reference and propose a comprehensive design



## **2.1.3 Section 1- Supply, Install, Test & Commission CCC solution**

### **2.1.3.1 Command & Control Centre**

#### *2.1.3.1.1 CCC Site Preparation with Civil, Interior, Electrical & Network Works*

The System Integrator shall inspect the identified site for its feasibility for commissioning of CCC. This feasibility of the site will include components such as floor load bearing capacity, structural soundness, building requirement as per TIA 942 standards used for building critical ICT based infrastructure. The bidder shall make necessary arrangement at their costs for conducting any tests for site feasibility. The authority would need to be apprised and consent shall be obtained before commencing the tests such UTM (Universal Testing Machine) then it shall be done by competent qualified professional and report shall be submitted to the authority before commencement. The positive outcome of this assessment finding shall be used as basis for commencement of site preparation work.

SI shall also ensure that also bear all expenses for getting solution infrastructure certified by governing bodies such CEIG (for electrical work), pollution department and other statutory clearance for having the CCC in the building

Post successful completion of site feasibility, different floor layout design options shall be prepared by SI and presented to authority for final decision making. Based on the approval of the authority on the same, SI shall work on detailed drawings for other interior, electrical & network layouts / drawings.

The design of CCC shall which include the IT design (functional architecture, network topology, bandwidth sizing, Cloud compute & storage sizing, BOM with make & model) and Non-IT design (civil, interior, electrical, building safety/security control systems, BOM with make & model) and get the same approved by the authority. Subsequent to approval of the same the site preparation shall be carried out towards successful commissioning before targeted commissioning period.

#### *2.1.3.1.1 Commissioning of Video Wall for CCC Solution*

The SI shall evaluate site which has been approved by the authority and give different option of CCC Video Wall grid placement with a design approach to maximize wall occupancy. For the given identified site the a sampled video grid sizing was carried out and 12x2 (12 columns & 2 rows) is planned out which can be scaled up to 14 x 3 in future. In similar lines the SI needs to propose the design for the approved site.

### **2.1.3.2 Cloud Data Centre / Disaster Recovery Services**

The SI shall plan to host the Data Centre & Disaster Recovery Infrastructure on cloud environment. The SI shall as per their strategy can adopt Infrastructure as a Service (IaaS) or choose collocate exclusive server/storage ear-marked for this project in the cloud environment. SI shall only use Ministry of IT, Gol's empaneled cloud service providers for the DC-DR cloud services of this project. The DC-DR shall be designed in such a way that it supports the Business Continuity Planning prescribed in section 1.1.3.9 in this RFP.

The surveillance data feed shall primarily routed to the police department's control room and then re-routed to this CCC. The Si shall commission for entire network connectivity from field location, to edge gateway to the destinations of CCC operated through the DC/DR cloud.

The SI shall ensure that they DC-DR cloud shall comply with ISO 27001 certifications and ensure for all complete security compliance and prescribed service levels in this RFP. The Cloud based DC-DR scalability services shall on back-to-back i.e. as soon as the new integrations services as made live.

### **2.1.3.3 Field level Smart Components Sensors / Variable Messaging Boards / Smart Poles /**

- SI shall provide all the necessary field components required for complete the Solution. The indicative BOM is provided in RFP Vol I.
- SI shall provide Power (provisioning of power including one-time charges and energy meter) and Network (Last mile including bandwidth- Internet & Intranet) at the field location and the CCC and DC.
- ROW and RI charges including getting permission and approvals is part of the SI scope.
- SI has to design the poles and structures to mount the cameras and other sensors required for this project ensuring future scalability. The SI has to submit the design to the authority for the approvals. After the confirmation from the authority SI can install the poles at the respective location.
- SI has to the site survey to identify the number of poles, cantilever, foundation, passive cable, electrical cable, Junction Box, energy meter, earthing etc.
- Authority shall appoint a team to accompany the SI during the joint site survey. It is the responsibility of the SI to organize the electrical, network service provider and police department during the site survey.
- The location of the pole, Junction Box, sensors and direction of the cameras shall be finalized after the consultation with the department. It is the responsibility of the SI to submit the site survey drawing and getting approvals from the authority on timely basis.
- SI shall provide last mile connectivity at all the field location, DC and CCC. For the Backbone connectivity for the entire project SI can propose their own network or any other network service provider.

#### 2.1.3.4 City Surveillance & Disaster Management

**City Surveillance :** Surveillance cameras being planned in 100 critical locations given in this RFP as annexure. The SI shall joint discussion with authority and associated stakeholder's department such as Police, Highways, etc. Authority shall be responsible for facilitating and convening these joint meeting on the request of SI. During the meeting the SI shall present the design criteria / assumption for camera positioning, quantity, commissioning for different possible street junction scenarios. The stakeholders shall review their SI's approach and give feedback and recommendations on the local site conditions and also apprise incase of any change in site locations of cameras. The SI shall carryout a survey to all the field locations and identified locations and prepare site-wise sketch detailing on the location-wise of deployment, poles position, camera directions, camera type Vs quantity and site-specific challenges if any. SI shall ensure and adequately in both design and commercials to ensure to successfully address the commissioning of the camera at the field locations. The SI shall also plan for edge level intelligence which may aid in analytics at the edge level itself.

**Disaster Management:** Integration of rain gauges, flood sensor, cameras at Subways, data from related agencies such as, Meteorological department, INCOIS, Dams, bridges, New Channel feeds in Television, Radio, social media, GCC toll-free disaster help-line, disaster-relief mobile-groups, etc. are to be integrated with the disaster management software and this would aid predicting the impact of disaster and send automatic pre-configured alerts to other associated agencies such as zonal officers, hospital, ambulance, drugs in pharmacy. The solution would also have on real time basis information such as digital assets, physical earth-moving assets used during disaster (pumps, tree cutter, power saw, etc.), snake catchers, relief centers, medical camps, bridges, NGO's, etc. In addition to the above the solution is also envisaged to have integration with Building Management System installed in all the buildings this would particularly aid proactive preparation of fire breakout locally in a building / multi-floor premises in the city. To start with the it is desired to connect two Government buildings where there is BMS system installed for first level cross checking later the same needs to be scaled up to the other buildings / premises across the city. The SI needs to plan the integration & bandwidth for such integrations.

The SI shall have a joint discussion with authority and associated stakeholders department such as Disaster Management, Police, Metrological, Highways, Electricity, CMWSSB, Fire etc. Authority shall be responsible for facilitating and

convening these joint meeting on the request of SI. During the meeting the SI shall present the Standard Operating Procedure (SOP), design criteria / assumption which. The stakeholders shall review their SI's SOP for disaster & Normal operations and give feedback and recommendations. The SI shall carryout necessary recommendations and submit the final SOP document for operations and configuration of DRM tool. This SOP shall used as a ready reckoner for CCC operations during both disaster and normal periods. The SI shall also plan for edge level intelligence which may aid in analytics at the edge level itself.

#### **2.1.3.5 Mobile Command & Control Centre**

All the edge smart components are planned at strategic locations covering the length and breadth of the city; however, during disaster / point of interest it becomes critical to have avenues of interest which may not under radar / coverage of the field level smart components. Therefore, this Mobile Command Centre vehicle has been envisaged which can CCC services on the go. The real-time physical detailing of the ground realities can be got from Mobile CCC which can traverse to the actual area of interest and get the required details for second degree of data analytics and processing by the CCC. The SI shall plan a all-terrain robust vehicle for the Mobile CCC which shall effectively house all the disaster management related equipment (refer BOM & Price Bid for sub-component details). This vehicle call act as mobile CCC and incase of challenges at the CCC site then this can be one of alternate locations of CCC operations to be carried as well.

#### **2.1.3.6 ICT enabled Smart Solution for Solid Waste Management**

The CCC shall enabled with video feeds from top 100 locations of perineal issues of the overflowing waste bins. The cameras are being planned at strategic locations for these bins locations where these SWM related challenges exists. The edge level analytics would enable to throw up an automatic alert where there is potentially predict the potential bins that are likely to get filled and proactively alerts the waste-collecting-vehicles for re-routing and collections. Also, the weighbridge at the two dumpyards in the city needs to get connected to the central CCC. The SI shall ensure to connect the weighbridge details of loaded and unloaded truck are transmitted to the CCC.

#### **2.1.3.7 Integration with Smart Parking System**

The city is in the process of selecting exclusive service provider for Parking Management system, the feeds from each parking lots (at a car parking space level details) needs to be plotted in GIS system in CCC. The SI scope under this

RFP shall be ONLY to integrate the parking management related data from PMS service provider to the CCC which may be showcased on GIS & MIS templates. The same may be used for city governance by superimposing similar data on the common base map.

#### **2.1.3.8** Connectivity for on field smart components to the CCC

- The SI is required to provide the data connectivity for smart components through edge level gateway; this data from gateways shall need to be connected on IP based protocol to the central cloud DC/DR. This would feed the data to CCC.
- The SI shall also provide the required connectivity through MPLS between the Help Desk and the application at cloud infrastructure. The typical network design architecture is given in this RFP for reference.
- Required infrastructure and connectivity for SMS gateway shall also be provided by the SI
- The SI would be responsible to design the network solution with adequate capacity and redundancy to meet the Service level requirements mentioned in the RFP.
- All the connectivity provided under this project should be secured and reliable.
- Network throughput requirement (Both Internet & Intranet)
- Backup requirement

Detailed planning of hardware deployment and configuration should be submitted to the Authority. The configuration planning should include following details.

- Network architecture planning including
  - VLAN configuration planning
  - IP address planning
  - Subnet planning and routing planning
  - Firewall configuration planning
  - Backup methodology
  - Backup links between DC & Near DR

#### **2.1.3.9 Business Continuity Planning**

The CCC solution shall be designed on High Availability mode even during disaster situations with the following objectives

Record Point Objective (RPO) : near to zero data loss

Record Time Objective (RTO) : 1 minute

SI shall design the connectivity & infrastructure accordingly to meet this BCP requirement & Prescribed SLA.

#### **2.1.3.10 GIS based Services**

The SI shall exclusive GIS based software to carryout the GIS based analytics and also build additional shape files & layers for facilitating decision making. The some of base shape file and layer details of basic utilities such existing above ground utilities of corporation are being captured through LIDAR based survey as a part of another initiatives undertaken by GCC & CSCL. The SI needs to create base map using these existing shape files from various departments. The authority shall aid getting the details of shape files from various departments. The shape files and its reflections on the base map needs to be updated inorder to have real-time analysis, the updations can be done through field survey or crowdsourcing approach as well, the SI shall bear the cost for such updations till contract period.

#### **2.1.3.11 Helpdesk Services**

The SI shall set up the Help Desk at a suitable location. The SI shall inform the location of the Help Desk. The SI shall submit the solution for the proposed Help Desk and implement the same. The Help Desk will be utilized 24x7 basis, by all the project stakeholders during the implementation phase and as well as during the O & M phase. The Help Desk will register the issues that will be faced by all the stake holders and the issue will be followed up, till it is closed. The functioning and performance of the help desk is critical in order to meet the SLA. The SI will coordinate with the OEMs for maintenance of the infrastructure during the O&M phase through the same help desk. So, the help desk module shall have the functionality to generate the periodical help desk reports and customized SLA reports from the help desk database. The Help Desk shall also be ITIL (Latest version) compliant.

The Help Desk should exclusive Toll Free number for addressing the concerns and recording of tickets. The existing 1913 emergency held by Greater Corporation of Chennai shall also be integrated such that during disaster there shall be single number required and all sub-systems shall use the data coming from various sources to effective synergised and analysed at CCC. Initial capital investment and all the recurring charges to be borne by the Sland prices needs to showcased in the price bid.

The selected System Integrator will be responsible for installation of application software at the Helpdesk under the purview of this Project. The functional requirements of the Helpdesk application are listed below:

<b>Helpdesk – Functional Requirements</b>	
1	Helpdesk should be able to receive requests from internet / intranet / chat/ phone.
2	All requests received from external and internal users from the portal / intranet / chat/ phone should be logged into the Helpdesk application along with details of who made the request (User name, email ID), time and date of request etc
3	For requests received via phone, the system shall have the capability of Calling Line Identification (CLI) or the Automatic Number Identification (ANI) from the telephone system.
4	A menu based IVR should help categorize the calls and for every call landing on the Helpdesk through the Helpline, it shall be possible to intelligently route the calls to specific operators, based on nature of call. If a caller abandons/disconnects the call while waiting for an agent, such abandoned calls shall be removed from the queue.
5	System should be able to match the detected number of the caller with the existing database to retrieve their profile/related information.
6	System should allow categorization of the request based on type of problem. The application should be menu-based to arrive at the category of the request.
7	System should provide unique reference number for all requests logged which can be quoted by the users at the Helpdesk to know the status of the request
8	System should send acknowledgement of request received at Helpdesk through SMS or email to the users (if the user is internal staff or a registered dealer)
9	Depending upon the category of the request, system should route the request logged into the Helpdesk application to the designated Helpdesk operator or to a designated officer within the Department as per process agreed for resolution of requests.
10	System allows queuing of request by category. Requests should be resolved on a FIFO basis
11	System should allow the user to submit details relating to the response / resolution of the request
12	After the resolution of any issue, system should send e-mail and SMS requesting for confirmation of the issue resolution from the internal user who had logged the request. System shall facilitate capturing the feedback, in both quantitative and qualitative manner as agreed with Department, from the caller through email, SMS or online form for each call logged by the caller
13	User should be able to close the request after receiving confirmation from the internal user or otherwise in case of external user
14	System should allow voice recording of calls as per requirements of the Department.
15	System should provide facility in Helpdesk application to create a knowledge base



**Helpdesk – Functional Requirements**

	of all request logged through various channels and their resolution to allow operators to search / query the knowledge base based on keywords
16	The knowledge base should provide for FAQs and also be able to provide for the import of any issue along with its resolution method into the knowledge base

All users (departmental and external) of the system should be able to log a request in the system using any of the following channels:

1. email
2. Telephonic call on the Toll-free Helpline
3. Online AI based chatbot on the smart web-portal for citizen interface
4. Through intranet for departmental users or web-portal for external users

The detailed description of activities to be performed by the selected System Integrator for the Helpdesk is as listed below:

The selected System Integrator has to operate the central Helpdesk on a 24x7 basis from the Department office in Chennai. The space for the Helpdesk will be provided by the GCC Department near CCC site.

The selected System Integrator will be responsible for the site preparation at the proposed Helpdesk location. The minimum site preparation requirements are given in the table below. The selected System Integrator has to deploy all necessary infrastructures and prepare the site so as to meet the SLAs mentioned in the RFP.

S. No.	Location	Minimum Site preparation Requirements per Site
1.	Helpdesk (Space to be provided by Department)	<ol style="list-style-type: none"> <li>1. Adequate firefighting equipment</li> <li>2. Generators</li> <li>3. UPS with at least 30 minutes of backup upgradeable to 2 hours. The minimum battery backup required to be provisioned by selected System Integrator is 30 minutes</li> <li>4. Structured cabling for Electrical and Network Wiring and Cabling. The SI needs to undertake the assignment to design, lay &amp; maintain structured cabling for providing electrical and network connectivity to all the required devices. The cabling done should ensure adequate rodent protection, protections at difficult corners of the building, waterproof cabling. The cabling should be done in a manner so that least changes are required for future expansion &amp; should also be resistant to wear &amp; tear.</li> </ol>

S. No.	Location	Minimum Site preparation Requirements per Site
		<p>5. Required Furniture for seating operators</p> <p>6. Toll-free number with adequate PRI 5 lines</p> <p>7. Air-conditioning if deemed necessary by the System Integrator</p> <p>8. Partitioning of the space for operator as required should be done by the SI</p> <p>Please note that Civil works, flooring etc at Helpdesk are not required to be done by the selected System Integrator as part of this Project</p>

#### 2.1.4 Section 1- Final Acceptance Testing of CCC solution

After successful installation of equipment in accordance with the requirements in the Tender, the Successful Bidder would need to carry out Final Acceptance Testing in 2 different phases - (a) Unit Testing and (b) Integration Testing. These tests would be carried out based on the test cases developed and validated by Authority. Apart from the functional testing of the entire system components, the testing would also verify following aspects:

- Configuration Testing (to ensure that all the components are configured properly)
- Security Testing (to review & evaluate security controls)

Final acceptance certificate shall be issued by Authority to the Successful Bidder after successful testing in a real time condition for at least 45 days of trouble free operation. The date on which final acceptance certificate is issued for final phase shall be deemed date of the successful commissioning of the Project. Authority shall consider implementation of 95 percent smart components of the project as a sufficient condition for the Project Go-Live. Any delay by the Successful Bidder in the performance of its contracted obligations shall render the Successful Bidder liable to the imposition of appropriate liquidated damages or termination, unless agreed otherwise by Authority.

##### 2.1.4.1 System Documents, User Documents

The Successful Bidder will provide documentation, which should follow the ITIL (Information Technology Infrastructure Library) standards. This documentation should be submitted as the Project undergoes various stages of implementation. Indicative list of documents include:

- **Project Commencement Documentation:** Project Plan in giving out micro level activities with milestones & deadlines.
- **Cabling Layout:** Systems Integrator shall submit the detailed cabling layout including cable routing, telecommunication closets and telecommunication outlet/ connector designations. The layout shall detail locations of all equipment and indicate all wiring pathways.
- **Equipment Manuals:** Original Manuals from OEMs.
- **Installation Manual:** For all the application systems
- **Training Material:** Training Material will include the presentations used for trainings and also the required relevant documents for the topics being covered. Training registers should be submitted for same.
- **User Manuals:** For all the application software modules, required for operationalisation of the system.
- **System Manual:** For all the application software modules, covering detail information required for its administration.
- **Standard Operational Procedure (SOP) Manual:** The Bidder shall be responsible for preparing SOP Manual relating to operation and maintenance of each and every service

as mentioned in this Tender. The draft process (SOP) document shall be formally signed off by Authority before completion of Final Acceptance Test. This SOP manual will be finalised by the Bidder within 2 months of operationalisation of each phase, in consultation with the Authority and formally signed off by the Authority.

**Note:** The Successful Bidder will ensure upkeep & updation of all documentation and manuals during the contractual period. The ownership of all documents, supplied by the Successful Bidder, will be with Authority. Documents shall be submitted in two copies each in printed (duly hard bound) & in softcopy formats.

**2.1.4.2 Compliance to Standards & Certifications**

- a. For a large and complex set up such as the Project, it is imperative that the highest standards applicable are adhered to. In this context, the SI will ensure that the entire Project is developed in compliance with the applicable standards.
- b. During project duration, the SI will ensure adherence to prescribed standards as provided below:

#	Component/Application/System	Prescribed Standard
1.	Information Security	ISO 27001
2.	IT Infrastructure Management	ITIL specifications
3.	Service Management	ISO 20000 specifications
4.	Project Documentation	IEEE/ISO/CMMi (where applicable) specifications for documentation

- c. Apart from the above the SI need to ensure compliance of the project with Government of India IT security guidelines including provisions of:
  - The Information Technology Act, 2000” and amendments thereof and
  - Guidelines and advisories for information security published by Cert-In/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.
- d. While writing the source code for application modules the SI should ensure high-quality documentation standards to improve the readability of the software module. An illustrative list of comments that each module contained within the source file should be preceded by is outlined below:
  - The name of the module
  - The date when module was created
  - A description of what the module does
  - A list of the calling arguments, their types, and brief explanations of what they do

- A list of required files and/or database tables needed by the module
  - Error codes/Exceptions
  - Operating System (OS) specific assumptions
  - A list of locally defined variables, their types, and how they are used
  - Modification history indicating who made modifications, when the modifications were made, and what was done.
- e. Apart from the above SI needs to follow appropriate coding standards and guidelines inclusive of but not limited to the following while writing the source code -
- Proper and consistent indentation
  - Inline comments
  - Structured programming
  - Meaningful variable names
  - Appropriate spacing
  - Declaration of variable names
  - Meaningful error messages
- f. Quality Audits
- CSCL at its discretion, may also engage independent auditors to audit any/some/all standards/processes. The SI shall support all such audits as per calendar agreed in advance. The result of the audit shall be shared with the SI who has to provide an effective action plan for mitigations of observations/non-compliances, if any.

## 2.1.5 Section 1- Training & Capacity Building

The proposed CCC solution is very different from the existing system and hence necessary change management workshop/awareness camps have to be conducted for the field level staff and for the officials. The SI shall prepare the necessary content and conduct the change management workshop for the staff and the officers in batches. The selected System Integrator would be required to provide training on various aspects to enable effective use of the new system to achieve the envisaged outcomes.

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:
  - ✓ *Employees of CSCL of Chennai Smart City*
  - ✓ *Municipal Corporations' employees*
  - ✓ *Stakeholder departments*
2. The SI's scope of work also includes preparing the necessary documentation and aids required for successful delivery of such trainings.
3. The details provided in this section are indicative and due to the complex nature of the project the number of training sessions may increase. Over and above the team considered for performing the training as detailed in subsequent sections,
4. Further the SI has to provide cost for additional and optional training sessions in its Financial proposal in case more training's are required. SI has to conduct such additional training sessions on City SPV's request.
5. SI will develop a training and capacity building strategy that will also include a detailed plan of implementation. SI should have comprehensive hands on system training strategy and schedule for users doing Smart Datacenter and ICCC Operations.
6. SI will get the Training and capacity building strategy including training material finalized with City SPV before starting the training programs.
7. SI will prepare all the requisite audio/visual training aids that are required for successful completion of the training for all stakeholders. These include the following for all the stakeholders:
  - a. Training manuals for City SPV employees / stakeholder departments such as Municipal Corporation, Police, and Electricity Board etc.
  - b. Computer based training modules
  - c. Video (recorded sessions) for ICCC operations, back end modules, business intelligence, dynamic reporting
  - d. Presentations e. User manuals
  - e. Operational and maintenance manuals for the ICCC modules
  - f. Regular updates to the training aids prepared under this project
8. SI must plan all the training and its material keeping defined and agreed SOPs of ICCC as prime focus.
9. SI will maintain a copy of all the training material on the knowledge Portal and access will be provided to relevant stakeholders depending on their need and role. The access to

training on the portal would be finalized with City SPV. SI has to ensure the following points:

- a. For each training session, the SI has to provide the relevant training material copies to all the attendees.
  - b. The contents developed shall be the property of CSCL / City SPV with all rights.
10. There are estimated 250 batches (with 20 trainee per batch) who need to be trained. SI may accordingly plan the training budget.
11. SI has to ensure that the training sessions held are effective and that the attendees would be able to carry on with their work efficiently. For this purpose, it is necessary that the effectiveness of training sessions is measured. The SI will prepare a comprehensive feedback form that will capture necessary parameters on measuring effectiveness of the training sessions. This form will be discussed and finalized with City SPV.
12. After each training session, feedback will be sought from each of the attendees on either printed feedback forms or through a link available on the web portal. One member of the stakeholder group would be involved in the feedback process and he/she has to vet the feedback process. The feedback received would be reported to City SPV for each training session.
13. For each training session, the SI 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 threshold score to be decided by authority.

**i. Preparation of Training material**

- a) Training Plan: The selected System Integrator would be required to prepare a detailed training plan covering atleast the trainings to be conducted, targeted audience, location, dates for training, duration and training content. The training plan would be submitted to the Department as per timelines mentioned in this RFP for feedback and approval from the Department.
- b) Training Materials: The following minimum training materials will be required to be prepared by the selected System Integrator to facilitate the training of users:

Method of training	Brief description	Training Artifacts	Languages of Training Material
Class room training (Hands-on training)	This approach can be adopted for departmental users.	<ul style="list-style-type: none"> <li>• IT infrastructure and dummy data for hands-on training</li> <li>• Participant handouts</li> <li>• Online and Paper-based</li> </ul>	<ul style="list-style-type: none"> <li>• English</li> <li>• Tamil</li> </ul>

Method of training	Brief description	Training Artifacts	Languages of Training Material
		<p>tests to evaluate the quality of learning and Training</p> <ul style="list-style-type: none"> <li>• Provision for online and paper-based feedback submission</li> </ul>	
Self learning	<p>This will be useful for both the departmental users and for citizens to learn system operations in the new application. This would include several self learning methods for enablement of easy learning and adoption of the system by the departmental users and citizens</p>	<ul style="list-style-type: none"> <li>• Downloadable Computer Based toolkits, PPTs and videos on system operations and usage</li> <li>• FAQs</li> <li>• Online help modules with search by keywords, topic etc.</li> <li>• Online tests that may be taken up by the participant after completing the learning to evaluate his learning</li> <li>• Online forms to submit feedback on the quality of training material</li> </ul>	<ul style="list-style-type: none"> <li>• English</li> <li>• Tamil</li> </ul>

Approval for training materials prepared should be obtained from the authority **at least 2 weeks** before delivery of the training program.

## ii. Training Programs



The selected System Integrator would be required to conduct the following Training programmes.

#	Typical Target Audience	Min. of Batches
1	Functional Training (batch of 20 trainees per batch)	200
2	Administrative Training batches	10
3	Sr. Management Training Batches	10
4	Project Management/Coordination during implementation	12

Maximum number of participants per Batch: 20

Please note that the selected System Integrator would have to plan for training programs in various locations in line with the proposed implementation plan. For instance, the selected System Integrator would have to make arrangements for completing training for the targeted number of users at the pilot location before the pilot rollout so as to facilitate evaluation of all aspects of the Project.

### iii. Training Assessment and Collection of Feedback

All users who have undergone the training provided by the selected System Integrator would be assessed. As part of training assessment, Department would perform the following:

- Design forms for gathering feedback on the training course and satisfaction level of trained participants. The feedback would be aimed at gathering participant inputs on parameters including course coverage and its relevance, quality of presentation, quality of training material provided, relevant examples / practice sessions, quality of faculty, logistics for the training, etc.
- Supervising conduct of training exams with the help of SI manpower
- Evaluation of exams by the Department or its appointed Third Party Agency with support from the selected System Integrator.

The selected System Integrator's responsibilities as part of training assessment are as follows:

- Develop computer-based tests for evaluation of training and collecting training feedback. Details of the parameters for tests / feedback, duration of tests, specific questions etc will be discussed with the selected System Integrator during the implementation stage.
- Incorporate the feedback to improve the Training Materials and Methods

### iv. Space and Physical Infrastructure

- The space required to conduct training will be provided by the Department. The training space provided will be furnished with seating arrangement and a machine per participant for hands-on Training. The selected System Integrator may provide

anything over and above this, as may be deemed fit to meet the training requirements of this Project.

**v. Staffing and Training**

The selected System Integrator must ensure that:

- deployed trainers possess needed skills and experience in the specific domains and are fully aware of the deployed systems and have a prior experience of training personnel in the Government sector
- deployed trainers should be fluent in speaking and writing in English and Tamil

**vi. Other arrangements**

- The training environment where users are provided hands-on training should be exact replica of the live application allowing entry of dummy data etc. Any additional infrastructure required for this may be budgeted for by the Bidder in the Price Bid. The Bidder may provision for this Training environment separately or may provision to use the Test environment for the purpose of delivery hands-on training to Departmental Staff. This training environment will be handed over to the Authority along with all other assets at the end of Contract Period.
- Arrangements for travel/boarding/lodging for the training instructors and supporting staff at all designated locations across the state would be done by the selected System Integrator at no additional cost.

### **2.1.6 Solution Stabilization & Go-Live**

After the successful demonstration of the Final Acceptance Testing of CCC solution (hardware & software), the solution is put for reliability, consistency & accuracy test for period of one month. During this stabilisation period, the CCC solution shall successfully comply to the minimum Service Levels Prescribed.

During the Stabilisation period the authority through designated agency shall assess the compliance to the SLA on a periodic basis.

Upon on satisfactory compliance the prescribed Service Levels for continuous period of 10 days, the CCC solution shall be ready to be LIVE. Subsequently a mutually agreeable Go-Live date taking into consideration number residual days left in the month when the CCC is declared ready for Go-Live.

## **2.2 Overview of Phase II**

The System Integrator shall operate, maintain and manage all the smart city solution on 24x7 basis over a period of five years from the date of issue of commissioning certificate.

### **2.2.1 Detailed Phase-II Requirements**

The SI shall provide Operation, Maintenance and Management services ( phase II services) for the Smart City solution commissioned for a period of 5 years from the date of issue of Commissioning Certificate as per the Service Level Agreement (SLA) and as per the scope , terms & conditions in the tender.

The phase II services to be provided is as given below, but not limited to:

The phase II services to be provided as per the approved phase II requirements. During the phase II operation, the department reserves the right to amend the tasks as per requirement. The phase II services shall cover the services to be provided through the help desk, at the CCC and DC and maintenance of all the smart applications.

### **2.2.2 Section 1- Operation & Maintenance Services**

#### **2.2.2.1 Post Implementation Services**

Success of the Project would lie on how professionally and methodically the entire Project is managed once the implementation is completed. From the Systems Integrator perspective too this is a critical phase since the quarterly payments are linked to the SLA's in the post implementation phases. System Integrator thus is required to depute a dedicated team of professionals to manage the Project and ensure adherence to the required SLAs.

#### **2.2.2.2 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 Near DR backup testing through regular mock drills

### **2.2.2.3 Provision of the Operational Manpower to view the feeds at Command & Control Center**

Authority may ask the System Integrator to provide suitable manpower to monitor the feeds at Command and Control Center and support Authority in operationalisation of the Command and Control Center. The exact role of these personnel and their responsibilities would be defined and monitored by Authority personnel. System Integrator shall be required to provide such manpower meeting following requirements:

- All such manpower shall be minimum graduate pass
- All such manpower shall be without any criminal background / record.
- Authority reserves the right to carry out background check of the personnel proposed on the Project for verification of criminal record, at the beginning of deployment or during deployment.
- System Integrator shall have to replace any person, if not found suitable for the job.

All the manpower shall have to undergo training from the System Integrator for at least 15 working days on the working of Command and Control Center. Training should also cover dos & don'ts and will have few.

- Sessions from Authority officers on right approaches for monitoring the feeds & providing feedback to Police Personnel / Surveillance System and other smart components .
- Each person shall have to undergo compulsory 1 day training every month
- Operational Manpower shall work in 3 shifts, with no person being made to see the feeds for more than 8 hours at a stretch.

Detail operational guideline document shall be prepared during implementation which shall specify detail responsibilities of these resources and their do's & don'ts.

Authority reserves the right to include or exclude this scope of providing operational manpower in the Project scope or include it partly at the time of signing of the contract or during execution of the contract.

## **2.2.3 Section 2- Facility Management Services**

### **2.2.3.1 Helpdesk and Facilities Management Services**

The Successful Bidder will be required to establish the helpdesk and provide facilities management services to support the Authority officials in performing their day-to-day functions related to this system.

The Successful Bidder shall setup a central helpdesk dedicated (i.e. on premise) for the Project, which shall be supported by their field units, proposed to be setup at Command & Control Center. Providing helpdesk/support services from a shared facility of any other party/provider is not permitted. Central Helpdesk can be set up at the Command and Control Center.

Functional requirements of the helpdesk management system, fully integrated with the enterprise monitoring and network management system. The system will be accessed by the Authority officials for raising their incidents and logging calls for support. The detailed service levels and response time, which the Successful Bidder is required to maintain for provisioning of the FMS services are described in the Service Level Agreement of this Tender. Systems Integrator is also required to depute a dedicated, centralised project management & technical team for the overall Project management and interaction with Sr. Police Dept. personnel.

### **2.2.3.2 Application Monitoring and Administration**

- Monitoring all the smart applications on a day-to-day basis to ensure application availability and reliability.
- Monitor application to ensure that the application does not suspend, hang etc.
- Monitor components, including but not limited to, Application servers, Web Servers, Middleware and other application servers on an ongoing basis to ensure smooth functioning of the applications.
- Expertise in the application to have the ability to troubleshoot problems, monitor erratic behavior through the application logs
- Configuration reviews to isolate bottlenecks and bring out parameters affecting the performance.
- Performance monitoring of the application and facilitating performance tuning.
- Maintenance of application response time logs.
- Manage patch upgrade as and when required with minimal downtime.
- Ensure configuration management and backups of patch to facilitate rollback in case of problems.

### **2.2.3.3 Managed Services**

Managed Services shall include a range of services related to the infrastructure services at the CCC, DC & near DR, helpdesk services and management of all the smart applications. Following services shall form a part of managed services:

#### **2.2.3.4 Help Desk & SLA Management Services**

The help desk service will serve as a single point of contact for all incidents and service requests. The service will provide a Single Point of Contact (SPOC) and also escalation / closure of incidents for the end users such as at the CCC, DC & DR& other concerned department officials, field locations and citizens. The activities shall include:

- Provide Help Desk facility during agreed service period window for end users.
- Provide necessary channels for reporting issues to the help desk. The incident reporting channels could be the following:
  - Specific E-Mail account
  - Telephone Line (toll free)
  - Portal
- Implement a call logging system in line with the severity levels as per the SLAs. The Help desk shall log user calls and assign an incident/ call ID number. Severity shall be assigned to each call as per the SLAs.
- Creation of knowledge base on frequently asked questions to assist the end users in resolving the issues.
- Track each incident / call to resolution
- Escalate the calls, to the appropriate levels, if necessary as per the escalation matrix.
- Analyze the incident / call statistics and provide periodical reports(daily/weekly/monthly/quarterly) including but not limited to:
  - Type of incidents / calls logged
  - Incidents / calls resolved
  - Incidents / calls open

Automatic generation of customized Periodical SLA reports as per requirement.

#### **2.2.3.5 Monitoring and Management Services**

The system integrator shall provide the following monitoring and management services at the DC and CCC and for the help desk.

- Server Monitoring, Administration & Management Services
- Database Administration & Management Services
- Storage Administration & Management Services
- Backup & Restore Services
- Security Administration Services.

#### **2.2.3.6 Server Monitoring, Administration & Management Services**

The activities shall include but not limited to:

- Configuration of server parameters, operating systems administration and tuning.

- Operating system administration, including but not limited to management of users, processes, resource contention, preventive maintenance and management of updates & patches to ensure that the system is properly updated.
- Re-installation in the event of system crash/failures.
- Maintenance of a log of the performance monitoring of servers including but not limited to monitoring CPU, disk space, memory utilization, I/O utilization, etc.
- Event log analysis generated in all the sub systems including but not limited to servers, operating systems, databases, applications, security devices, messaging, etc. Ensuring that the logs are backed up and truncated at regular intervals.
- Periodic health check of the systems, troubleshooting problems, analysing and implementing rectification measures.
- Identification, diagnosis and resolution of problem areas and maintenance of assured SLA levels.
- Implementation and maintenance of standard operating procedures for maintenance of the infrastructure.
- Management of the user names, roles and passwords of all the relevant subsystems, including, but not limited to servers, applications, devices, etc.
- System administration activities shall include tasks including but not limited to setting up the servers, executing hardware and software updates when necessary.

#### **2.2.3.7 Database Administration & Management Services**

The activities shall include but not limited to:

- End-to-end management of database on an ongoing basis to ensure smooth functioning of the same.
- Management of changes to database schema, disk space, storage, user roles.
- Conduct code and configuration reviews to provide tuning inputs to the State / User Department in order to improve the application performance or resolve bottlenecks if any.
- Performance monitoring and tuning of the databases on a regular basis including, preventive maintenance of the database as required.
- Management of database upgrade or patch upgrade as and when required with minimal downtime.
- Regular backups for all databases in accordance with the backup and archive policies and conduct recovery whenever required with appropriate permissions

#### **2.2.3.8 Storage Administration & Management Services**

The activities shall include but not limited to:

- Installation and configuration of the storage system.
- Management of storage environment to maintain performance at desired optimum levels.



- Development of storage management policy, configuration and management of disk array, SAN fabric / switches, NAS, tape library, etc.
- Configuration of SAN shall include activities such as management of storage space, volume, RAID configuration, LUN, zone, security, business continuity volumes, NAS, performance, etc.

### **2.2.3.9 Backup and Restore Services**

The activities shall include but not limited to:

- Backup of operating system, database and application as per stipulated policies.
- Monitoring and enhancement of the performance of scheduled backups, schedule regular testing of backups and ensure adherence to related retention policies.
- Ensuring prompt execution of on-demand backups of volumes, files and database applications whenever required by department or in case of upgrades and configuration changes to the system.
- Real-time monitoring, log maintenance and reporting of backup status on a regular basis. Prompt problem resolution in case of failures in the backup processes.
- Media management including, but not limited to, tagging, cross-referencing, storing, logging, testing, and vaulting in fire proof cabinets.
- Physical security of the media stored in cabinets.
- Ongoing support for file and volume restoration requests
- A backup of all transactions shall be done so that in case any disaster / emergency at Datacenter the Near DR will have all the data.
- SI shall be responsible for supply, install, test & commission of the backup storage of the archival of data.

### **2.2.3.10 Security Administration Services**

The activities to be carried out under security administration shall include but not limited to:

- Addressing the ongoing needs of security management including, but not limited to, monitoring of various devices / tools such as firewall, intrusion detection, content filtering and blocking, virus protection, and vulnerability protection through implementation of proper patches and rules.
- Root domain administration by creating the root and sub-domains and setting the root level security policies such as authentication mechanisms (single/multi factor), password policies such as password length, password complexity, password expiry, account lockout policy, certificate policies, IPSEC policies etc.
- Maintaining an updated knowledge base of all the published security vulnerabilities and virus threats for related software and microcode etc.
- Ensuring that patches / workarounds for identified vulnerabilities are patched / blocked immediately.

- Respond to security breaches or other security incidents and coordinate with respective OEM in case of a new threat is observed to ensure that workaround / patch is made available for the same.
- Provide a well-designed access management system, security of physical and digital assets, data and network security, backup and recovery etc.
- Maintenance and management of security devices, including, but not limited to maintaining firewall services to restrict network protocols and traffic, detecting intrusions or unauthorized access to networks, systems, services, applications or data, protecting email gateways, firewalls, servers, from viruses.
- Ensuring that the security policy is maintained and updates to the same are made regularly as per ISO 270001, ISO 20000 and BS 15000 guidelines

### **2.2.3.11 Network management & Monitoring Services**

The activities shall include but not limited to:

- The system integrator shall ensure the management of network environment to maintain performance at optimum levels on a 24 x 7 basis.
- The system integrator shall monitor and administer the network connectivity provided for the help desk, connectivity at the DC, CCC, near DR and field locations.
- The system integrator shall create and modify VLAN, assignment of ports to appropriate application traffic.

### **2.2.3.12 Change Management**

- Tracking the changes in hard / soft configurations, changes to applications, changes to policies, applying of upgrades / updates / patches, etc.
- Plan for changes to be made - draw up a task list, decide on responsibilities, coordinate with all the affected parties, establish and maintain communication between parties to identify and mitigate risks, manage the schedule, execute the change, ensure and manage the port change tests and documentation.
- SI shall be responsible for making any changes demanded by CSCL anytime during the contract period. The SI needs to adequately plan & deploy to carry out the change in the agreed timeline without any additional charge
- In case of any additional requirement which mandates additional developmental activities in any of the smart application then SI shall do the same as per requirements of CSCL without any additional charge. Therefore SI to plan to deploy adequate programmers during the Phase II – Operation & Maintenance phase as well.

### **2.2.3.13 Change request**

The system Integrator shall ensure that the change requests for any of the smart components (Hardware / Software) are deployed after carrying out the following technical tasks to ensure smooth roll out of the change request.

- Functional Testing: Ensuring that the Hardware/ Software functionality meets the functional and technical requirement of the project.
- Performance Testing: Ensuring that the Hardware/ Software meets expressed performance requirements.
- Security Testing: Testing for exploitable application security weaknesses that undermine the application security or the security of the infrastructure.

#### **2.2.3.14 Periodic Security and Performance Testing & conformance**

SI shall conduct Security and Performance testing by the CERT-IN empanelled TPA (preferred to use the same TPA) agency approved by CSCL. Any approved Change Request in any of the smart components (Hardware/ Software) would call for Vulnerability, security & performance audit. The SI shall also plan for half-yearly basis conduct an

- Audit of application vulnerability
- Security for both application & compute
- Performance load testing for application & network connectivity assessment

In case of any degradation identified in this periodic assessment the SI needs to highlight proactive measures to mitigate the same. Any Non-conformance & vulnerability aspects identified by the TPA during this exercise need to be immediately mitigated & closed before 2 weeks of succeeding quarter. In case of any default there would penalty levied as per SLA & Tender conditions

#### **2.2.3.15 SLA monitoring**

The Service Level mentioned in these tender needs to be captured, analyzed & reported to the CS&CP Department. The consultant & department nodal officers shall review the SLA reports & ratify the same on a quarterly basis. Based on the ratification SLA/performance report the payments would be estimated i.e. after deducting any penalties and the same would be released to SI.

#### **2.2.4 Section 3- Knowledge Transfer & Exit Management**

- i. This sets out the provisions, which will apply on expiry or termination of the Master Service Agreement, the Project Implementation, Operation and Management SLA.
- ii. 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.
- iii. The Parties shall ensure that their respective associated entities carry out their respective obligations set out in this Exit Management Schedule.

#### **2.2.4.1 Cooperation and Provision of Information**

During the exit management period:

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

#### **2.2.4.2 Confidential Information, Security and Data**

- i. The SI will promptly on the commencement of the exit management period supply to the CSCL or its nominated agency the following:
  - Information relating to the current services rendered and customer and performance data relating to the performance of sub-contractors in relation to the services;
  - Documentation relating to Intellectual Property Rights;
  - Documentation relating to sub-contractors;
  - All current and updated data as is reasonably required for purposes of CSCL or its nominated agencies transitioning the services to its Replacement SI in a readily available format nominated by the CSCL or its nominated agency;
  - All other information (including but not limited to documents, records and agreements) relating to the services reasonably necessary to enable CSCL or its nominated agencies, or its Replacement SI to carry out due diligence in order to transition the provision of the Services to CSCL or its nominated agencies, or its Replacement *System integrator* (as the case may be).
- ii. Before the expiry of the exit management period, the SI shall deliver to the CSCL or its nominated agency all new or up-dated materials from the categories set out in Schedule above and shall not retain any copies thereof, except that the SI shall be permitted to retain one copy of such materials for archival purposes only.

#### **2.2.4.3 Knowledge Transfer of Certain Agreements**

On request by the CSCL or its nominated agency the SI shall effect such assignments, transfers, licences and sub-licences CSCL, or its Replacement SI in relation to any equipment lease, maintenance or service provision agreement between SI and third party

lessors, vendors, and which are related to the services and reasonably necessary for the carrying out of replacement services by the CSCL or its nominated agency or its Replacement SI.

#### **2.2.4.4 General Obligations of the SI**

- i. The SI shall provide all such information as may reasonably be necessary to effect as seamless a handover as practicable in the circumstances to the CSCL or its nominated agency or its Replacement SI and which the SI has in its possession or control at any time during the exit management period.
- ii. For the purposes of this Schedule, anything in the possession or control of any SI, associated entity, or sub-contractor is deemed to be in the possession or control of the SI.
- iii. The SI shall commit adequate resources to comply with its obligations under this Exit Management Schedule.

#### **2.2.4.5 Exit Management Plan**

- i. The SI shall provide the CSCL or its nominated agency with a recommended exit management plan ("Exit Management Plan") which shall deal with at least the following aspects of exit management in relation to the MSA as a whole and in relation to the Project Implementation, and the Operation and Management SLA.
  - A detailed program of the transfer process that could be used in conjunction with a Replacement SI including details of the means to be used to ensure continuing provision of the services throughout the transfer process or until the cessation of the services and of the management structure to be used during the transfer;
  - Plans for the communication with such of the SI's sub-contractors, staff, suppliers, customers and any related third party as are necessary to avoid any material detrimental impact on the CSCL's operations as a result of undertaking the transfer;
  - (If applicable) proposed arrangements for the segregation of the SI's networks from the networks employed by CSCL and identification of specific security tasks necessary at termination;
  - Plans for provision of contingent support to CSCL, and replacement SI for a reasonable period after transfer.
- a. The SI shall re-draft the Exit Management Plan annually thereafter to ensure that it is kept relevant and up to date.
- b. Each Exit Management Plan shall be presented by the SI to and approved by the CSCL or its nominated agencies.
- c. The terms of payment as stated in the Terms of Payment Schedule include the costs of the SI complying with its obligations under this Schedule.
- d. In the event of termination or expiry of MSA, and Project Implementation, each Party shall comply with the Exit Management Plan.
- e. During the exit management period, the SI shall use its best efforts to deliver the services.

- f. Payments during the Exit Management period shall be made in accordance with the Terms of Payment Schedule.
- g. This Exit Management plan shall be furnished in writing to the CSCL or its nominated agencies within 90 days from the Effective Date of this Agreement.

### 3 Section 3- Service Level Agreements

- Service Level Agreement (SLA) shall become the part of contract between Authority and the successful bidder. SLA defines the terms of the successful bidder's responsibility in ensuring the timely delivery of the deliverables and the correctness of the same based on the agreed Performance Indicators as detailed in this section.
- The successful bidder has to comply with service level requirements to ensure adherence to project timelines, quality and availability of services, throughout the period of this contract i.e. during implementation phase and for a period of five (5) years. The successful bidder has to supply appropriate software/hardware/automated tools as may be required to monitor and submit reports of all the SLAs mentioned in this section.
- For purposes of the SLA, the definitions and terms as specified in the document along with the following terms shall have the meanings set forth below:
  - "Total Time" - Total number of hours in the quarter (or the concerned period) being considered for evaluation of SLA performance.
  - "Uptime" – Time period for which the specified services/ outcomes are available in the period being considered for evaluation of SLA. Formulae for calculation of Uptime: 
$$\text{Uptime (\%)} = \{1 - [(\text{Downtime}) / (\text{Total time} - \text{scheduled maintenance time})]\} * 100$$
  - "Downtime"- Time period for which the specified services/ components/ outcomes are not available in the concerned period, being considered for evaluation of SLA, which would exclude downtime owing to Force Majeure & Reasons beyond control of the successful bidder.
  - "Scheduled Maintenance Time" - Time period for which the specified services/ components with specified technical and service standards are not available due to scheduled maintenance activity. The successful bidder is required to take at least 10 days prior approval from Authority for any such activity. The scheduled maintenance should be carried out during non-peak hours (like post mid-night, and should not be for more than 4 hours. Such planned downtime would be granted max 4 times a year.
- "Incident" - Any event / abnormalities in the service being rendered, that may lead to disruption in normal operations and services to the end user.
- "Response Time" - Time elapsed from the moment an incident is reported in the Helpdesk over phone or by any applicable mode of communication, to the time when a resource is assigned for the resolution of the same.
- "Resolution Time" - Time elapsed from the moment incident is reported to Helpdesk either in person or automatically through system, to the time by which the incident is resolved completely and services as promised are restored.

### 3.1.1 Implementation SLAs

- These SLAs shall be used to evaluate the timelines for completion of deliverables that are listed in the deliverable.

Delay (Weeks)	Penalty (INR)
For every one week of delay upto 12 weeks for Go-Live Date	0.1% of total CAPEX of Section 1 of the Price Bid.
For every one week of delay beyond 12 weeks from Go-Live Date	0.2% of total CAPEX of Section 1 of the Price Bid. Subject to total cumulative penalty capped at 10% of CAPEX

- In case the penalties for the selected bidder reaches 10% of the CAPEX value in the form of penalty, cumulative of penalties for all smart elements, at any point of time during the duration of pre- implementation phase, GCC reserves the right to invoke the termination clause.

### 3.1.2 Operation & Maintenance SLAs

- These SLAs shall be used to evaluate the performance of the services on quarterly basis.
- Penalty levied for non- performance as per SLA requirements shall be deducted through subsequent payments due from Authority.
- The upper limit of penalty would be capped at 10% of the OPEX value for each quarter. In case the calculated penalty crosses 10% penalty of the OPEX value in 2 subsequent quarters, GCC reserves the right to invoke the termination clause.
- Uptime definition: All devices have to be working and deliver the desired results. The no. of hours that the particular device/ equipment does not work will be treated as down time. Uptime shall be calculated as  $Uptime (\%) = \{1 - [(Downtime) / (Total time - scheduled maintenance time)]\} * 100$ . For ex, if 10 nos. of Sensors for Digital display are deployed at various locations, and 2 device/ units does not work for 5 Hrs, the total non-working device hours will be 10 unit hours ( and the uptime would be  $\{1 - (10 / (10 * 90 * 24))\}$ , 10 being the number of units, for 90 days on 24 hours basis.
- The penalties would be levied for every unit down time hour.



**3.1.2.1 SLA and Penalty for Helpdesk Response and Resolution time**

In any circumstances the total cumulative penalty derived from SLA non-compliances that may be levied on the SI shall be capped to 10% of OPEX of Section I of Price Bid.

#	Location	SLA applicabilityE	SLA parameter & Penalty (Quarterly basis)																
1	CCC Services measured through Help desk tool	<p><b>Critical :</b> Availability/functionality of all the hardware, software, network connectivity, Portal, CCC Solution Smart Component, that is deployed by the SI.</p> <p><b>Non critical :</b> Performance issues of all the hardware/software/network connectivity/ CCC Solution /Portal that are deployed by the SI</p> <p><b>Reference hours :</b> 24x7x365</p> <p><b>Note:</b> The critical and Non critical SLA parameters will be firmed up by the department in consultation with the SI.</p>	<p><b>Critical:</b></p> <table border="1"> <thead> <tr> <th>Uptime</th> <th>Penalty (%)</th> </tr> </thead> <tbody> <tr> <td>&gt; 99.5 %</td> <td>Nil</td> </tr> <tr> <td>&gt;98.5% &amp; less than 99.5%</td> <td>0.1% on the OPEX payable</td> </tr> <tr> <td>For Every 0.5% drop from &lt;98.5%</td> <td>Additional 0.2% on the OPEX payable</td> </tr> </tbody> </table> <p><b>Non-Critical:</b></p> <table border="1"> <thead> <tr> <th>Uptime</th> <th>Penalty (%)</th> </tr> </thead> <tbody> <tr> <td>&gt; 95 %</td> <td>Nil</td> </tr> <tr> <td>&gt;90% &amp; less than 95%</td> <td>0.02% on the OPEX payable</td> </tr> <tr> <td>For Every 1% drop from &lt;90%</td> <td>Additional 0.04% on the OPEX payable</td> </tr> </tbody> </table>	Uptime	Penalty (%)	> 99.5 %	Nil	>98.5% & less than 99.5%	0.1% on the OPEX payable	For Every 0.5% drop from <98.5%	Additional 0.2% on the OPEX payable	Uptime	Penalty (%)	> 95 %	Nil	>90% & less than 95%	0.02% on the OPEX payable	For Every 1% drop from <90%	Additional 0.04% on the OPEX payable
Uptime	Penalty (%)																		
> 99.5 %	Nil																		
>98.5% & less than 99.5%	0.1% on the OPEX payable																		
For Every 0.5% drop from <98.5%	Additional 0.2% on the OPEX payable																		
Uptime	Penalty (%)																		
> 95 %	Nil																		
>90% & less than 95%	0.02% on the OPEX payable																		
For Every 1% drop from <90%	Additional 0.04% on the OPEX payable																		

**3.1.2.2 SLA for Business Continuity Planning**

#	Parameter	Metric	Frequency	Penalty
1.	Data Loss	Near to zero	At all times	> for loss of every 0.5 MB of data 0.15% on the OPEX payable capped to 10% OPEX
2.	Returning to Business-as-usual	RTO = 1 minute	At all times	> for loss of every 0.5 minute delay of RTO above the 1 minute 0.15% on the OPEX payable capped to 10% OPEX

## 3.1.2.3 SLA for Change Requests or enhancements

#	Parameter	Metric	Frequency	Penalty
1	Criticality of Change – <b>Low</b>	< T, where T is the timeframe for completion of the Change request as agreed upon by Authority and successful bidder	Weekly per Occurrence	1 % of change request value per week for the first two weeks for each occurrence, 2 % of change request value per week for every subsequent week, subject to a maximum of 10% post which Authority may invoke termination clause of the contract.
2	Criticality of Change – <b>Medium</b>	< T, where T is the timeframe for completion of the Change request as agreed upon by Authority and successful bidder	Weekly per Occurrence	1.5 % of change request value per week for the first two weeks for each occurrence, 2.5 % of change request value per week for every subsequent week, subject to a maximum of 10% post which Authority may invoke termination clause of the contract.
3	Criticality of Change – <b>High</b>	< T weeks, where T is the timeframe for completion of the Change request as agreed upon by Authority and successful bidder	Weekly per Occurrence	2 % of change request value per week for the first two weeks for each occurrence, 3 % of change request value per week for every subsequent week, subject to a maximum of 10% post which Authority may invoke

#	Parameter	Metric	Frequency	Penalty
				termination clause of the contract.
4	Resource Replacement	Within 7 days of exit of resource (in case of Authority initiated or supplier initiated)	Per Occurrence	Rs. 5,000 per day for unapproved non-availability of resource
5	Application Security	Cyber Crime / Hacking / Data Theft / Fraud attributable to the service provider	Per Occurrence	Depending on the type of incident and its impact, a Penalty of 10% on the entire contract value or in case of severe issue (as defined by Authority) such breach may lead to termination clause of contract

#### 3.1.2.4 Definitions:

- Severity 1: Command and Control Center or e-Governance or Smart City applications down for more than 70% users.
- Severity 2: Command and Control Center or e-Governance or Smart City applications down for more than 30% users.
- Severity 3: Modules of Command and Control Center or e-Governance not functional for users.
- Severity 4: Minor functionality issues with Command and Control Center or e-Governance or Smart City applications
- Response Time: Response time is defined as the time the support vendor takes to respond from the time that ticket was raised.
- Resolution Time: Resolution time is defined as the time the vendor takes to resolve the issue or provide acceptable workaround for the issue.

#### 3.1.2.5 Conditions for No Penalties

Penalties shall not be levied on the Bidder in the following cases:

- There is a force majeure event effecting the SLA which is beyond the control of the successful bidder. Force Majeure events shall be considered in line with the clause mentioned RFP.
- The non-compliance to the SLA has been due to reasons beyond the control of the successful bidder.
- Theft cases by default/ vandalism would not be considered as “beyond the control of bidder”. Hence, the Bidder should be taking adequate anti-theft measures, spares strategy, Insurance as required to maintain the desired Required SLA.

## 4 Project Implementation Timelines

The implementation timelines for the project components are as given below.

T = Date of signing of Contract Agreement

G= Go-Live Date

#	Payment Milestone	Timelines
1	Letter of Acceptance (LoA)	T
2	Inception Report	T + 15 days
3	CCC Solution Design Sign-off	T + 45 days
4	Supply & Installation of all IT & Non-IT Infrastructure, at CommandCommunications Center	T+150 Days
5	Pre-Acceptance Testing by SI & OEM as per approved Test Cases and submitting Readiness request for carrying out Final Acceptance Testing	T+210 Days
5	Final Acceptance Testing of the CCC Solution sign-off	T+240 Days
6	CCC Solution stabilization	G =T + 300 Days
7	Go-Live	
8	Commencement of Operations & Maintenance Phase for a period of 5 years	G+20Quarters
9	Project Closures Exit Management	G+ 20th Quarter

## 5 Functional & Technical Specifications

### 5.1 Command and Control Center (CCC)

#### 5.1.1 Objectives

- 1) The vision of the Command and Control Center (CCC) is to have an integrated view of all the smart initiatives undertaken by Authority with the focus to serve as a decision support engine for city administrators in day-to-day operations or during exigency situations. This dynamic response to situations, both pre-active and re-active will truly make the city operations “SMART”.
- 2) Command and Control Center (CCC) involves leveraging on the information provided by various departments and providing a comprehensive response mechanism for the day-to-day challenges across the city. CCC shall be a fully integrated solution that provides seamless incident – response management, collaboration and geo-spatial display.
- 3) CCC shall facilitate the viewing and controlling mechanism for the selected field locations in a fully automated environment for optimized monitoring, regulation and enforcement of services. The smart city operations center shall be accessible by operators and concerned authorized entities with necessary authentication credentials.
- 4) Various smart elements are able to use the data and intelligence gathered from operations of other elements so that civic services are delivered lot more efficiently and in an informed fashion.
- 5) Command & Control Center should be able to integrate with various Utility systems such as Water/SCADA, Power, GIS, ITMS, Sewerage/ Drainage system, Disaster Mgmt. System etc.

#### 5.1.2 Proposed Components of CCC Solution

- Event Management System
- Flood / Tsunami / Cyclones Modelling System
- Incident Management System
- Alerting System
- Unified Communications & Contact Center
- Radio & Communication Systems
- Video Display System
- Social Media System
- Logging Solution for Voice, Video & Radio
- Debriefing module
- Mobile engine

### 5.1.3 Functional Specifications

#### 5.1.3.1 Functional Specifications of the Application Software

Various functional requirements of the CCC application System are given in the table below:

#	Functions	Minimum Specifications
1.	Solution & Platform	The Command & Control solution should be implemented and complied to the industry open standards based Commercial-of-the-shelf (COTS) products.
2.		<p>The CCC shall embody the following characteristics:</p> <ol style="list-style-type: none"> <li>1. Client/server architecture</li> <li>2. Support multi-site, multiple-hierarchy deployment</li> <li>3. Provide clear scalability</li> <li>4. Central administration capability</li> <li>5. Support local redundancy and high availability options</li> <li>6. Employ encrypted communications over TCP/IP LAN's and WAN's</li> <li>7. Capable of running in a virtual environment</li> <li>8. Provide a mechanism to define key performance indicators, trends, leading indicators and visualize the indicators on a web based configurable dashboard infrastructure</li> <li>9. Provide a mobile portal to allow viewing of incidents and relevant details</li> <li>10. Display a configurable indication of overall situation threat level</li> <li>11. Provide communication capability to include email, text, telephone, intercom, mass notification, and application-based messages</li> <li>12. Support a mobile app for field personnel, which enables its users to receive incident details (including: tasks, forms, photos) and a comprehensive set of GIS capabilities, to ensure collaborative response aligned with the control room's operator</li> <li>13. Support mobile app for Chennai citizens who can register themselves after downloading the app on iOS or Android phones and then share incident related videos, text, photos etc. To the command center</li> <li>14. Support the simulation of events, such as alarms, for training purposes.</li> </ol>
3.		Software (Application, Database and any other) must not be restricted by the license terms of the OEM from scaling out on unlimited number of cores and servers during future expansion.

#	Functions	Minimum Specifications
4.		System must provide a comprehensive API (Application Programming Interface) or SDK (Software Development Kit) to allow interfacing and integration with existing systems.
5.		The solution should be network and protocol agonistic and provide option to connect legacy system through APIs with either read, write or both options. It should connect diverse on premise and/or cloud platforms and makes it easy to exchange data and services between them.
6.		The system shall allow seamless integration with all of the department's existing and future initiatives (e.g. open source intelligence, situation management war room, etc.)
7.		The platform should be able to integrate with any type of sensor platform being used for the urban services irrespective of the technology used. The platform should also allow the manufacturers of the sensors to develop integrations themselves using SDKs without affecting the northbound applications and existing integrations"
8.	Convergence of Multiple feeds / services	System need to have provision that integrates various services and be able to monitor them and operate them. The solution should provide option to integrate existing deployed solution by City and also need to provide scalability option to implement new use cases.  System should have capability to source data from various systems implemented in Chennai (being implemented as part of this project or other projects) to create actionable intelligence
9.	Industry Standards for the Command and Communications Center	The solution should adhere to the industry standards for interoperability, data representation & exchange, aggregation, virtualization and flexibility
10.		IT Infrastructure Library (ITIL) standards for Standard Operations Plan & Resource Management
11.		Geo Spatial Standards like GML & KML etc.
12.		Business Process Model and Notation (BPMN) or equivalent for KPI Monitoring.
13.	Command and Communications Operations	The solution shall provide a unified viewing and management GUI that enables operators to manage situations in a consistent manner, regardless of underlying integrated systems.
14.		The Solution shall process events automatically, perform correlations, prioritization and rulebased calculations based on a predefined business logic.



#	Functions	Minimum Specifications
15.		The Solution shall facilitate the management of situations, as opposed to individual alarms
16.		The Solution shall have facilities to support routine management, such as scheduler, tour management tool, intercom and messaging and allow seamless escalation from routine to emergency management.
17.		The Solution shall have applications to support the complete operational cycle of Planning, Responding and Debriefing.
18.		The Solution shall support the planning and activation of dynamically adapting response plans to real time varying situations.
19.		The Solution shall have an at-a-glance operational status view that will indicate all exceptions such as alarms, outstanding events that still require attention, and escalations.
20.	Incident Management Requirements	The system must provide Incident Management Services to facilitate the management of response and recovery operations:
21.		Define conditional tasks with pre-configured branching options for presentation to users and with procedures and response plans which change dynamically based on users' selections
22.		define automatic procedure tasks that initiate actions, including <ul style="list-style-type: none"> <li>a) sending messages</li> <li>b) displaying video</li> <li>c) popping up pre-configured GIS map views</li> <li>d) adjusting incident's details, such as editing incident name or raising the severity</li> <li>e) level</li> <li>f) inserting another procedure into action</li> </ul>
23.		define key performance indicators, trends, leading Indicators for visualization on a web-based configurable dashboard
24.		configure and monitor service levels and trigger actions for monitored key performance indicators
25.		Should support for multiple incidents with both segregated and/or overlapping management and response teams.
26.		Should support Geospatial rendering of event and incident information.
27.		Should support plotting of area of impact using polynomial lines to divide the area into multiple zones on the GIS maps.
28.		GIS map functions shall include 2D and 3D views, synchronized, displaying the same objects and areas, and easily switched from one

#	Functions	Minimum Specifications
		view to the other
29.		The GIS map function shall provide the ability to track movements, real-time and historical, and status of all location-based technologies, including GPS and RFID
30.		The GIS map function shall further support: <ol style="list-style-type: none"> <li>1) layer types capable of being toggled on/off per pre-defined rule</li> <li>2) saving of multiple GIS map views for later on-demand or automatic popup</li> <li>3) customization and real time activation of multiple-level drill downs by linking objects placed on map layers to other GIS view</li> <li>4) definition and drawing of zones of arbitrary shapes and sizes and rendering as layers</li> </ol>
31.		An operator shall be able to perform below on GIS map views <ol style="list-style-type: none"> <li>b. place of predefined objects on map locations to include cameras, other sensors, sensors, alarm points, representation of sensor groups, vehicles, and people</li> <li>c. add points, polylines, and polygons to maps to identify multiple locations related to an incident</li> <li>d. place or directly open incidents on a map</li> <li>e. filter display multiple locations related to an incident</li> </ol>
32.		Should support incorporation of resource database for mobilizing the resources for response.
33.		Should provide facility to capture critical information such as location, name, status, time of the incident and be modifiable in real time by multiple authors with role associated permissions (read, write). Incidents should be captured in standard formats to facilitate incident correlation and reporting.
34.		The system must identify and track status of critical infrastructure / resources and provide a status overview of facilities and systems
35.	Integrated User Specific & Customizable Dashboard	Should provide integrated dashboard with an easy to navigate user interface for managing profiles, groups, message templates, communications, tracking receipts and compliance
36.		Should provide current status (snapshot) of organization's facilities, departments and a holistic perspective of incidents and situations, including incident handling time, number of false alerts, and number of active and closed incidents

#	Functions	Minimum Specifications
37.		<ul style="list-style-type: none"> <li>• Collects major information from other integrated City sensors/platforms.</li> <li>• Should allow different inputs beyond cameras, such as, PC screen, web page, and other external devices for rich screen layout</li> <li>• Multi-displays configurations</li> <li>• Use of GIS tool which allows easy map editing for wide area monitoring (Google map, Bing map, ESRI Arc GIS map, etc.).</li> </ul>
38.		Should provide dashboard filtering capabilities that enable end-users to dynamically filter the data in their dashboard based upon criteria, such as region, dates, product, brands, etc. and capability to drill down to the details
39.	Integration with Social Media & Open Source Intelligence	Should provide integration of the Incident Management application with the social media. Should provide analytics based on the social media feed collected from the open source intelligence and collate with the surveillance inputs to alert the responders for immediate action on the ground.
40.		Should extract messages and display it in an operational dashboard.
41.		Should be able to correlate the extracted message from the social media with existing other events and then should be able to initiate an SOP.
42.		Should be able to identify the critical information and should be able to link it to an existing SOP or a new SOP should be started.
43.		Should provide notifications to multiple agencies and departments (on mobile) that a new intelligence has been gathered through open source/social media.
44.	Device Status, Obstruction	Should provide ICON based user interface on the GIS map to report non-functional device.
45.	Detection and Availability Notification	Should also provide a single tabular view to list all devices along with their availability status in real time.
46.		Should provide User Interface to publish messages to multiple devices at the same time.
47.	Event Correlation	Command and Communications Center should be able to correlate two or more events coming from different subsystems (incoming sensors) based on time, place, custom attribute and provide correlation notifications to the operators based on predefined business and operational rules in the configurable and customizable rule engine.

#	Functions	Minimum Specifications
48.	Standard Operations Procedures (SOP)	Command and Communications Center should provide for authoring and invoking un-limited number of configurable and customizable standard operating procedures through graphical, easy to use tooling interface.
49.		Standard Operating Procedures should be established, approved sets of actions considered to be the best practices for responding to a situation or carrying out an operation.
50.		The solution shall provide a visual environment to design business workflow processes that map business rules into a set of workflows to provide automatic responses.
51.		The users should be able to edit the SOP, including adding, editing, or deleting the activities.
52.		The users should be able to also add comments to or stop the SOP (prior to completion).
53.		There should be provision for automatically logging the actions, changes, and commentary for the SOP and its activities, so that an electronic record is available for after-action review.
54.		The SOP Tool should have capability to define the following activity types:
55.		<b>Manual Activity</b> - An activity that is done manually by the owner and provide details in the description field.
56.		<b>Automation Activity</b> - An activity that initiates and tracks a particular work order and select a predefined work order from the list.
57.		<b>If-Then-Else Activity</b> - A conditional activity that allows branching based on specific criteria. Either enter or select values for Then and Else.
58.		<b>Notification Activity</b> - An activity that displays a notification window that contains an email template for the activity owner to complete, and then sends an email notification.
59.		<b>SOP Activity</b> - An activity that launches another standard operating procedure.
60.		Key Performance Indicator
61.	The CCC shall allow configuration and monitoring of service levels for key performance indicators and triggering of actions towards the incident management system when those service levels are breached	

#	Functions	Minimum Specifications
62.		<b>Green</b> indicates that the status is acceptable, based on the parameters for that KPI, no action is required.
63.		<b>Yellow</b> indicates that caution or monitoring is required, action may be required.
64.		<b>Red</b> indicates that the status is critical and action is recommended.
65.	Reporting Requirements	Command and Communications Center should provide easy to use user interfaces for operators such as Click to Action, Charting, Hover and Pop Ups, KPIs, Event Filtering, Drill down capability, Event Capture and User Specific Setup
66.		The solution should generate Customized reports based on the area, sensor type or periodic or any other customer reports as per choice of the administrators
67.		The CCC shall provide a repository of built-in relevant reports, including: <ol style="list-style-type: none"> <li>1) Incident Reports                             <ol style="list-style-type: none"> <li>a) Detailed incident reports shall include an incident summary, all the tasks associated with the incident, sensor related activities, relevant snapshots, and maps.</li> </ol> </li> <li>2) Periodic Reports</li> <li>3) Maintenance Reports</li> <li>4) Statistical Reports</li> </ol>
68.		The CCC shall have a built-in reporting engine that will allow on demand or automatic report generation, configurable by the Administrator and with customization options
69.	Collaboration among Stakeholders	The CCC shall enable stakeholder collaboration where incidents/tasks triggered automatically or manually by control room operators are distributed to the correct owners in incident/task context, such collaboration to include: <ol style="list-style-type: none"> <li>a) allowing departments to work autonomously</li> <li>b) allowing logical locations or project groups to work autonomously</li> <li>c) allowing inter-department collaboration</li> </ol>
70.		Collaboration shall include content such as markups, comments, tasks, and forms.
71.	Asset Management	The system shall provide the capability to define, search, and locate assets of various types, including vehicles, buildings, and people.
72.		Asset management shall be fully integrated with the events correlation/ workflows / rules engine and shall allow defining various triggers based on specific assets, asset types, asset groups and assets attributes.

#	Functions	Minimum Specifications
73.		<p>The system shall enable assets to be displayed on maps with their corresponding GIS locations and unique icons.</p> <p>a. The context menu associated with an asset's map icon shall allow direct dialing of a phone number, if available.</p>
74.	Communication Requirements	The solution should adhere to the below mentioned communication requirements.
75.		The system shall allow email messages based on templates to be initiated by users in response to incidents or invoked by rules-based automatic actions.
76.		Provide the capability to invite using information provided during the location of those individuals or roles, invite them to collaborate and to share valuable information.
77.		<p>The System shall support on-demand or automatic outgoing call initiation.</p> <p>a) The SMS shall maintain an electronic telephone book that may be searched or used for on-demand calling.</p> <p>b) Calling capability shall be available via GIS map icons.</p> <p>c) SIP protocol shall be supported.</p>
78.		Provide a single webbased dashboard to send notifications to target audiences using multiple communication methods including voice-based notification on PSTN/Cellular, SMS, Voice mail, E- mail and Social Media
79.		The solution should provide Dispatch Console integration with various communication channels. It should provide rich media support for incidents, giving dispatchers the power to consolidate information relating to an incident and instantly share that information among responder teams. It should assess the common operating picture, identify & dispatch mobile resources available nearby the incident location. Augment resources from multiple agencies for coordinated response.
80.	Authentication	Use authentication information to authenticate individuals and/or assign roles.
81.	Events and Directives control	Should provide the capability for the events that are produced from a sub- system and are forwarded to the Command and Communications Center. Events could be a single system occurrence or complex events that are correlated from multiple systems. Events could be ad hoc, real-time, or predicted and could range in severity from informational to critical. At the Command and Communications Center, the event should

#	Functions	Minimum Specifications
		be displayed on an operations dashboard and analyzed to determine a proper directive.
82.		Directives issued by the Command and Communications Center should depend on the severity of the monitored event. Directives will be designed and modified based on standard operating procedures, as well as state legislation. A directive could be issued automatically via rules, or it could be created by the operations team manually.
83.	Alert & Mass Notification Requirements	The system should provide the software component for the message broadcast and notification solution that allows authorized personal and/or business processes to send large number of messages to target audience (select-call or global or activation of pre-programmed list) using multiple communication methods including SMS, Voice (PSTN/Cellular), Email and Social Media.
84.		Provide a single webbased dashboard to send notifications to target audiences using multiple communication methods including voice-based notification on PSTN/Cellular, SMS, Pager, Voice mail, E-mail and Social Media
85.		Provide function for creating the alert content and disseminating to end users. Provision of alerting external broadcasting organizations like Radio, TV, Cellular, etc., as web-service.
86.	Security & Access Control	Provide Role based security model with Single-Sign-On to allow only authorized users to access and administer the alert and notification system.
87.	Internet Security	Provide comprehensive protection of web content and applications on back-end application servers, by performing authentication, credential creation and authorization.
88.	Authorization	Comprehensive policy-based security administration to provide all users specific access based on user's responsibilities. Maintenance of authorization policy in a central repository for administration purposes.
89.	User group	Should provide support to enable assignment of permissions to groups, and administration of access control across multiple applications and resources. Secure, web-based administration tools to manage users, groups, permissions and policies remotely
90.	Flexible single sign-on (SSO)	SSO to Web-based applications that can span multiple sites or domains with a range of SSO options.
91.	Authentication	Support LDAP authentication mechanism
92.	Rule Engine &	Should have ability to respond to real-time data with intelligent &

#	Functions	Minimum Specifications
	Optimization	automated decisions
93.		Should provide an environment for designing, developing, and deploying business rule applications and event applications.
94.		The ability to deal with change in operational systems is directly related to the decisions that operators are able to make
95.		Should have at-least two complementary decision management strategies: business rules and event rules.
96.		Should provide an integrated development environment to develop the Object Model (OM) which defines the elements and relationships
97.	Debriefing Module	Debriefing and analysis tools enable detailed incident reporting and debriefing with time-coded playback of events. Using the Control Room application, planners can simulate alarms and events for realistic training exercises and to help find gaps in existing procedures.
98.		The control room operator should have access to Dial 100, Citizen helpdesk and radio gateway recorded calls along with surveillance camera (new & existing) video feeds. The CCC solution should support scenario reconstruction with Voice & Video data on a single timeline.
99.		Debriefing Tool should enable immediate access to incident data, allowing it to be synchronized and replayed exactly as it happened for postmortem analysis and review. The recorded multimedia, whether it be audio, CCTV, telephony, photos, radar screen captures and more, can be reviewed, tagged and organized in a secured incident folder, and then easily and securely distributed and shared within an organization or between agencies.
100		All communications (Video + Voice – Radio & Telephony etc..) related to a single incident should be able to replay in the sequence in which the communications occurred to better understand the entire incident and the SOPs that were carried out with timestamp for completion of each SOP. This will enable the city operations to find gaps in the incident handling and improve or rewrite any SOP.
101		The debriefing module should allow multi-media and multi-source searches from a single application without the need to shift between applications and databases eg: recorded audio from radio logger and telephony logger, recorded video from video logger etc..
102	Mobile Module – 2-way communication for Field	<ul style="list-style-type: none"> <li>a. Create an incident from the field</li> <li>b. View incidents and relevant incident information including location and attachments</li> <li>c. Exchange comments with the control room operators and other</li> </ul>



#	Functions	Minimum Specifications
	personnel	users d. Support incident management at offline mode with ability to sync information when reconnect with network e. Use a native app (iPad) running IOS operating systems or webbased portal
103	Mobile Module - Citizen	Should be a mobile app downloadable via IOS and Google play for the citizens to download and register. Users should be able to send video, text, photos, locations etc... to the CCC. CCC should create a new incident when a registered user sends any incident they have witnessed.

5.1.3.2 Functional Requirement Specifications

Sr. No	Functional Requirement Specifications - Web Portal- User Management
1	System would allow user to view any Service information from Departments displayed on Web portal.
2	User – self registration and first time password change prompt. System would allow user to login and avail services from any of the modules.
3	During user id creation system would ask for Security question for any password reset request by user in future.
4	System would prompt user to create password as per security policy. Alphanumeric passwords would be asked.
5	System would ask user to create a transaction password to be used for performing any financial transaction with the concerned departments or while making any changes in the profile.
6	During user id creation, system would ask user to furnish all personal details like <ul style="list-style-type: none"> <li>• Name</li> <li>• Sex</li> <li>• Age</li> <li>• Address</li> <li>• Phone no.</li> <li>• Email id</li> <li>• Occupation</li> <li>• Family details</li> <li>• PAN/License/Passport/Voter Registration No. / UID No. or any other Id proof details.</li> </ul>

Sr. No	Functional Requirement Specifications - Web Portal- User Management
7	System would prompt user to login using user id and password created and verify them.
8	On successful password match, system would allow the user to login to the portal and allow him to access his/her profile.
9	On unsuccessful password match, System would generate password error message and ask user to enter correct password in order to login to his/her profile.
10	System would allow user to view his/her profile after login.
11	System would allow user to edit his/her personal details like Name, Address etc.
12	System would display the service related information/Instructions to fill up requested details in the entry forms like applicable fee and documents to be attached/submitted along with application request.
13	For CCC Operator, system would initially allow CCC operators to login using their login ids and passwords as given by System administrator. After first time login by all CCC operators the system would ask them to change their password (alphanumeric) as per the security policy.
14	After successfully changing the password and verifying the same on to the system, CCC operator would get access to all the modules, can accept and insert details of the requests received by the citizens for specific modules.
15	System would display instructions to CCC operators at the time of inserting details in the request form for various applications.
16	CCC Operator would read out the instructions to citizen like applicable fee, documents required along with service request and collect the same. Required documents would be scanned & attached with the request by CCC Operator.
17	System would ask CCC operator “Do you really want to submit the form” to cross-verify and register a request when he clicks on the submit button for each request.
18	System would allow Department official to login using his/her user id and password as provided by System administrator.
19	On successful password match, system would allow Department user to access requests submitted to him/her, pending for his approval or pending for field verification.
20	On unsuccessful password match, System would generate password error message and ask department user to enter correct password.
21	System would allow Department user to perform service processing functions as discussed in Department application module in following sections.

Sr. No	Functional Requirement Specifications - Web Portal- User Management
	<ul style="list-style-type: none"> <li>• If any of the login details are not authenticated then the User would be shown the error message “Invalid login details. Please re-enter”.</li> <li>• Deactivated Users should not be able to login into the application.</li> <li>• For all other active Users, in case of a successful login, the User would be directed to “My Dashboard/Profile” section of the application.</li> </ul>
22	User Logout: System would allow user to log out whenever he intends to.
23	System would automatically terminate the login session if user closes the window by any chance without logging out of the system.
24	System would automatically terminate the login session if no activity is noticed in the profile after login for a specified time interval. The time period defined in “web.config” file must be configurable as per the requirements and when required. By default the time should be 15 minutes.
25	Once the user has logged out or automatically logged out by the system, the system would prompt user to re-enter User details and verify password if the user wants to login.
26	System would prompt users to change their profile & transaction password after regular time intervals.
27	System would notify the CCC/Department user on successful password change by showing alert message on screen during password change. Whereas for citizens an email would be sent to their registered mail id as specified in their profile informing the change in password for their user account.
28	In case user forgets the password, system would allow user to reset the password.
29	System would ask user to answer the security question created during profile creation for resetting the password.
30	System would match the user response with the user records.
31	On successful security question and answer match, system would ask user to update new password. System would prompt the user to re-enter the new password.
32	System would match the new password entered twice before submission and notify user on successful password reset activity.
33	In case of unsuccessful match, system would prompt user to enter same password twice for matching.
34	Once the password has been changed, system shall ask user to use new password for any request submission.

For any online service request citizens would fill up their details in the web page shown on screen after selecting the specific department along with attaching the required supporting documents. System would generate a receipt number for each request submitted by citizen, which would be displayed on screen after submission of the request and also the details of the request would be sent on the registered email-id of citizen. Also an intimation of acceptance of the request would be sent on his/her mobile no as an SMS. For CCC operator system would ask for all citizen details at the initial instance as mentioned in the Functional Requirement above. (Point No. 6), so the email would be sent on the citizen email id and also an intimation would be sent to citizens mobile no.

❖ **Reliability**

- Disclaimers, privacy and security policies, terms and conditions and copyright information to encourage people to use e-government services and information

❖ **Profile Management:**

- Enable registered users to manage their accounts and profiles and as appropriate

❖ **Security**

- Based on ISO 27001/BS 7799 standards, user access to the system must be through a single sign on process, which should involve specification of a user Identification, a password and the applications displayed must be as per the user profile and authority. The system should allow user to change his/her password based on a given time frame as well as give the user the option to change his password at any time. The system should disable the User profile after five unsuccessful log-on attempts. The system should be able to log successful and failed attempts to the system.
- This section highlights the security architecture proposed for the e-Municipality system –

**A. General Requirements**

- i. Information, hardware and software would be secured to both internal and external parties (such as through password encryption).
- ii. The security measures adopted should be of wide range and of high quality, to create confidence in the systems security and integrity. The system should be protected against deliberate or accidental misuse that might cause a loss of confidence in it or loss or inconvenience to one or more of its users.
- iii. System level and application level authentication between portal and between applications within portal, if any, to ensure against security attacks

- iv. The application system would strictly be password protected and access to different modules would be role specific
- v. Audit trails would be provided to allow the activities of users to be monitored.
- vi. For the system, security must be available at Functional level, User group/class level, Menu level and Transaction type level. The following

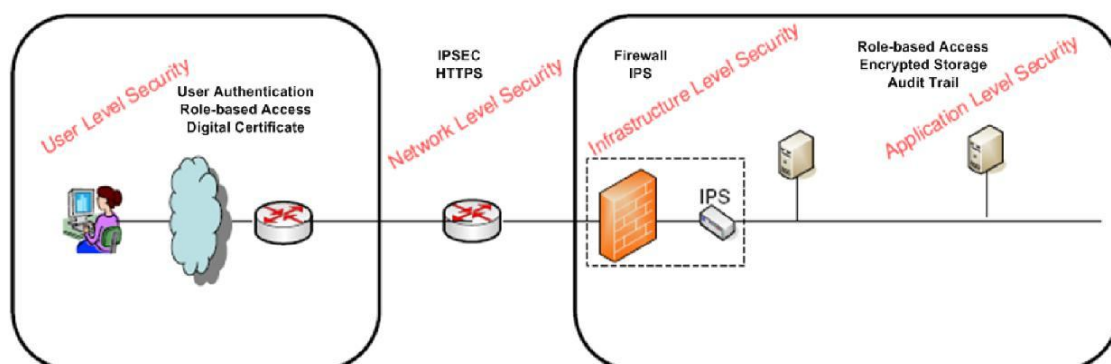


figure depicts the hardware level security at Data Center.

- vii. There should be four levels of security considerations as described below:-
  - a. Key Security Considerations at the User level:
    - (i) User authentication
    - (ii) Role based access to services, transactions and data
  - b. Key Security Considerations at the Network/ Transport level:
    - (i) Network Link Encryption (IPSEC)
    - (ii) Encrypted HTTP session using SSL (HTTPS)
  - c. Key Security Consideration at the Infrastructure Level:
    - (i) Firewall to filter unauthorized sessions/traffic
    - (ii) Intrusion Prevention System to detect/prevent unauthorized activities/sessions
  - d. Key Security Considerations at the Application & Database level:
    - (i) Secure storage of user credentials
    - (ii) Server-to-Server communication encryption
    - (iii) Secured/ encrypted storage of data/ data elements in the Database & DB Backups
    - (iv) Comprehensive logging & audit trail of sessions and transactions

#### 5.1.3.2.1 Security Services for CCC solution

The security services will cover the user profile management, authentication and authorization aspects of security control. This is an application framework service that will be available by any government interfaces and applications accessing the overall framework. 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 framework for which the user is entitled to.

The security service will provide the following security control features –

- User Registration & User Profile Management – This service will allow system administrator of the application software, various govt. agencies to register and create user profiles for users who will access the system.
- User Authentication – This security service will validate the identity of the users against specific security credentials. This service will be realized using underlying HTTP Server and directory service features, which adds a comprehensive set of Web single sign-on services, and extends them further with centralized user provisioning that is available in any open LDAP, version 3-compliant directory service. End users logging on to the interface will be authenticated against the user name / password credentials.
- User Authorization - Users, groups, roles and security policies will be defined to prevent unauthorized access to specific government services.
- The systems implemented for project should be highly secure, considering that it is intended to handle sensitive data relating to the citizens of the State. The overarching security considerations are described below.
  - ✓ The security services used to protect the solution shall include: Identification, Authentication, Access Control, Administration, Audit and support for industry specific standard protocols.
  - ✓ The solution shall support advanced user authentication mechanisms including digital certificates and biometric authentication.
  - ✓ Security design should provide for a well-designed identity management system, security of physical and digital assets, data and network security, backup and recovery and disaster recovery system.
  - ✓ The solution should provide for maintaining an audit trail of all the transactions and should also ensure the non-repudiation of audit trail without impacting the overall performance of the system.
  - ✓ The overarching requirement is the need to comply with ISO 27001 standards of security.
  - ✓ The Application design and development should comply with OWASP top 10 principles
  - ✓ Security for Mobile Application standards should be followed
  - ✓ The solution should use Captcha based login authenticated for users, to address Denial of service, Brut force attack etc.
- Security of Application and the data contained therein is paramount for the success of this Project. Hence, the SI should take adequate security measures to ensure confidentiality, integrity and availability of the information.

- ✓ The proposed solution should include design and implementation of a comprehensive IS security policy in line with ISO 27001 standards to comply with the security requirements mentioned in this section. All the necessary procedures / infrastructure / technology required to ensure compliance with IS security policy should be established by the SI and should be approved by authority before they are implemented. The IS Policy shall include all aspects such as physical and environmental security, human resources security, backup and recovery, access control, incident management, business continuity management etc.
- ✓ The designed IS policy is not in conflict with the security policy of the State Data Centre where the infrastructure would be hosted.
- ✓ The proposed solution should ensure proper logical access security of all the information Assets
- ✓ The proposed solution should be able to classify information assets according to criticality of the information asset.
- ✓ The proposed solution should provide security including identification, authentication, authorization, access control, administration and audit and support for industry standard protocols
- ✓ The proposed solution should have a security architecture which adheres to the security standards and guidelines such as
  - i. ISO 27001
  - ii. Information security standards framework and guidelines standards under eGovernance standards (<http://egovstandards.gov.in>)
  - iii. Information security guidelines as published by Data Security Council of India (DSCI)
  - iv. Guidelines for Web Server Security, Security IIS 6.00 Web-Server, Auditing and Logging as recommended by CERT-In ([www.cert-in.org.in](http://www.cert-in.org.in))
  - v. System shall comply with IT Act 2000 & subsequent amendments.
- ✓ The proposed solution should support the below Integration security standards:
  - i. Authentication
  - ii. Authorization
  - iii. Encryption
  - iv. Secure Conversation
  - v. Non-repudiation
  - vi. XML Firewalls
  - vii. Security standards support
  - viii. WS-Security 1.0
  - ix. WS-Trust 1.2
  - x. WS-Secure Conversations 1.2
  - xi. WS-Basic Security Profile
- ✓ The proposed solution should be a multi-layered detailed security system covering the overall solution needs having the following features:
  - i. Layers of firewall

- ii. Network IPS
  - iii. Enterprise-wide Antivirus solution
  - iv. Information and incident management solution for complete State landscape
  - v. Two factor authentication for all administrators i.e. system administrators, network administrators, database administrators.
  - vi. Audit Log Analysis
- ✓ The SI must ensure that the security solution provided must integrate with the overall system architecture proposed
  - ✓ The proposed solution should facilitate system audit for all the information assets to establish detective controls. The SI is required to facilitate this by producing and maintaining system audit logs for a period agreed to with authority
  - ✓ The proposed solution should ensure that data, especially those pertaining to registration process, transaction process as well as the data that is stored at various points is appropriately secured as per minimum standard 128 Bit AES/3DES encryption.
  - ✓ The proposed solution should provide database security mechanism at core level of the database, so that the options and additions to the database confirm the security policy of GoTN/Gol guidelines.
  - ✓ The proposed solution should support native optional database level encryption on the table columns, table spaces or backups.
  - ✓ The database of the proposed solution should provide option for secured data storage for historic data changes for compliance and tracking the changes.
  - ✓ The proposed solution should be able to ensure the integrity of the system from accidental or malicious damage to data
  - ✓ The proposed solution should be able to check the authenticity of the data entering the system
  - ✓ The proposed solution should be able to generate a report on all “Authorization Failure” messages per user ID
  - ✓ The proposed solution should be able to monitor the IP address of the system from where a request is received.
  - ✓ The proposed solution should be able to differentiate between the systems supplied as part of e-District project & other projects
  - ✓ Retention periods, archival policies and read-only restrictions must be strictly enforceable on all logs maintained in the system
  - ✓ The proposed solution should provide ability to monitor, proactively identify and shutdown the following types of incidents through different modes of communication (email, SMS, phone call, dashboard etc):
    - Pharming
    - Trojan
    - Domains (old/new) similar to Government of Tamil Nadu etc.



- ✓ The proposed solution should be able to monitor security and intrusions into the system and take necessary preventive and corrective actions.
- ✓ The proposed solution should have the option to be configured to generate audit-trails in and detailed auditing reports
- ✓ The proposed solution must provide ACL objects and a security model that can be configured for enforcement of user rights
- ✓ The proposed solution should be designed to provide for a well-designed security of physical and digital assets, data and network security, backup and recovery and disaster recovery system.
- ✓ The proposed solution should have tamper proof data storage to prevent unauthorised data tampering
- ✓ The proposed solution should have a Business Continuity Plan and a Disaster Recovery Plan prepared and implemented by the SI before commencement of the operations. Robust backup procedures to be established for the same.
- ✓ **Password Requirement**  
The proposed solution should allow the Stateto define password policies. The minimum password policies to be defined are:
  - Minimum/ Maximum password length
  - Alpha numeric combination of password
  - Compulsory use of special characters
  - Minimum password age
  - Password expiry period
  - Repeat passwords etc.
- ✓ The proposed solution should be able to automatically check the passwords with the password policy, which can be customized by authority
- ✓ The proposed solution should enforce changing of the default password set by the system (at the time of creation of user ID) when the user first logs on to the system. The proposed solution should enforce all password policies as defined at the time of first change and thereafter.
- ✓ The proposed solution should store User ID's and passwords in an encrypted format. Passwords must be encrypted using MD5 hash algorithm or equivalent(SI must provide details)
- ✓ The proposed solution should be capable of encrypting the password / other sensitive data during data transmission
- ✓ The proposed solution should ensure that the user web access shall be through SSL (https) only for all level of communication for providing higher level of security.

#### 5.1.3.2.1.1 Intrusion Prevention System (IPS)

Intrusion Prevention System (IPS) on application and database server can stop well-known attacks, new/ unknown attacks and encrypted-tunnel based attacks

that target the application/ database servers. The following are the benefits of using IPS:

- i. IPS monitors system activity and notifies administrators when it suspects suspicious activity
- ii. IPS blocks suspicious executable or processes from running by default
- iii. Allows System Administrators to determine which traffic and applications to permit and block
- iv. Protects Files, Registry and Computer Settings of Operating System and Application Integrity Check
- v. Reduces the risk of downtime caused by malware, spyware and other malicious content and helps to keep your critical application up and running
- vi. Helps to log all relevant events to help with compliance, reporting and investigations.

#### 5.1.3.2.1.1.1 Antivirus & Anti-Spam

The following activities need to be performed.

- i. Monitor the Antivirus tool updated on daily basis and ensure that the latest patches are updated in all the systems.
  - ii. Monitor the security console and clean the virus from the systems, which are affected and if necessary, isolate those systems to avoid further spreading of viruses.
  - iii. Alert users on new virus breakouts based on the info received from CERT-IN
  - iv. Install, configure and test latest security patches.
  - v. Troubleshoot and rectify all virus related problems reported and also escalate if not rectified by the Antivirus tool.
  - vi. Monitor the client security tools and adhere to the security policies as finalized with the Authority.
  - vii. Monitoring the efficiency and effectiveness of the Anti-Virus tool.
  - viii. Registering and updating the Anti-Virus tool on the server and the clients periodically
  - ix. Providing feedback on any new viruses detected and alarm/alert the protection systems
- 
- Security techniques and measures provide security measures to protect information belonging to the Portal and the entities (departments) from unauthorized access, modification, or deletion.
  - Monitor, log and audit security incidents with date/time stamping.
  - Maintain and ensure data integrity and visitors' confidentiality and privacy.
  - Implement a password complexity, automatic blocking of user logins after given number of unsuccessful login attempts, controlled access to content stored on the portal and logging of security incidents.

- Provide a facility to securely store critical data within the transaction database so that administrators don't have access to items such as transaction information, passwords, user profiles and other critical items.
- Provide a facility to perform password management functions including: controlled password expirations, minimum password lengths, and enforcement of alphanumeric password standards, password history logging, and user lockout from failed login attempts
- Authenticity of the sender of each service request to be established by login-password as specified at the time of registration by the sender

#### 5.1.3.2.2 *Unified Messaging system:*

- **SMS:** The Web-Portal shall have facility to send SMS to Mobile number of a citizen which was provided while requesting certain information or service. The SMS shall be auto-generated based on the information or service requested on occurrence of its change of status. All the application needs to be integrated with SMS gateway.
- **E-mail:** The Web-Portal shall have facility to send e-mails to
  - The e-mail address of a citizen, provided while requesting certain information or service.
  - The e-mail shall be auto-generated based on the information or service requested on occurrence of its change of status.
  - Reporting Officials maintaining the hierarchy, in cases of delay (as per the Citizens' Charter) in providing services.

#### 5.1.3.2.3 *Workflow Management System as an Application:*

Workflow Management System would serve as an integrated functionality across all the departmental modules to receive and process the request / applications received via any of the service delivery channels. Each request/application should be processed via workflow engine mechanism. I.e. each of the application should be routed to the respective department official's activity dashboard. WMS should also have a facility of delegation of powers.

Following functionalities should also be part of the integrated applications proposed by a successful bidder:

- 1) **Role based Access Management System** – Proposed User management module should have following categories of Users:
  - a. Super User – IT Cell, IT Manager, Municipal Commissioner
  - b. Master Admin – IT cell
  - c. Admin – IT Manager, HoD of a department

- d. Regular / Anonymous Users – Employees from various departments of Authority, Citizens requesting/applying for any service/information.

Available information and user options will vary on all pages throughout the system depending on privileges assigned to the users.

2) **Admin Section** – This section should be privilege restricted and should have the facility to:

- a. Create, modify delete Users and Groups
- b. Assign and remove privileges(modules, sub-modules, workflow & other) to individuals and groups
- c. Administer restricted sections / modules / Webpages

### 3) **Content Management**

- System Integrator would be responsible for maintaining and uploading of content on the web portal for implementation phase and also under operation and maintenance period of 5 years.
- Necessary approval from the associated department needs to be taken by the System Integrator for uploading and maintaining of CMS (Content Management System).

#### 5.1.3.3 **Functional Requirements – General**

- ❖ The system requires continuous availability (24 \* 7)
- ❖ The system shall be designed in such a way so as to ensure that the loss of data is minimized due to network 'drop outs'. Automatic refreshing of data at specified time intervals. The information shall be refreshed from the database and shall not require user intervention
- ❖ System should have an online help capability, which should be customizable. Should have a facility for online learning and collaboration
- ❖ All reports should be query based and should have options like departments zones, wards, employees, from date, to date, etc.
- ❖ Authority Users will access the system using Ethernet LAN / Lease Line / RF / Internet

## 5.1.3.3.1 Functional Requirements for Web Portal

Functionality	Integration required with
A] Home Page	
<ul style="list-style-type: none"> <li>▪ Message from Mayor, Commissioner</li> </ul>	
<ul style="list-style-type: none"> <li>▪ Vision, Mission, Objectives</li> </ul>	
<ul style="list-style-type: none"> <li>▪ Link to various sub-sections               <ul style="list-style-type: none"> <li>○ City Information</li> <li>○ Online Services</li> <li>○ About Authority</li> <li>○ Projects</li> <li>○ Citizen Grievances</li> <li>○ RTI</li> </ul> </li> </ul>	
B] City Information	
<ul style="list-style-type: none"> <li>▪ History of Chennai</li> </ul>	
<ul style="list-style-type: none"> <li>▪ Tourist Locations</li> </ul>	
<ul style="list-style-type: none"> <li>▪ City Map with citizen related GIS information</li> </ul>	GIS
C] About Authority	
<ul style="list-style-type: none"> <li>▪ Administrative Information</li> </ul>	
<ul style="list-style-type: none"> <li>▪ Information on Elected Representatives, Various Committees</li> </ul>	
D] RTI <ul style="list-style-type: none"> <li>▪ Names of PIO.</li> <li>▪ Departments/Wards: Intro, Objectives, responsibilities, powers &amp; duties of officers, employees with gross salary, activities, time limit, directory with telephone no.</li> <li>▪ Committee: Members, purpose, type, freq. of meeting, docs available for public.</li> <li>▪ Projects/ Activities: Budget head, work activities, allocated amount, current statistics.</li> <li>▪ Details of concessions, subsidies given, computerization done in various depts.</li> <li>▪ Integration required for updation of data for RTI with projects, accounts, HRMS, Fleet, material, asset.</li> <li>▪ Scope as per RTI Act 2005 sec. 4(1).</li> </ul>	Projects, Accounts, HRMS, Material Mgmt., Fleet Mgmt., Hospital Mgmt., Asset Mgmt.
<ul style="list-style-type: none"> <li>▪ Opinion Poll</li> </ul>	
<ul style="list-style-type: none"> <li>▪ Photo Gallery</li> </ul>	

Functionality	Integration required with
<ul style="list-style-type: none"> <li>▪ Tenders</li> </ul>	Accounts, Projects
<ul style="list-style-type: none"> <li>▪ FAQ's</li> </ul>	
<ul style="list-style-type: none"> <li>▪ Emergency Information</li> </ul>	
<ul style="list-style-type: none"> <li>▪ Employee Login using LDAP</li> </ul>	HRMS, Associated Department
<ul style="list-style-type: none"> <li>▪ Feedback</li> </ul>	HRMS
<ul style="list-style-type: none"> <li>▪ Contact Us</li> </ul>	
E] Online Services	
<ul style="list-style-type: none"> <li>▪ Application acceptance for various services / certificates                             <ul style="list-style-type: none"> <li>○ Birth / Death Certificates</li> <li>○ Duplicate Bills</li> <li>○ Building Permission related services</li> <li>○ Water Connection</li> <li>○ No Dues Certificates</li> </ul> </li> <li>▪ Vendor Registration</li> </ul>	Accounts, Corresponding Module, CCRS
<ul style="list-style-type: none"> <li>▪ Downloading of Forms</li> </ul>	
<ul style="list-style-type: none"> <li>▪ Online Tendering                             <ul style="list-style-type: none"> <li>○ Sale of Tender Forms</li> <li>○ Acceptance of Tenders</li> </ul> </li> </ul>	
<ul style="list-style-type: none"> <li>▪ Complaints                             <ul style="list-style-type: none"> <li>○ Acceptance</li> <li>○ Status Tracking</li> </ul> </li> </ul>	
<ul style="list-style-type: none"> <li>▪ Status on Applications / Complaints</li> </ul>	
<ul style="list-style-type: none"> <li>▪ Payment Details, Bill Details</li> </ul>	
<ul style="list-style-type: none"> <li>▪ Online Payments</li> </ul>	
<ul style="list-style-type: none"> <li>▪ Self-Assessment of Property Tax</li> </ul>	Property Tax Module

#### 5.1.3.3.1.1 Security Requirement for Portal

This section elaborates specific security requirements which would have to be provided in the Web portal.

- i. Effective password management controls: The portal solution would have the ability to perform password management functions including:
  - a. Controlled password expirations,
  - b. Forced password change with optional grace logins,
  - c. Minimum password lengths (eight characters),
  - d. Alphanumeric password standards,
  - e. Minimum number of numeric characters,
  - f. Non-dictionary words,
  - g. Password history logging and user lockout from failed login attempts.
- ii. Access control to information: The security solution would be facilitating access controls for specific users to only certain resources/services in the portal and at the same time system must provide single sign-on to all functional areas.
- iii. Scalable and portable solution: The security solution would provide scalable access services for the Portal, including scalability in terms of number of users, user groups, resources, and access control policies.
- iv. Secure Communication over the network: The portal should support the exchange of data through secure channels of communication protected by standards such as the SSL protocol. Such facility should provide the following functionality, at a minimum:
  - a. Confidentiality of communication: Encryption of all messages between client and server
  - b. Authenticity: Digital certificates to authenticate all messages between client and server, confirming the identities of messages/transactions
  - c. Integrity: Message Authentication Codes (MACs) provide integrity protection that allows recognizing any manipulation of exchanged messages.
  - d. Secure communication between the user and the portal with SSL and encrypted logon information using algorithms with strong key lengths.
- v. Uninterrupted security services /automated load balancing to backup services:The security solution should provide for load balancing/high-availability to enable a fully scalable and available solution. It should enable continued service on failure of one or more of its component parts.
- vi. Secure storage of critical items: The security solution would provide for the ability to securely store critical data within the LDAP or other user directory structure or any user related databases so that database

administrators or any unauthorized users do not have access to items such as transaction information, passwords, user profiles and other critical items.

- vii. Detailed session management abilities: The security solution would provide for session settings such as idle or max session time-outs, concurrent sessions and other session control settings.
- viii. Web Access Filtering
  - a. The portal security solution should examine all traffic to all resources of the solution and all access attempts to the portal or directly to any resource managed/access by the portal, should be intercepted by the security solution, and examined for authentication and authorization requirements defined for the resource.
  - b. At the same time, the performance overhead of examining all web-traffic and performing the authentication and authorization requests should not become the bottleneck in the service delivery process and should not impact on the performance of the portal solution.
- ix. Security Monitoring: The security solution implemented for portal must be capable of comprehensive logging of the transactions and access attempts to the resources/applications through the portal. It should be capable of logging transaction history, unauthorized access attempts, and attempts to login that fail. It should also be capable of notifying appropriate Authority officials of any suspicious activity.
- x. Security- User profiles:
  - a. Initially the citizen would have to create his profile by Registering at the web portal by specifying the details as asked in the Registration form. Citizen also needs to create profile and transaction password at the time of registration.
  - b. For the first login by a user at CCC/Authority offices, the system should prompt the user to change his password.
  - c. When a user logs-in, the system should show him the date & time of last login
  - d. The System must restrict user access based on the privileges assigned to the user
  - e. The system should maintain a log of all the activities carried out by a user along with a date and time stamp.
  - f. The System must maintain a log of all activities carried out by an administrator.
- xi. Other Security Services:
  - a. The sensitive and confidential information and documents of the users must be stored in an encrypted format in the database.
  - b. The system should support 128-bit encryption for transmission of the data over the Internet.



- c. All the systems in solution network should run most up-to-date anti-virus software to avoid malicious programs to cause damage to the systems
  - d. Any access to the end users to database should only be via application/portal authorization
  - e. Physical security for the solution should address securing all information assets from physical access by unauthorized personnel. For example, the data center server infrastructure should not be physically accessible by anyone other than the persons responsible for on-site maintenance of the systems
  - f. The technology solution should comply with ISO27001 standards. Security certification process should include audit of network, server and application security mechanisms.
- xii. Auditing features and Requirements: The security solution for portal must provide the capability to track and monitor successful and unsuccessful transactions with the portal. Accountability for transactions must be tied to specific users. The architecture/systems should facilitate audit of all significant security events including authentication, accessing of services and security administration. The auditing capabilities need to be built into various layers of the portal infrastructure including Application Software, Operating System, Database, Network, Firewall etc.
- a. SI would have to implement Intrusion Prevention Systems (IPS) at all the critical network points, both internal and external, for monitoring and addressing the unauthorized access attempts and the malicious activities in the network.
  - b. Information and communications systems handling sensitive information must log all security relevant events. Examples of security relevant events include, but are not limited to:
    - i. attempts to guess passwords,
    - ii. attempts to use privileges that have not been authorized,
    - iii. modifications to production application software,
    - iv. modifications to operating systems,
    - v. changes to user privileges, and
    - vi. changes to logging subsystems
  - c. Detailed audit trail of transactions performed in the system (approvals, rejections, renewals etc.) which should capture the details of individuals performing the transactions, date & time stamp etc.
  - d. Stringent security measures should be implemented surrounding the audit data to ensure that audit records are not modified, deleted, etc.
  - e. The web portal should facilitate reporting facilities in a simple and readable manner for the Authority officials to review audit

trails for the transactions occurring in the system.

- xiii. Security Requirements for Portal Databases: Database is the critical components of the portal, which stores the entire data related to Services & functions. Following outlines the security requirements of the database, which at a minimum (included but not limited to) should be implemented.
- a. The database for portal should support and implement encryption capabilities while transferring data over networks, and ability to encrypt data stored in the database at the column level
  - b. Comprehensive auditing for inserts/ deletes/ updates / selects to quickly spot and respond to security breaches.
  - c. The critical data and the related documents stored in the portal database should be stored in encrypted format.

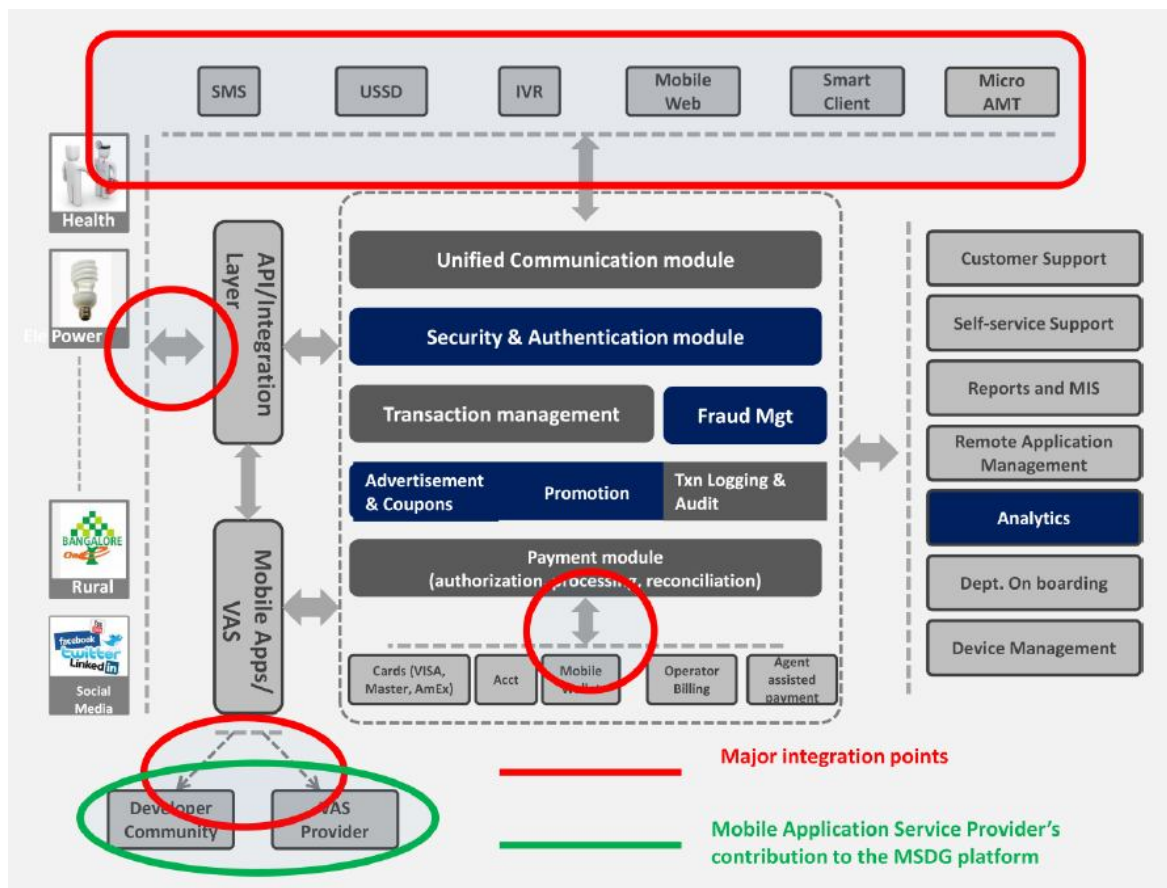
#### 5.1.3.3.2 *Mobile Governance Module*

The purpose of mobile governance platform is to provide mobile enabled services to citizen of Chennai. The platform should be able to interact with the various smart city applications / platform deployed as a part of the Chennai Smart City Project and any other system that may need to be integrated for the purpose of delivering services on the mobile to the citizen. The platform shall be accessed by citizen, businesses, government employees, authorized agents and others authorized agencies.

The mobile application shall be developed on a single platform and shall have various modules to communicate with the smart city applications. It will help the users to access all the smart modules under a single mobile application. Also the system should allow customization, addition, deletion of any modules in the mobile application platform.

The various components of the platform as envisaged are described below. This information should be used to get a broad idea of the functional elements of the platform.

The Bidder is required to provide a detailed functional, technical and architectural description of the Mobile Service Delivery Gateway (MSDG) platform and components.



### 5.1.3.3.3 Unified Communication Module

Unified Communication Module (UCM) will act as an entry point for all the channels to interact with the rest of the MSDG components. The UCM will communicate with Telco SMSC, SMS Aggregator, MMS, CBC, IVR Server (to be deployed in Smart City Data Center), Mobile POS, Government's Smart Client application, Government's Mobile Web portal using the protocol supported by the various applications. UCM shall cater to any new message format or new device in future. UCM is expected to create an open communication layer for any external device to securely communicate with the MSDG platform. Future proofing the platform is of paramount important. The UCM shall support at a minimum SMPP, UCP, HTTP, HTTPS, ISO 8583, Web-Services (SOAP, REST) protocols. The UCM will have minimum logic and will transfer the incoming message to the appropriate MSDG module using a common interface protocol defined by the applications after verifying the data, the UCM may interface with other module for verification / authentication of the message before passing it on to the next module for further processing. Similarly all the outgoing messages will pass through UCM, UCM will translate the message in the appropriate format before sending it to the mobile / external device.

### 5.1.3.3.4 Security & Authentication Module (SAM)

Mobile governance platform need to support multi-level security and authentication process. Departments may choose to use one or more methods to authenticate the user and verify the transaction authenticity and consistency. The module is responsible for authenticating the user as defined by the various transition types. The module will also verify the mobile#, check for the registration of the user, verify the PIN, Biometric, One-Time-Password, check for consistency of the message, check for repeat attack on the server.

The SAM must have the ability to interact with external systems to carry out necessary security and authentication checks as required and defined by the system (ex. Verify biometric based on UID by calling UID's Authentication API). The SAM may also be required to carry out encryption and decryption of the information by calling external API. Security module will also be responsible for checking various roles and permission associated with the activity.

#### *5.1.3.3.5 Transaction Management*

This is the core transaction management module of the platform, all the messages will be routed through transaction management platform for further processing, transaction management will interact with external systems for verification & presentment of the information, will interact with payment module for handing over the information to for payment processing, will interact with department / merchant module, customer/citizen profile module and other modules for various types of verifications. Transaction management will also be responsible for calling business rules API for checking various business rules as well as with service charges module for calculation of transaction charges prior to sending the transaction for further processing.

#### *5.1.3.3.6 Business Rules*

The platform needs to support a comprehensive, configurable business rules engine to cater to various business requirements. The transaction manager will interact with business rules engine before processing the transaction. The business rules module need to support intra business object as well as inter-business object rules.

Setting up of business rules, reporting on failed / passed business rules and transactions as well as analysis to measure the effectiveness of business rules by effectively integrating it with transaction management and other modules of the MSDG platform need to be essential part of the business rule module.

The business rules engine may also need to calculate convenience fee for payment or any other type of transactions.

The business rules engine may also need to have ability to post the transactions in real time or in batch with ability to detect and retry posting.

#### *5.1.3.3.7 System & Transaction Alerting Module*

The system should have the ability to alert other system components, users, administrators upon occurrence of certain activity or event, the module should have the ability to define rules to detect the occurrences and provide alerting to various types of users.

Few examples of alerting are given below

- A. Upon reaching a certain transaction milestone – send informational message to the authorities
- B. Alert the system administrator as well as program management unit when the transaction failure rate goes up by X%
- C. Alert system administrator as well as PMU upon sudden spike or decline in transaction activity
- D. Alert system administrator on failure of a system component or upon abnormal behavior of a certain system component
- E. Real-time / batch messaging (SMS, Outbound dialer) to inform the requestor of the service upon resumption of the service / upon fixing any issues encountered during service fulfillment.

#### *5.1.3.3.8 Transaction Logging & Audit Control Module*

The system need to support extensive, configurable, traceable transaction logging & audit control.

Transaction logging involves life-cycle details of the transaction with information about each and every process step. The module should have the ability to configure not logging of certain data elements (ex. Credit Card details, mPIN, Biometric details) as well as the ability to turn-off or turn-on either partial or complete logging. The module need to log all the API calls to the external system with reference data and date-time stamp as well as all the API calls into the system with reference data and date-time stamp. Another aspect of transaction logging is error detection, logging and propagation to the appropriate level after mapping the external error message to the platform specific error message to effectively communicate to the citizen. A graphical user interface to show the life cycle of the transaction with the necessary details is a necessary requirement of the logging module.

The audit control module serves the purpose of tracking any changes to the system configurations. The module needs to have ability to configure various elements of the system like data base tables, UI, functional flow, parameters at various levels. The system need to provide user interface to setup the audit control parameters as well as generate the necessary reports to monitor and track the changes to the system configuration.

#### *5.1.3.3.9 Marketing & Promotions Module*

An integrated mobile governance platform provides great opportunity for various Government departments as well as businesses to promote their services and reach out to a significant portion of the population in an effective manner. Government departments spend significant amount of resources to provide the information to the citizen – this includes education, awareness building and promotions. The system shall have the ability to integrate with the 3rd party / open source module and deliver the message across all the supported modes of communications (channels). The module shall have the ability to send information / messages to the citizen, business, government employees and agencies as part of the transaction (i.e. part of SMS receipt for payment transaction, part of status update from

department, during IVR or outbound call, as part of mobile web etc...) or as a separate totally independent process as required by the government.

#### *5.1.3.3.10 Payment*

Payment and Banking using mobile phone is an integral part of the comprehensive mobile governance platform. The payment module of the mobile governance platform needs to support various payment instruments allowed by RBI. The module needs to be intelligent enough to route the authorization request to the appropriate payment processing unit. The platform at a minimum need to support processing of mobile payment transactions using credit card, debit card, prepaid card, mobile wallet (also known as semi-closed wallet) issued by authorized private companies, bank account with direct connectivity to bank, bank accounts via NPCI network, cash payment at citizen centric service centers by Govt of Tamil Nadu for. The platform must also support operator billing integration where by the services can be charged to the mobile bill of the consumer.

The payment module will have to be integrated with various banks' payment gateway, various Telco's semi-closed wallet, other authorized private player's wallet, various banks, NPCI. The payment module needs to support communication based on ISO 8583 message format, http/ https based communication or any other industry standard protocol as required by the banking / financial institutions.

The payment transactions need to fully comply with Mobile Banking & Payment Guidelines published by RBI.

#### *5.1.3.3.11 Device management*

Mobile Device Management (MDM) software secures, monitors, manages and supports mobile devices deployed across mobile operators, service providers and enterprises. MDM functionality typically includes over-the-air distribution of applications, data and configuration settings for all types of mobile devices, including mobile phones, smartphones, tablet computers, ruggedized mobile computers, mobile printers, mobile POS devices, etc. This applies to both company-owned and employee-owned (BYOD) devices across the enterprise or mobile devices owned by consumers.

By controlling and protecting the data and configuration settings for all mobile devices in the network, MDM can reduce support costs and business risks. The intent of MDM is to optimize the functionality and security of a mobile communications network while minimizing cost and downtime

The Mobile Governance initiative plans to empower the government departments and agencies with application developed on mobile device to bring in efficiency and transparency in the Government processes.

As these mobile applications are going to be equipped with various features to capture, retrieve citizen information and process citizen payments it is important to have adequate level of security and privacy built into the application.

The responsibility of certifying and enabling these applications will be with the individual departments. These departments will also be required to identify the employees / agencies

for giving access to these applications. The device management service may need to provide LBS (Location Based Service) wherever required.

A number of security and privacy issues need to be addressed for effective implementation of G2G services on mobile at the departmental level.

The issues listed below are limited to enablement of G2G (Government to Government) and related services on mobile to the government employees and authorized agencies of the department.

- A. Lost Device
- B. Unauthorized access to device or application
- C. Inappropriate use of the device or application
- D. Change in the employee / agency status (transfer, termination, change of responsibility within department etc...)
- E. Changes in the procedures and government rules / laws

The above issues can be effectively addressed by implementing the following features in MDM

- A. Ability to uniquely identify the device assigned to an employee
- B. Ability to assign functional role to enable business functions and data based on delegation model
- C. Ability to encrypt the information stored in the device and during transit
- D. Ability to provide secure access to the application
- E. Ability to remotely locate the device
- F. Ability to identify abnormal use of the application
- G. Ability to prevent use by unauthorized person - by way of secure access, location control, usage control etc...
- H. Ability to remotely erase the data from the device in case of lost device or inappropriate or suspicious usage of the device or application
- I. Ability to remotely lock the application and / or device from any use
- J. The requirements related to access to data, ability to modify data will need to be implemented by the departments by providing appropriate APIs and user level data access controls, logging and auditing mechanisms.

The MDM module must expose APIs for the individual department applications to call these APIs. As the individual applications may be developed by a 3rd party vendor, MSP is expected to provide clear guidelines and API calls to MDM enable the application on the MSDG platform. 22 | P a g e

#### *5.1.3.3.12 Service Management*

One of the important aspects of mobile service delivery platform is effectiveness in m-enabling various departments and businesses. Service management module helps enable various department services on mobile, the module should provide a self-service portal for

administrators and departments to manage services, enable / disable various channels, view status of services. Some of the key features of this module are

- A. On-board the department / business
- B. Department / Business profile management
- C. Service Definition including channels, type of service (informational, payment, data capture)
- D. Integration with campaign management module
- E. List of services and status of each service

This module needs to integrate effectively with the integration module which is responsible for exposing the APIs for departments to consume. The APIs should use SOAP or REST protocol and the data exchange using XML. The service management module must support the ability to configure various messages (SMS, USSD, Voice, http/ https based) to be delivered to the recipient and the departments should have the ability to configure messages in the system.

#### *5.1.3.3.13 Remote Application Monitoring (RAM)*

Mobile service delivery platform is going to have multiple loosely coupled modules to facilitate scalability and management of the platform. The platform needs to have high availability and load balancing built into it. Apart from the core modules of the platform, the platform would be integrated with various external entities like payment gateways, banks, telecom operators, SMS aggregators and departments as well as businesses.

The real time monitoring and management of the MSDG platform using single portal is key to provide uninterrupted and high available service to the citizen and businesses in Chennai. The MSDG platform needs to be monitored for effective measurement of the SLA, the responsibility of monitoring and measuring SLA shall be with the MSP.

The Bidder is required to provide necessary software and support for effective monitoring of the platform.

#### *5.1.3.3.14 Self-service management*

The platform needs to provide self-service management facility to departments, businesses, program management unit and administrators to manage various activities of the mobile governance platform. The entire process need to follow role-based delegation model. Various activities like on-boarding the department and services, management of business rules, mobile device management services, transactional reports etc... need to be serviced using a user friendly interface. As much as possible a template based approach should be used by MSP to enable services across various channels.

It is important to note here that anything that is available via user interface (Mobile Web, IVR, USSD etc...) shall be available as part of programmatic interface (API). The programmatic interface shall help enable newer technologies with minimum of re-work.



#### *5.1.3.3.15 MIS Reporting and Dashboard*

The platform need to provide extensive parameterized reporting facility for both department users and administrators to run various reports from time to time.

The reporting module need to have the capability to configure event based or time based reports. These reports need to be delivered via multiple channels like push reports in email, on-demand through browser, downloadable in XLS or XML format, tablets, iPad and other similar technologies, mobile device. The reporting module needs to support various formats including HTML, XML, PDF, XLS, and CSV.

The multi-dimensional report with drill-down capability will need to support dimensions like departments, time, district, city, taluka, service category, channels.

Integration with map and display of real time activity on the map in the form of points on the map, detailed location details, directions and other information useful for display of executive dashboard needs to be supported.

A detailed list of parameters for transactional reports and dimensions for the dashboard reports would be made available during the implementation phase. The reporting and dashboard module need to have the capability to configure event based or time based reports, need to provide tools and techniques to define various dimensions and parameters for the report based on the various business objects supported by the system.

#### *5.1.3.3.16 Application Integration Module*

The mobile governance platform needs to provide well defined, open standards based, well published APIs for various entities (departments, business, developer community) to consume and integrate with the platform. In order for the mobile governance platform to enable services, the platform needs to be integrated with various department's IT services (two way integration where mobile governance platform calls department API and department API calls platform API), the information exchange can be either push or pull based depending on the need. The application integration layer should provide a step by step process for the departments to integrate with the mobile governance APIs to M-enable their services. Similarly, the platform need to provide a step by step process for the departments to develop standards based open API. At a broad level the platform shall have Pre-Processing API, Post-Processing API and Business Logic API (which may be broken into business logic and payment API wherever required). Apart from open standards based web-services, the integration module should support data exchange based on XLS, XML, delimited text and other acceptable and widely used formats. The integration module should also provide a on line and batch mode integration facility. Integration with popular social networking sites like Facebook, Twitter and Google+ using the published API as well as integration with mail server would be considered as desirable features. Any new service enabled on the platform will need to be notified/popularized via Twitter, Facebook, Google+ or any other social media platform.

The integration module will need to be integrated with state and national portal / platform.

#### 5.1.3.3.17 Mobile Application Service (MAS) enabler

The mobile governance platform is expected to act as a catalyst for innovation in Chennai. As the platform provides an out of the box integration with telecom operators and various mobile channels as well as the payment instruments including operator billing, the mobile application service providers can use the facility to enable application services on the platform. The Mobile application service enabler module need to provide the necessary deployment, certification, provisioning and management features for the MAS providers to publish their application. The module needs to provide support for enabling services across channels. MAS module should also expose a payment service API (preferably one API for all payment instruments supported) for the mobile application service providers to integrate. Apart from the payment instruments enabled for payment services, the MAS module need to provide integration with operator billing as well as enabling MAS service upon collection of cash.

#### 5.1.3.3.18 Functional and Data Security

The mobile governance platform needs to provide comprehensive functional and data security. The functional security can be achieved by enabling role and permissions based delegation model. The data security can be achieved by business logic or by way virtualization of the data. Both functional security and data security need to be configurable modules of mobile governance platform. The platform may need to import the data from external systems (department systems), store it and make it available for various other services.

#### 5.1.3.3.19 Usage Profile

The users of the mobile governance service should be able to detect and use the service in an effective manner. The platform should have the ability to group and present the service intelligently. The grouping of services need to support various parameters like Zones, Category of Service, Department, Usage, Awareness need and many such parameters. The platform should look at the usage at an aggregate as well as at an individual level. The presentation of these services across channels (modes of communications) may need to be monitored, managed and altered depending on various parameters as decided by CSCL in consultation with various departments, the usage profile module should have the ability to configure, detect and act on these configuration parameters.

#### 5.1.3.4 Functional Requirement Specification for compliances

Category	Feature Description
Product Feature	Unified Communication Module
	Support for Single or Bulk message (SMS) Push in real time and batch mode to the recipient

Category	Feature Description
	Ability to integrate with IVR technology to provide interactive voice recording based system to the recipient (IVR includes inbound voice, outbound, missed call)
	Ability to process incoming SMS transaction
	Support for USSD based communication, the USSD communication may be initiated from server/network or by citizen
	Support for Mobile Web / WAP based application communication (http, https or any other widely industry standard communication mode)
	Support for Smart Client based application communication ( http, https or encrypted SMS, other widely used industry standard communication protocol)
	Support for SMPP, ISO 8583, http, https based protocol
	Support for outbound dialer based (voice) communication to the recipient
<b>Product Feature</b>	Transaction Management
	Support for end-to-end transaction management system
	Support for extensive, configurable transaction logging
	Support for payment and non-payment based transactions
	Support to track and trace the transaction end-to-end along with time-stamp and time taken at every step
	Support for routing of the transaction to external system for further processing
	Support for processing the transaction based on the response from external system
	Support for complete transaction consistency and ability to reverse the transaction if required
	Ability to add pre-processing and post-processing logic for services
	Ability to connect to external system for pre-processing and post-processing logic

Category	Feature Description
	Ability to post the payment in real-time and batch mode
	Ability to reverse the transaction in case of failure in one of the steps ( the reversal logic or step to be determined by the service )
<b>Product Feature</b>	Business Rules
	Ability to define business rules based on business object attributes
	Ability to validate transaction based on business rules and take necessary action
	Ability to detect abnormal transactions and report / alert one or more users
<b>Product Feature</b>	Messaging / Alerting
	Configurable method to send communication upon occurrence of an event ( SMS, Outbound dialer - voice, USSD, notification in the application )
	Support to customize the message for a specific department, event , transaction type or any other business object that is identified by Govt of Tamil Nadu for effective communication to various entities
	Support to alert various stakeholders upon happening of a certain event - for exampl, availability of new service or feature
	Support for creating a list for sending the message out - the list creation need to be based on some business logic - the system should have the ability to configure the rules to extract the list in various formats ( in DB table, XLS, XML, text or any other industry standard format)
	Support for inserting 'communication message' at the end of the transaction receipt
	Ability to configure 'Communication Message' based on business rules , example of a communication message - Use CFL bulbs to save energy - to be inserted after bill information in the SMS

Category	Feature Description
<b>Product Feature</b>	Communication Protocol Support
	Support for http, https, ISO 8583, Web-Services, XML and other industry standard communication protocols
	Flexibility to support a communication protocol which is not yet supported on the platform
<b>Product Feature</b>	Device Support
	Ability to support any mobile device to enable mobile governance features
	Support to enable services and features based on device characteristics
<b>Product Feature</b>	Language Support
	Support for regional language (Tamil) along with english - the support need to be available at a minimum on voice, SMS, USSD, Mobile Web & Smart Client - The platform should have the ability, any limitation due to external factors like telecom operator's inability to support the feature, limitations of the mobile device etc need to be explicitly mentioned in the vendor comment
	Ability to support additional languages as desired by CSCL, Govt. of Tamil Nadu
<b>Product Feature</b>	Mobile Web
	Mobile Governance portal need to work across all the available devices in a seamless manner
	Ability to detect device characteristics and provision the content in the best possible manner
	Local language support on the devices supporting the local language

Category	Feature Description
<b>Product Feature</b>	Platform Capabilities
	Support for developing application across devices and ability to support new devices and device families
	Support to configure services to be enabled across multiple channels (communication modes)
	Support to enable / disable services based on business rules
	Support for enabling services based on the backend workflow definition without the need to re-download the application
	Support for automatic detection of new service
	Support for auto-upgrade of the client application
	Support for manual upgrade of the client application
	Support for user to use all the available communication modes (channels) to access the service
	Templates with well defined steps (manual and automated) to enable services of various categories
	Ability to deploy and manage multiple instances of the same service
	Support for load balancing of different services
	Support for hot patching
	Support for high availability of services and platform
	Support for loosely coupled application
	Support for asynchronous processing of the transactions
<b>Product Feature</b>	Security
	Support for 2-factor authentication
	Support for multiple authentication factors (PIN, OTP, static password, biometric, profile question, department specific information etc...)
	Support for calling external service to authenticate the user

Category	Feature Description
	Support to authenticate user based on only mobile #
	Support for end-to-end encryption (Mobile Device to MSDG Platform)
	The platform should be able to detect man-in-the middle and repeat attacks wherever possible and desired by business
	Support for encryption of data in database
	Ability to log /no-log sensitive information to meet regulatory and CSCL's security and privacy guidelines
<b>Product Feature</b>	Profile
	Support for Service provisioning based on user preferences
	Support for service provisioning based on business rules like usage, timeline,location etc
	Support for service provisioning based on default logic as determined by CSCL or Department
	Support to subscribe / unsubscribe to the service
	Support to receive service in the language of choice
	Ability to select language of choice as default language
	Ability to control service list and display sequence at the various levels (user, user group, location etc...)
<b>Product Feature</b>	Payment
	Support for http, https based integration with various payment gateways, banks, financial institutions
	Support for ISO 8583 based integration with payment gateways and banks, payment gateways and financial institutions
	Support for Card based payments
	Support for NPCI - IMPS payment
	Support for Account based payment

Category	Feature Description
	Support for Cash Card, Semi-Closed Wallet and other wallet based payment
	Support for agent based payment (Agent accepts cash and uses his financial instrument to process payment)
	Support for integration with Telecom Operator's billing system
	Ability to route the transaction to the appropriate payment gateway based on business logic
	Ability to seamlessly connect to 3rd party payment gateway to process payment directly on their platform (includes platform, 3rd party application, 3rd party web page, 3rd party wap page or any other mechanism that is used in the industry)
<b>Product Feature</b>	Compliance
	Platform and service offerings should meet TRAI & DOT guidelines
	Platform and service offering should meet RBI guidelines for payment
<b>Product Feature</b>	Reconciliation
	Ability to reverse transaction
	Ability to generate failed / suspense transaction report and process it manually or automatically
	Ability to query the status and re-process the transaction
	Ability to track the transaction internally and also with external system by having common reference number
<b>Product Feature</b>	Reporting
	Support for generating transaction report based on user input parameters ( date range, status of txn, dept, txn type etc...)
	Support for summarized reports based on various dimensions and drill downs



Category	Feature Description
	Support for reconciliation report
	Support for various report formats like PDF, XLS, XML, HTML
	Ability to run reports on a periodic basis and send to the pre-defined set of users automatically
	Ability to send report to email or to the mobile phone ( SMS, out-bound call, notification in application )
	Ability to create new reports using well defined templates
<b>Product Feature</b>	Marketing & Promotions
	Ability to configure marketing campaign with deals, communication for citizen
	Ability to track the effectiveness of marketing campaign
<b>Product Feature</b>	Mobile Device Management
	Ability to uniquely identify the device assigned to an employee
	Ability to assign functional role to enable business functions and data based on delegation model
	Ability to encrypt the information stored in the device and during transit
	Ability to provide secure access to the application
	Ability to remotely locate the device
	Ability to identify abnormal use of the application
	Ability to prevent use by unauthorized person - by way of secure access, location control, usage control etc...
	Ability to remotely erase the data from the device in case of lost device or inappropriate or suspicious usage of the device or application
	Ability to remotely lock the application and / or device from any use

Category	Feature Description
<b>Product Feature</b>	Service On-Boarding
	Ability to configure services across multiple channels
	Ability to enable role based logic for services
	Ability to define business rules for services at various levels of services ( for example - service, service category, department or channel level)
	Ability to enable or disable channels for a service, service category or department
	User interface to manage the services , role based access to view and manage the services
<b>Product Feature</b>	Remote Application Management
	Ability to manage all the services running on the platform remotely
	Well defined dashboard to view the health of the platform and service
	Ability to send alert to various entities to alert failure or abnormal behaviour of service
	Ability to provide uptime and downtime details
	Ability to configure message for scheduled / unscheduled downtime and send communication to the concerned entities
	Support for integration with SDC' remote application management platform
<b>Product Feature</b>	Customer Support
	Support for raising trouble ticket and managing the life-cycle of the ticket
	Export / Import of the trouble ticket - Batch Mode
	Web-Services to integrate with external system to pull trouble ticket or push the trouble ticket data or status
	Escalation of trouble ticket and necessary alerting to various entities

Category	Feature Description
	Management Dashboard and drill-down into details
<b>Product Feature</b>	Self-Service Portal
	Ability to manage the platform setup and various functions through well defined user interface
	Role based access to the Modules or UI
	Support for role based delegation model for access to various business functions
<b>Performance / Scalability</b>	Performance / Scalability
	Provide documentary evidence of the ability of the database design to scale the DB from 5 TPS to 50 TPS.
	Ability of the individual component to scale to 50 TPS and the documentary proof to show that there is no performance degradation due to increased load / transaction volume on the system
	Ability of the platform as a whole to scale to 50 TPS and the documentary proof to show that there is no performance degradation due to increased load / transaction volume on the system
	Documentary evidence on performance / scalability tests carried out on the platform
	Detailed process and technology used for performance / scalability testing of the platform
	Documentary evidence on how single point of failure is avoided by the platform architecture and in case there is a specific case of single point of failure due to technological or other constraints -describe the risk mitigation strategy
<b>Framework</b>	Integration Support
	Support for integration with Telecom Operator's prepaid system

Category	Feature Description
	Support for integration with Telecom Operator's Postpaid billing system
	Support for integration with aggregator's utility bill payment system
	Support for Open-Standards Web-Services based integrations with external entities
	Support for batch mode integration with ability to process various data formats like XML, csv, text
	Interaction with mail server to send and receive mail
	Ability to process mail received in a pre-defined / structured format
	Ability to send structured formatted mail
	Support for extensive integration framework to process in batch and online mode, batch mode to support various file formats, support for picking up data from ftp/sftp server
	Support for REST / SOAP based API
	Support for XML data format
	Support for integration template for various categories of services, departments should be able to pick from one of these templates based on their need, additional templates to be developed as and when need arises - the primary objective is to bring down the time required to on-board the services with minimum manual steps
<b>Framework</b>	Architecture
	Detailed architecture of the platform to demonstrate functional and technical capabilities of the solution
	Detailed architecture of DR setup
	Documentary proof on the ability of the platform to continue to function inspite of failure of one or more instances of the components (both internal or external) with scenarios

#### 5.1.3.5 Functional Requirement for Document Management System

1. All departments of GCC and employee should have an access of this module. The system should be linked with all Smart Governance applications where there is a

functionality to upload while processing and submission of application. It should also aid users to refer any document related to that functional activity on the repository on which they are working.

2. The DMS will facilitate the system to maintain the details/report about, Document creation date, creator name, access rights, subject, description, department details etc. DMS should have capability of:
  - Categorization of documents in folders-subfolders
  - Document Version Management
  - Extensive document and folder level operation such as move / copy, email, download, delete
  - Repository should be format agnostic which can archive documents of any format
  - Indexing of the documents on user defined parameters
  - Association of the key words with the documents
3. The system should have minimum of the following:
  - Assign unique id to every document uploaded
  - Have the facility to create, store, view and update the document.
  - Have the facility to assign the view and edit rights for existing document by the creator
  - Have the facility to scan upload the documents
  - Have the facility to index the submitted documents for referencing the file no and transactions
  - Store the index such that data can be easily converted into logical file/ set
  - Have the facility to store different pages of the document as a single set. It should assign the image no to the pages of the single document. However system should be able to retrieve the complete document as a single set.
  - Assign note and annotation to the uploaded document for further reference of any other documents if required
  - Allow the documents to be referenced to the concerned file number
  - Have the facility of archiving the document with time and date stamp
  - Have the facility to import and export email, print and encrypt the document
  - Have the facility to group the documents in a docket and unique id should be assigned to the docket
  - Have the facility to manage the version of the documents and dockets by means of time, user and date stamps
  - Allow the user to search information (within document) by keying keywords, and page no#.
  - Have the search facility to locate documents or Folders
  - Have the combined search facility on Profile, Indexed and Full Text
  - Have the facility to search document or folder profile information such as name, created, modified or accessed times, keywords, owner etc.
  - Support the view of thumbnails for the pages in the documents

- Maintain extensive Audit-trails at user and folder levels.
- Maintain Audit trails on separate actions, and between specific date/times
- Document Repository for managing information
- Organizing documents into hierarchical storage like Folders and Subfolders for management and classification of information
- Provide easy filing and indexing for quick retrieval
- System should support the storing of document (Image & Metadata)
- 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.
- 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.
- Association of the document with Workflow Management System
- Movement of the document based on selected parameters
- Provision to edit the document Metadata
- Versioning of the document
- Provision for marking comments
- Archival of data on pre-defined parameters
- Role based access to the documents
- Final Decision by the Decision Authority
- 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.
- 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.
- 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.

### **Workflow Management System**

- Movement of Proposals on various parameters
- Facility to mark the application to pre-defined hierarchy
- Inbox for officers (listing applications received)
- FIFO principle for taking action on application
- Creation of a Note Sheet for Scanned Documents
- Alerts for delay in action
- Compliance to workflow standards: BPMN, BPEL and WFMC
- Shall support Inbuilt Graphical workflow designer for modelling complex Business Processes using drag and drop facilities.

- Information/Alert to be sent to higher authority in case of delay in action by specific employee of the department
- Pre-defined scrutiny for citizen applications
- Display of all application data during scrutiny process
- Check-list for rejection
- Should have inbuilt Rule Engine for defining rules
- Facility to mark the application to other officer
- Facility to mark the application to other department for their NOC / Comments / Input
- Final Decision by the Decision Authority
- Shall provide graphical and tabular tools to create reports and view progress of each individual process.

### **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.

#### **5.1.3.6 Functional Requirement for Knowledge Management Solution**

Common Knowledge Management solution for all smart cities, to create their knowledge repositories.

##### **a) Archival of Knowledge Content**

- Allow creation of a central knowledge repository of documents that can be accessed by all officials based on their roles and privileges.
- Allow to add description with the uploading documents / knowledge content.
- Should have a well-defined workflow that allows processes for knowledge creation, approval and archival for re-use.

- Should allow multiple / bulk file upload
- Should have folder wise categorization
- Should allow to upload and archive documents of any format including tiff, jpeg, pdf, pdf/a, audio, video etc.
- Should allow categorization of Knowledge into different categories like personnel, financial, legal etc.
- Should allow multimedia content archiving / sharing.

#### **b) Knowledge Content Collaboration**

- Should allow only authorized employees to locate, update and share documents
- Should allow authorized users to post questions / answers.
- Should provide an online discussion forum to hold conversation on posted topics.
- Should allow documents to be stored and modified with proper versioning.
- Should support Individual/group/section/office specific centralized information repository to store knowledge content.
- Should allow collaborative working on the knowledge content.
- Should keep a track of different document versions modified by different users
- Should have an add-on feature of rating the content.
- Should have capability to attach citations and synopsis with the respective knowledge content.
- Should provide the capability to subscribe for the knowledge content, category, so that the users get notifications once any new document, content is getting uploaded for the respective category or knowledge source.
- Should allow users to share the documents on Social media platforms such as Facebook, Twitter etc.
- Should have online chat facilities, where users can initiate a discussion with concerned expert or group of users and can send messages, documents and interact on common platform.
- Discussion forum should have an administrator who can add, edit and delete discussions post.
- Should have functionality to define the To-Do list for the tasks to be done.

#### **c) Strong Searching Capabilities**

- Provides facility for index based content search
- Support content searching using content categories, sub categories, Title, author, File/Content types
- Should allow to search for contents based on Keywords, Tags, From/To Date etc.
- Supports automatic full text indexing for Text based search

#### **d) Notification & Messaging**



- Should allow users to mail knowledge content to users / departmental officials.
- Should have feature to send the notifications to a user about his/her content being approved /rejected.
- Should have an intelligent feature to either email knowledge content on a specific date and time.
- Should have a built in alert mechanism (Email and SMS) for subscribed documents.

#### **e) Architecture & Scalability**

- Should be built using Enterprise Content Management framework
- Should be COTS based solution and platform independent and support for all major operating systems such as Windows, Linux etc. on server side with or without virtualization.
- Multi-tier architecture having web-based solution and support for clustering
- Supports separate Document/Image server for better management of documents and store only metadata information in database.
- Proven Scalability for thousands of users
- Support for de-centralized/distributed architecture
- Store billions of documents in repository

#### **f) Viewing & Annotations**

- Support for viewing and annotating on image documents through inbuilt viewer through web and mobile devices
- Inbuilt viewer for viewing scanned documents and facilitates zoom- in/zoom-out, zoom percentage and other image operations like Invert, rotate etc.
- Support view of multipage document having capability to download and view document page by page
- Support view & annotation of PDF/A format documents using inbuilt viewer (open ISO standard for long term archival of documents)
- Provides facility of putting text and image annotations on scanned document.

#### **g) Reporting & Dashboards**

- Should have dashboard and reporting capability for viewing the reports such as knowledge content added by users, number of documents per category, content pending to be approved etc.

#### **h) Compliance with Open Standards**

- Should compliant to ODMA and WebDAV standards
- Supports interoperability through CMIS compliance
- Workflows of the proposed Knowledge Management System should compliant to open standards such as BPMN, BPEL, WFMC.
- Should compliant to records and metadata management standards such as DoD 5015.15, ISO 15489, Dublin Core

#### **i) Document Management Security**

Knowledge Management system should allow for multiple permission levels such as:

- At Folder level – All rights (system, group, and user) are assigned at folder level.
- At system level – Set global access rights at the overall system level.
- At the group level – The most efficient way to manage security rights is defining the access rights at group level wherein users who are part of the specific groups will be able to perform operations accordingly.
- At the user level – Set permissions for Individual users.

Apart from this, Knowledge Management System should also have various other key security features having support for:

- Defining multiple levels of access rights (Delete/ Edit/ View/ Print/ Copy or Download).
- Define system privileges like Create/Delete Users, Define indexes etc.
- Support for Digital certificate
- Facility to define password policy with extensive password validations like passwords must be of minimum 8 characters which shall be alphanumeric, locking of user-id after three un- successful attempts, password expiry, password history so that passwords are not same as previous passwords etc.
- Extensive Audit-trails at document, Folder and for highest levels for each action done by user with user name, date and time
- Encryption of documents and metadata

#### **j) Application Integration Capability**

- Support for web services, Java based API, and URL-based integration
- Integration based on standards such as XML
- Active Directory/LDAP integration

#### **5.1.3.7 Functional Specifications of Non-IT components at CCC**

Proposed specifications for various Non-IT components, required at Command Center and the Edge Level, are given in this section. It is essential that Fire Proof material be

used as far as possible and Certification from Fire Department be taken for Command Centers before Go Live.

#### 5.1.3.7.1 *Civil and Architectural work*

##### 5.1.3.7.1.1 False Ceiling (at Command Center)

- 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.
- 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.

##### 5.1.3.7.1.2 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.
- 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.
- 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.
- 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.

##### 5.1.3.7.1.3 Partitions (wherever required as per approved drawing)

- Full height partition wall of 125 mm thick fire line gyp-board partition using 12.5 mm thick double fire-line gyp-board on both sides with GI steel metal vertical stud frame of size 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 cutouts for switch board, sockets, grill etc. It shall also include preparing the surface smoothly and all as per manufacture's specification etc. finally finishing with one coat of approved brand of fire resistant coating.
- With glazing including the framework of 4" x 2" powder coated aluminum section complete (in areas like partition between server room & other auxiliary areas).
- 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.

#### 5.1.3.7.1.4 Painting

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

#### 5.1.3.7.2 PVC Conduit

- The conduits for all systems shall be high impact rigid PVC heavy-duty type and shall comply with I.E.E regulations for standardized conduit 1.6 mm thick as per IS 9537/1983.
- All sections of conduit and relevant boxes shall be properly cleaned and glued using appropriate epoxy resin glue and the proper connecting pieces, like conduit fittings such as Mild Steel and should be so installed that they can remain accessible for existing cable or the installing of the additional cables.
- No conduit less than 20mm external diameter shall be used. Conduit runs shall be so arranged that the cables connected to separate main circuits shall be enclosed in separate conduits, and that all lead and return wire of each circuit shall be run to the same circuit.

- All conduits shall be smooth in bore, true in size and all ends where conduits are cut shall be carefully made true and all sharp edges trimmed. All joints between lengths of conduit or between conduit and fittings boxes shall be pushed firmly together and glued properly.
- Cables shall not be drawn into conduits until the conduit system is erected, firmly fixed and cleaned out. Not more than two right angle bends or the equivalent shall be permitted between draw or junction boxes. Bending radius shall comply with I.E.E regulations for PVC pipes.
- Conduit concealed in the ceiling slab shall run parallel to walls and beams and conduit concealed in the walls shall run vertical or horizontal.
- 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.

#### 5.1.3.7.3 *Wiring*

- PVC insulated copper conductor cable shall be used for sub circuit runs from the distribution boards to the points and shall be pulled into conduits. They shall be stranded copper conductors with thermoplastic insulation of 650 / 1100 volts grade. Color code for wiring shall be followed.
- Looping system of wiring shall be used, wires shall not be jointed. No reduction of strands 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.

#### 5.1.3.7.4 *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. Earthing 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, 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.
- 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 in the UPS room.

- 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 small copper loop to bridge the top cover of the transformer and the tank shall be provided to avoid earth fault current passing through fastened bolts, when there is a lightning surge, high voltage surge or failure of bushings.
- 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 need to be in place for this copper mesh.
- Provide separate Earthing pits for Servers, UPS & Generators as per the standards.

#### 5.1.3.7.5 *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 crisscrossing 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 118standard 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 earthing 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.

#### 5.1.3.7.6 *Water Leak Detection*

The water leak detector shall be installed to detect any seepage of water into the critical area and alert the Security Control Room for such leakage. It shall consist of water leak detection cable and an alarm module. The cable shall be installed in the ceiling & floor areas around the periphery.

- Water Leak Detection system should be for the Server and Network room Areas to detect and water flooding below the floor of the DC.
- Water Leak Detection System should be wire based solution with alarm; the wire needs to lay in DC surrounding the PAC units, which is the probable source of water leakage.

Supply Voltage:	230Vac @ 50Hz
Supply current	50mA max.
Output	12A @ 250Vac
Response time	<1 sec. after exposure
Electrical	Terminals for 0.5-2.5 <sup>2</sup> cable
Ambient:	
Temperature	-10 to 50°C
RH	0-80% non-condensing
Material	PVC Twisted pair with stainless 316 elements
Dimension	3.5mm dia. Maximum cable run 200m (Including detection cable)

#### 5.1.3.7.7 *Gas Based Fire Suppression System*

The Clean Agent Fire Suppression system cylinder, CCOE, Nagpur approved seamless cylinders, discharge hose, fire detectors and panels and all other accessories required to provide a complete operational system meeting applicable requirements of NFPA 2001 Clean Agent Fire Extinguishing Systems, NFPA 70 National Electric Code, NFPA 72 National Fire Alarm Code or ISO standards must be considered to ensure proper performance as a system with UL/FM approvals and installed in compliance with all applicable requirements of the local codes and standards.



- The Clean Agent system considered for Total flooding application shall be in compliance with the provisions of Kyoto Protocol.
- Care should be taken that none of the Greenhouse Gases identified in the Kyoto Protocol is used for fire suppression application.
- The minimum criterion for the selection of the Clean Agent will be on the following parameters
  - Zero Ozone Depleting Potential.
  - Global Warming Potential not exceeding one.
  - Atmospheric Lifetime not exceeding one week.
- The clean agent fire suppression system with FK-5-1-12 and Inert Gas based systems are accepted as a replacement of HCFC and HFC as per Kyoto Protocol.
- The Clean Agent considered for the suppression system must be suitable for manable occupied areas with NOAEL Level (No observable adverse effect level) of 10% as compared to the design concentration to ensure high safety margin for the human who might be present in the hazard area.
- The minimum design standards shall be as per NFPA 2001, 2004 edition or latest revisions.
- Care shall be given to ensure proper early warning detection system with minimum sensitivity of 0.03% per foot obscuration as per NFPA 318 & NFPA 72 to ensure that one gets a very early warning to investigate the incipient fire much before the other detectors activate the fire suppression system automatically.
- All system components furnished and installed shall be warranted against defects in design, materials and workmanship for the full warranty period which is standard with the manufacturer, but in no case less than five (5) years from the date of system acceptance
- Additionally, Portable Extinguishers (CO<sub>2</sub> or Halon based Extinguishers are not acceptable) shall be placed at strategic stations throughout the Data Centre.

OR

- Fire suppression system shall deploy FM-200 (ETG-5) based gas suppression systems with cross-zoned detector systems for all locations. These detectors should be arranged in a manner that they activate the suppression system zone wise to cater to only the affected area.
- Illuminated Signs indicating the location of the extinguisher shall be placed high enough to be seen over tall cabinets & racks across the room. Linear heat detection cable should be placed along all wire pathways in the ceiling. This should not directly trigger the suppression system—rather; it should prompt the control system to sound an alarm
- The OEM (/ Bidder) shall give a Certificate stating that their FM-200 system is approved by UL / FM / VdS / LPC/CNPP for use with Seamless Steel Cylinders (Component as well as System Approval).
- The OEM (/ Bidder) shall also provide a Letter that the OEM has FM-200 Flow Calculation software suitable for Seamless Steel cylinder bided for as per the Bill

of materials and that such Software shall be type approved by FM / UL / VdS / LPC.

- The Storage Container offered shall be of Seamless type, meant for exclusive use in FM- 200 systems, with VdS/FM/UL/LPC/CNPP component approval. Welded cylinders are not permitted.
- The Seamless storage cylinder shall be approved by Chief Controller of Explosives, Nagpur and shall have NOC from CCoE, Nagpur for import of the same. Documentary evidence to be provided for earlier imports done by the bidder.
- The FM-200 valve should be Differential Pressure Design and shall not require an Explosive / Detonation type Consumable Device to operate it.
- The FM-200 Valve operating actuators shall be of Electric (Solenoid) type, and it should be capable of resetting manually. The Valve should be capable of being functionally tested for periodic servicing requirements and without any need to replace consumable parts.
- The individual FM-200 Bank shall also be fitted with a manual mechanism operating facility that should provide actuation in case of electric failure.
- The system flow calculation is to be carried out on certified software, suitable for the Seamless Steel Cylinder being offered for this project. Such system flow calculations shall be also approved by VdS / LPC/ UL / FM.
- The system shall utilize 25 Bar / High pressure (362 psi) technology that allows for a higher capacity to overcome frictional losses and allow for higher distances of the agent flow; and also allow for better agent penetration in enclosed electronic equipment such as Server Racks/ Electrical Panels etc.
- The designer shall consider and address possible Fire hazards within the protected volume at the design stage. The delivery of the FM-200 system shall provide for the highest degree of protection and minimum extinguishing time. The design shall be strictly as per NFPA standard NFPA 2001.
- The suppression system shall provide for high-speed release of FM-200 based on the concept of total Flooding protection for enclosed areas. A Uniform extinguishing concentration shall be 7% (v/v) of FM-200 for 21 degree Celsius or higher as recommended by the manufacturer.
- The system discharge time shall be 10 seconds or less, in accordance with NFPA standard 2001.
- Sub floor and the ceiling void to be included in the protected volume.
- The FM-200 systems to be supplied by the bidder must satisfy the various and all requirements of the Authority having Jurisdiction over the location of the protected area and must be in accordance with the OEM's product design criteria.
- The detection and control system that shall be used to trigger the FM-200 suppression shall employ cross zoning of photoelectric and ionization smoke detectors. A single detector in one zone activated, shall cause in alarm signal to

be generated. Another detector in the second zone activated, shall generate a pre-discharge signal and start the pre-discharge condition.

- The discharge nozzles shall be located in the protected volume in compliance to the limitation with regard to the spacing, floor and ceiling covering etc. The nozzle locations shall be such that the uniform design concentration will be established in all parts of the protected volumes. The final number of the discharge nozzles shall be according to the OEM's certified software, which shall also be approved by third party inspection and certified such as UL / FM / VdS / LPC.
- The Cylinder shall be equipped with differential pressure valves and no replacement parts shall be necessary to recharge the FM-200 containers.
- FM-200 shall be discharged through the operation of an Electric (solenoid) operated device or pneumatically operated device, which releases the agent through a differential pressure valve.
- The bidder shall provide all documentation such as Cylinder Manufacturing Certificates. Test and Inspection Certificates and Fill Density Certificates.
- The FM-200 discharge shall be activated by an output directly from the 'FM-200' Gas Release control panel, which will activate the solenoid valve. FM-200 agent is stored in the container as a liquid. To aid release and more effective distribution, the container shall be super pressurized to 600 psi (g) at 21°C with dry Nitrogen.
- The releasing device shall be easily removable from the cylinder without emptying the cylinder. While removing from cylinder, the releasing device shall be capable of being operated, with no replacement of parts required after this operation.
- Upon discharge of the system, no parts shall require replacement other than gasket, lubricants, and the FM-200 agent. Systems requiring replacement of disks, squibs, or any other parts that add to the recharge cost will not be acceptable.
- The manual release device fitted on the FM-200 Cylinder(s) shall be of a manual lever type and a faceplate with clear instruction of how to mechanically activate the system. In all cases, FM-200 cylinders shall be fitted with a manual mechanical operating facility that requires two-action actuation to prevent accidental actuation.
- FM-200 storage cylinder valve shall be provided with a safety rupture disc. An increase in internal pressure due to high temperature shall rupture the safety disc and allow the content to vent before the rupture pressure of the container is reached. The # contents shall not be vented through the discharge piping and nozzles.
- FM-200 containers shall be equipped with a pressure gauge to display internal pressure.
- Brass Discharge nozzles shall be used to disperse the 'FM-200'. The nozzles shall be brass with female threads and available in sizes as advised by the OEM

system manufacturer. Each size shall come in two styles: 180° and 360° dispersion patterns.

- All the Major components of the FM-200 system such as the Cylinder, Valves and releasing devices, nozzles and all accessories shall be supplied by one single manufacturer under the same brand name.
- Manual Gas Discharge stations and Manual Abort Stations, in conformance to the requirements put forth in NFPA 2001 shall be provided.

Release of FM-200 agent shall be accomplished by an electrical output from the FM- 200 Gas Release Panel to the solenoid valve and shall be in accordance with the requirements set forth in the current edition of the National Fire Protection Association Standard 2001.

#### *5.1.3.7.8 Comfort Air Conditioning at Command Centers*

- Cooling Capacity as per the requirements at each of the control rooms
- Compressor – Hermetically Sealed Scroll Type
- Refrigerant – R 22 Type
- Power Supply – Three Phase, 380-415 V, 50 Hz
- Air Flow Rate – minimum 19 cu m / min
- Noise Level - < 50 dB
- Operation – Remote Control

#### *5.1.3.7.9 Fire Alarm System*

Fire can have disastrous consequences and affect operations of a Control Room. The early detection of fire for effective functioning of the Control Room.

##### **System Description**

- The Fire alarm system shall be a single loop addressable fire detection and alarm system, and must be installed as per NFPA 72 guidelines.
- Detection shall be by means of automatic heat and smoke detectors (multi sensor) 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.

##### **Control and indicating component**

- The control panel shall be a microprocessor based single loop addressable unit, designed and manufactured to the requirements of UL/EN54 Part 2 for the control and indicating component and UL/EN54 Part 4 for the internal power supply.
- All controls of the system shall be via the control panel only.
- The system status shall be made available via panel mounted LEDs and a 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.

### **Manual Controls**

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

### **Smoke detectors**

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

### **Heat detectors**

- Heat detectors shall be of the fixed temperature (58° C) or rate of temperature rise type with a fixed temperature operating point.
- Devices shall be compatible with the CIE conforming to the requirements of UL/ EN54 Part 5 the detectors shall have a single LED to indicate the device has operated and shall fit a common addressable base.
- All bases shall be compatible with the type of detector heads fitted and the control system component used. Each base shall comprise all necessary electronics including a short circuit isolator.
- The device shall be automatically addressed by the CIE on power up of the loop without the need of the insertion of a pre-programmed EPROM or setting of DIL switches.
- Detector bases shall fit onto an industry standard conduit box.
- Addressable Manual Call points must also be provided

- Control & Monitor module must be provided for integration with 3<sup>rd</sup> party systems.

#### **Audible Alarms** –

- Electronic sounders shall be colored red with adjustable sound outputs and at least 3 sound signals. The sounders should be suitable for operation with a 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.

#### **Commissioning**

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

#### ***5.1.3.7.10 ASPIRATING SMOKE DETECTION SYSTEM***

- This specification covers the requirements of design, supply of materials, installation, testing and commissioning of Aspirating Smoke Detection System. The system shall include all equipment's, appliances and labor necessary to install the system, complete with high sensitive LASER-based Smoke Detectors with aspirators connected to network of sampling pipes.

#### **Codes and standards**

- The entire installation shall be installed to comply one or more of the following codes and standards
- NFPA Standards, US
- British Standards, BS 5839 part :1

#### **Approvals**

- All the equipment's shall be tested, approved by any one or more:
- LPCB (Loss Prevention Certification Board), UK
- FM Approved for hazardous locations Class 1,Div 2
- UL (Underwriters Laboratories Inc.), U
- ULC (Underwriters Laboratories Canada), Canada
- Vds (Verband der Sachversicherer e.V), Germany

#### **Design Requirements**

- The System shall consist of a high sensitive LASER-based smoke detector, aspirator, and filter.

- It shall have a display featuring LEDs and Reset/Isolate button. The system shall be configured by a programmer that is either integral to the system, portable or PC based.
- The system shall allow programming of:
  - a) Multiple Smoke Threshold Alarm Levels.
  - b) Time Delays.
  - c) Faults including airflow, detector, power, filter block and network as well as an indication of the urgency of the fault.
  - d) Configurable relay outputs for remote indication of alarm and fault Conditions.
- It shall consist of an air sampling pipe network to transport air to the detection system, supported by calculations from a computer-based design modeling tool.
- Optional equipment may include intelligent remote displays and/or a high-level interface with the building fire alarm system, or a dedicated System Management graphics package.
- Shall provide very early smoke detection and provide multiple output levels corresponding to Alert, Action, and Fire 1 & 2. These levels shall be programmable and shall be able to set sensitivities ranging from 0.025 – 20% obscuration / meter.

#### **Displays on the Detector Assembly**

- The detector will be provided with LED indicators.
- Each Detector shall provide the following features: Alert, Alarm, Fire 1 and Fire 2 corresponding to the alarm thresholds of the detector/Smoke Dial display represents the level of smoke present, Fault Indicator, Disabled indicator

#### **Sampling Pipe**

- The pipe shall be identified as Aspirating Smoke Detector Pipe along its entire length at regular intervals not exceeding the manufacturer's recommendation or that of local codes and standards.

#### **Installation**

- The Contractor shall install the system in accordance with the manufacturer's recommendation.
- Where false ceilings are available, the sampling pipe shall be installed above the ceiling, and Capillary Sampling Points shall be installed on the ceiling and connected by means of a capillary tube.
- Air Sampling Piping network shall be laid as per the approved pipe layout. Pipe work calculations shall be submitted with the proposed pipe layout design for approval.
- The bidder shall submit computer generated software calculations for design of aspirating pipe network, on award of the contract.

#### 5.1.3.7.11 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 entry / exit doors. These doors shall be provided with electric locks and shall operate on fail-safe principle. The lock shall remain unlocked in the event of a fire alarm or in the event of a power failure. The fire alarm supplier shall make potential free contacts available for releasing the locks in a fire 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.

#### 5.1.3.7.12 Rodent Repellent

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

- Configuration : Master console with necessary transducer
- Operating Frequency : Above 20 KHz (Variable)
  - Sound Output : 80 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

**5.1.3.7.13 Structured Cabling Components**

#	Parameter	Minimum Specifications
1.	Standards	ANSI TIA 568 C for all structured cabling components
2.	OEM Warranty	OEM Certification and Warranty of 15-/ 20 years as per OEM standards
3.	Certification	UL Listed and Verified

a

**5.1.3.7.14 Precision Air Conditioning**

The Data Centres Area shall be provided with fully redundant, microprocessor-based, gas-based, Precision Air-Conditioning system. Cool air feed to the Data Centres shall be bottom-charged or downward flow type using the raised floor as supply plenum through perforated aluminium tiles for airflow distribution. The return airflow shall be through the false ceiling to cater to the natural upwardly movement of hot air. Cooling shall be done by the Precision Air-Conditioning system only. Forced cooling using fans on the false floor is not acceptable. Air conditioning shall be capable of providing sensible cooling capacities at the design ambient temperature and humidity with adequate airflow. The Precision Air-Conditioning system shall capable to be integrated with the BMS for effective monitoring.

The SI shall assess, design, supply, transport, store, unpack, erect, and test the successful commissioning and satisfactory completion of trial operations of the Precision Air-Conditioning system for the Data Centres. The SI shall follow ASHRAE Standard for the HVAC and Ducting.

The SI shall be responsible for:

1. Connecting the indoor unit with the mains electrical point
2. Connecting indoor and outdoor units mechanically (with 18-gauge-hard copper piping).
3. Connecting indoor and outdoor unit electrically
4. Nitrogen pressure testing, triple vacuum, and final gas charging
5. Connecting the humidifier feed line with the point provided
6. Connecting the drain line with the point provided
7. Commissioning and handing over the unit to the customer
8. Operation and routine maintenance training for up to two persons nominated by the

CLIENT while commissioning the units at site

### **Temperature Requirements**

The environment inside the Primary and Secondary Data Centers shall be continuously maintained at  $23 \pm 1$  degrees Celsius. The temperature and humidity shall be controlled at desired levels. The necessary alarms for variation in temperatures shall be monitored on a 24/7 basis and logged for providing reports.

### **Indicating Lamps**

1. Indicating lamps assembly shall be screw type with built in resistor having non-fading color lens. LED type lamps are required.
2. Wiring for Remote ON, OFF, TRIP indicating lamps is required.
  - a. ON indicating lamp: Red
  - b. OFF indicating lamp: Green
  - c. TRIP indicating lamp: Amber
  - d. PHASE indicating lamp: Red, Yellow, Blue
  - e. TRIP circuit healthy lamp: Milky

### **Relative Humidity (RH) requirements**

Ambient RH levels shall be maintained at  $50\% \pm 5$  non-condensing. Humidity sensors shall be deployed. The necessary alarms for variation in RH shall be monitored on a 24/7 basis and logged for providing reports.

### **Temperature and Relative Humidity Recorders**

Temperature and relative humidity recorders shall be deployed for recording events of multiple locations within the Primary and Secondary Data Centers. Records of events for the past 7 days shall be recorded and presentable whenever required. Sensors shall be located at various locations within the Primary and Secondary Data Centers to record temperature and humidity automatically.

### **Air Quality Levels**

The Primary and Secondary Data Centers shall be kept at highest level of cleanliness to eliminate the impact of air quality on the hardware and other critical devices. The Primary and Secondary Data Centers shall be deployed with efficient air filters to eliminate and arrest the possibility of airborne particulate matter which may cause air-flow clogging, gumming up of components, causing short-circuits, or blocking the function of moving parts.

### **Additional Points**

1. The precision air conditioners shall be capable of maintaining a temperature range of 23 degrees Celsius with a maximum of  $\pm 1$  degree variation and relative humidity of 50% with a maximum variation of  $\pm 5\%$ .
2. The precision air conditioners shall have two (2) independent refrigeration circuits, each comprised of one scroll compressor, refrigeration circuit and condenser, and dual blowers for flexibility of operations and better redundancy.
3. The unit casing shall be in double-skin construction for longer life of the unit and low noise level.
4. For close control of the Data Centers temperature and relative humidity (RH) environment conditions, the controller shall have proportional integration and differential (PID).
5. The precision unit shall be air-cooled, refrigerant-based system to avoid chilled water in critical space.
6. The internal rack layout design shall follow the cold aisle and hot aisle concept as recommended by ASHRAE.
7. The refrigerant used shall be environmentally friendly HFC, R-407-C or equivalent in view of the long-term usage of the Data Centers equipment as well as the availability of spares and refrigerant.
8. The system shall include fully deployed Dynamic Smart Cooling with auto sequencing and auto power management features.
9. Thermal and computational fluid dynamics(CFD) analysis diagrams shall be provided
10. The fan section shall be designed for an external static pressure of 25 Pa. The fans shall be located downstream of the evaporator coil and be of the electronically commuted, backward, curved, centrifugal type, double-width, double-inlet, and statically and dynamically balanced. Each fan shall be direct-driven by a high efficiency direct current (DC) motor.
11. The evaporator coil shall be A-shape coil for down flow, incorporating draw-through air design for uniform air distribution. The coil shall be constructed of rifled bore copper tubes and louvered aluminum fins with the frame and drip tray fabricated from heavy gauge aluminum. Face area of coil shall be selected corresponding to air velocity not exceeding 2.5 m/sec.
12. Dehumidification shall be achieved by either reducing effective coil area by solenoid valve arrangement or using the dew point method of control. Whenever dehumidification is required, the control system shall enable a solenoid valve to limit the exchange surface of the evaporating coil, thereby providing a lower evaporating temperature.
13. The humidifier and heaters shall be built-in features in each machine individually. Humidification shall be provided by boiling water in a high-temperature, polypropylene steam generator. The steam shall be distributed evenly into the bypass airstreams of

the environment control system to ensure full integration of the water vapor into the supply air without condensation. The humidifier shall have an efficiency of not less than 1.3 kg/kw and be fitted with an auto-flush cycle activated on demand from the microprocessor control system. The humidifier shall be fully serviceable with replacement electrodes. Wastewater shall be flushed from the humidifier by the initiation of the water supply solenoid water valve via a U-pipe overflow system. Drain solenoid valves shall not be used. A microprocessor shall control the humidification and heating through suitable sensors.

14. The following microprocessor controls features shall be displayed on the units:
  - a. Room temperature and humidity
    - i. Supply fan working status
    - ii. Compressor working status
    - iii. Condenser fans working status
    - iv. Electric heaters working status
    - v. Humidifier working status
    - vi. Manual/Auto unit status
    - vii. Line voltage value
  - b. Temperature set point
    - viii. Humidity set point
    - ix. Working hours of main component i.e. compressors, fans, heater, humidifier.
    - x. Unit working hours
    - xi. Current date and time
    - xii. Type of alarm (with automatic reset or block)
    - xiii. The last 10 intervened alarms
15. The microprocessor shall be able to perform following functions:
  - c. Testing of the working of display system
  - d. Password for unit calibration values modification
  - e. Automatic restart of program
  - f. Cooling capacity control
  - g. Compressor starting timer
  - h. Humidifier capacity limitation
  - i. Date and time of last 10 intervened alarm
  - j. Start/Stop status storage
  - k. Random starting of the unit.
  - l. Outlet for the connection to remote system
  - m. Temperature and humidity set point calibration
  - n. Delay of general alarm activation

- o. Alarm calibration
- 16. Following alarms shall be displayed on screen of microprocessor unit:
  - p. Air flow loss
  - q. Clogged filters
  - r. Compressor low pressure
  - s. Compressor high pressure
  - t. Smoke /Fire
  - u. Humidifier low water level
  - v. High/Low room temperature
  - w. High/Low room humidity
  - x. Spare external alarms
  - y. Water under floor
- 17. The control system shall include the following settable features:
  - z. Unit identification number
  - aa. Start-up delay, cold start delay, and fan run on timers
  - bb. Sensor calibration
  - cc. Remote shutdown and general alarm management
  - dd. Compressor sequencing
  - ee. Return temperature control
  - ff. Choice of modulating output types
- 18. The unit shall incorporate the following protections:
  - gg. Single phasing preventers
  - hh. Reverse phasing
  - ii. Phase misbalancing
  - jj. Phase failure
  - kk. Overload tripping (MPCB) of all components

**5.1.3.7.15 DG Set**

#	Parameter	Requirement Description	Compliance	Remarks
---	-----------	-------------------------	------------	---------

#	Parameter	Requirement Description	Compliance	Remarks
1	General Specifications	Auto Starting DG Set Mounted on a common based frame with AVM (Anti- Vibration) pads, residential silencer with exhaust piping, complete conforming to ISO 8528 specifications and CPCB certified for emissions. KVA rating as per the requirement.		
2	Capacity	Minimum 325 KVA		
3	Fuel	High Speed Diesel (HSD) With 30 Ltr Tank Capacity or better. It should be sufficient and suitable for containing fuel for 12 hours continuous operation, Complete with level indicator, fuel inlet and outlet, air vent, drain plug, inlet arrangement for direct filling and set of fuel hoses for inlet and return.		
4	Power Factor	0.8		
5	Engine	Engine should support electric auto start, water cooled, multi cylinder, maximum 1500 rpm with electronic/manual governor and electrical starting arrangement complete with battery, 4 stroke multiple cylinders/single and diesel operated conforming to BS 5514/ ISO 3046/ IS 10002		
6	Alternator	Self-exciting, self-regulating type alternator rated at 0.8 PF or better, 415 Volts, 3 Phase, 4 wires, 50 cycles/sec, 1500 RPM, conforming to IS 4722/ BS 5000, Windings of 100% Copper, class H insulation, Protection as per IP 23.		
7	AMF (Auto Main Failure) Panel	AMF Panel fitted inside the enclosure, with the following meters/indicators: <ul style="list-style-type: none"> <li>• Incoming and outgoing voltage</li> <li>• Current in all phases</li> <li>• Frequency</li> <li>• KVA and power factor</li> <li>• Time indication for hours/ minutes of operation</li> <li>• Fuel Level in field tank, low fuel indication</li> <li>• Emergency Stop button</li> <li>• Auto/Manual/Test selector switch</li> <li>• MCCB/Circuit breaker for short-circuit and overload protection</li> <li>• Control Fuses</li> <li>• Earth Terminal</li> <li>• Any other switch, instrument, relay etc essential for Automatic functioning of DG set with AMF panel</li> </ul>		

#	Parameter	Requirement Description	Compliance	Remarks
8	Acoustic Enclosure	<ul style="list-style-type: none"> <li>The DG set shall be provided with acoustic enclosure / canopy to reduce the sound level and to house the entire DG set (Engine &amp; Alternator set) assembly outside (open-air).</li> <li>The enclosure shall be weather resistant powder coated, with insulation designed to meet latest MOEF/CPCB norms for DG sets, capable to withstand Mumbai climate. The enclosure shall have ventilation system, doors for easy access for maintenance, secure locking arrangement, complete</li> </ul>		
9	Output Frequency	50 Hz		
10	Tolerance	+/- 5% as defined in BSS-649-1958		
11	Enclosure	Acoustic enclosure with provision for a fuel tank		
12	Indicators	Over speed /under speed/High water temperature/low lube oil etc.		
13	Intake system	Naturally Aspirated		
14	Certifications	ISO 9001/9002, relevant BS and IS standard.		

#### 5.1.3.7.16 Other Requirements

- 1) The Command and Communications Center will be the nodal point of availability of all online data and information related to various current and future smart elements and will be connected to other network of services in Chennai through an integration layer.
- 2) The CCC will be established with all hardware, software and network infrastructure including switches and routers and will be maintained by the successful bidder throughout the mentioned period. Authority takes the responsibility of necessary civil work including furniture.
- 3) All required Servers, Storage, Software, Firewall, Network Switches for entire project shall be installed in an integrated manner.
- 4) The controls and displays should be mounted in ergonomically designed consoles to keep the operator's fatigue to a minimum and console's efficiency high.
- 5) Integration with Telecom / Internet service providers would aid in automatically capturing the CDR database for person of interest
- 6) **Security:** Under no circumstances the data accumulated and processed by Command and Control should be compromised. Hence, provisions will be made to keep all the data stored in the platform that is highly secured with required security framework implementation. The platform will be hosted in Data center at a location decided by Authority to be provided by successful bidder. Further the platform will provide an open

standardsbased Integration Bus with API Management, providing full API lifecycle management with governance and security.

#### 5.1.4 Technical Specifications

##### 5.1.4.1 Video Wall Screen

The Video Wall for CCC shall be configured with 6x3 formation of the following Professional Display (TV) Screens:

#	Parameter	Minimum Specifications
1	Videowall Grid	Videowall in the matrix of 12x2 scalable up to 14x3.
2	Screen	50" or higher - DLP Cube- With Laser Light Source – SLIM Cube
3	Resolution	Full high definition (1920X1080) 16:9 Widescreen
4	Contrast ratio	1800:1
5	Brightness	700 nit
6	Viewing angle	178 degree/178 degree (H/V)
7	Access to the Cube	Front Access
8	Input	HDMI
9	Control	- On Screen Display (OSD) - IR remote control
10	Operations	24 x 7, Life of light source 100000 hrs in eco-mode.
11	Standards	BIS or equivalent

##### 5.1.4.2 Video Wall Controller

#	Parameter	Minimum Specifications
1	Controller	Controller to control Video wall of 42 output cubes (considering future scalability) as per requirement along with software
2	Chassis	19" Rack mount
3	Processor	Latest Generation 64 bit x86 Quad Core processor (3.4 Ghz) or better
4	Operating System	Pre-loaded 64-bit Operating System Windows / Linux / Equivalent, with recovery disc
5	RAM	16 GB DDR3 ECC RAM
6	HDD	2x500 GB 7200 RPM HDD (Configured in RAID 0)



#	Parameter	Minimum Specifications
7	Networking	Dual-port Gigabit Ethernet Controller with RJ-45 ports
8	RAID	RAID 0, 1, 5, 10 support
9	Power Supply	( 1+1) Redundant hot swappable
10	Accessories	104 key Keyboard and Optical USB mouse
11	USB Ports	Minimum 4 USB Ports
14	Redundancy support	Power Supply, HDD, LAN port & Controller
15	Scalability	Display multiple source windows in any size, anywhere on the wall
16	Control functions	Brightness/ Contrast/ Saturation/ Hue/ Filtering/ Crop/ Rotate
17	Inputs	To connect to minimum 24 Universal Port.
18	Output	To connect to minimum 42 Displays through HDMI
19	Operating Temperature	10°C to 35°C, 80 % humidity
20	Cable & Connections	Successful bidder should provide all the necessary cables and connectors, so as to connect Controller with Display units
21	Integration	Seamless integration among display unit, controller, wall management software to be ensured. Preferred to have same OEM.

#### 5.1.4.3 Video Wall Management Software

#	Parameter	Minimum Specifications
1	Display & Scaling	Display multiple sources anywhere on display up to any size
2	Input Management	All input sources can be displayed on the video wall in freely resizable and movable windows
3	Scenarios management	Save and load desktop layouts from local or remote machines
4	Layout Management	Support all layout from input sources, Internet Explorer, desktop and remote desktop application
5	Multi View Option	Multiple view of portions or regions of Desktop, multiple application can view from single desktop
6	Other features	SMTP support
7		Remote Control over LAN
8		Alarm management
9		Remote management
10		Multiple concurrent client
11		KVM support
12	Cube Management	Cube Health Monitoring
13		Pop-Up Alert Service
14		Graphical User Interface

#### 5.1.4.4 Monitoring Workstations

#	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 ECC Memory @ 1600 Mhz. Slots should be free for future upgrade. Minimum 4 DIMM slots, supporting up to 32GB ECC
5.	Graphics card	Minimum Graphics card with 2 GB video memory (non- shared)
6.	HDD	2 TB SATA-3 Hard drive @7200 rpm with Flash Cache of 64GB SSD. Provision for installing 4 more drives.
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.	PTZ joystick controller <i>(with 2 of the workstations in CCC)</i>	<ul style="list-style-type: none"> <li>• PTZ speed dome control for IP cameras</li> <li>• Minimum 10 programmable buttons</li> <li>• Multi-camera operations</li> <li>• Compatible with all the camera models offered in the solution</li> <li>• Compatible with VMS /Monitoring software offered</li> </ul>
14.	Monitor	22" TFT LED monitor, Minimum 1920 x1080 resolution, 5 ms or better response time, TCO 05 (or higher) certified
15.	Certification	Energy star 5.0/BEE star certified
16.	Operating System	64 bit pre-loaded OS with recovery disc
17.	Security	BIOS controlled electro-mechanical internal chassis lock for the system.

#	Parameter	Minimum Specifications
18.	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)
19.	Power supply	SMPS; Minimum 400-watt Continuous Power Supply with Full ranging input and APFC. Power supply should be 90% efficient with EPEAT Gold certification for the system.

#### 5.1.4.5 Network Colour Laser Printer

#	Parameter	Minimum Specifications
1.	Print Speed	<b>Black : 16 ppm or above on A3, 24 ppm or above on A4 Colour : 8 ppm or above on A3, 12 ppm or above on A4</b>
2.	Resolution	<b>600 X 600 DPI</b>
3.	Memory	<b>8 MB or more</b>
4.	Paper Size	<b>A3, A4, Legal, Letter, Executive, custom sizes</b>
5.	Paper Capacity	<b>250 sheets or above on standard input tray, 100 Sheet or above on Output Tray</b>
6.	Duty Cycle	<b>25,000 sheets or better per month</b>
7.	OS Support	<b>Linux, Windows 2000, Vista, 7, 8, 8.1</b>
8.	<b>Interface</b>	<b>Ethernet Interface</b>

#### 5.1.4.6 IP Phone Specifications

#	Parameter	Minimum Specifications
1.	Display	2 line or more, Monochrome display for viewing features like messages, directory etc.
2.	Integral switch	10/100 mbps for a direct connection to a 10/100BASE-T Ethernet network through an RJ-45 interface
3.	Speaker Phone	Yes
4.	Head set	Port for Head set (Headset also to be provided)

#	Parameter	Minimum Specifications
5.	VoIP Protocol	SIP V2
6.	PoE	IEEE 802.3af or better
7.	Supported Protocols	SNMP, DHCP, DNS
8.	Codecs	G.711, G.722 including handset and speakerphone
9.	Speaker Phone	Full duplex speaker phone with echo cancellation Speaker on/ off button, microphone mute
10.	Volume control	Easy decibel level adjustment for speaker phone, handset and ringer
11.	Phonebook/Address book	Minimum 100 contacts
12.	Call Logs	Access to missed, received, and placed calls. (Minimum 20 overall)
13.	Clock	Time and Date on display
14.	Ringer	Selectable Ringer tone
15.	Directory Access	LDAP standard directory

IP PBX to support minimum 500 IP Phones with at least 100 concurrent sessions with features like –

- Provide reports for calls based on records, calls on a user basis, calls through gateways etc.
- Able to add bulk add, delete, and update operations for devices and users
- Session Initiation Protocol (SIP) Trunk support
- Centralized, configuration database, Web based management
- Lightweight Directory Access Protocol (LDAP) directory interface
- Facilities to users like Call Back, Call Forward, Directory Dial, Last number Redial, etc.
- Calling Line Identification

#### 5.1.4.7 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
11.	Max. loop resistance for analog trunk lines	1200 ohms at –48 Volts DC
12.	Other	<ul style="list-style-type: none"> <li>• ISDN supplementary services for Digital phone</li> <li>• Support for digital trunk lines</li> <li>• Working on 230v AC mains and DC voltage</li> </ul> <p>Support for ACD call center with CTI and advanced call routing</p>
13.	Design of EPABX System	<ul style="list-style-type: none"> <li>• Modular with universal slots, wall mountable</li> </ul>
14.	Conferencing	<ul style="list-style-type: none"> <li>• 5 party conferencing to be provided (to be configurable dynamically)</li> </ul>
15.	Digital / IP Extension telephone instrument programmable one touch keys	<ul style="list-style-type: none"> <li>•</li> </ul>

	with	
--	------	--

#### 5.1.4.8 Desktop

#	Item	Minimum Specifications
1	Make	Must be specified
2	Model	Must be specified
3	Processor	Intel Core i5-latest generation (3.0 Ghz) or higher OR AMD A10 7850B (3.0 Ghz) processor or higher OR Equivalent 64 bit x86 processor
4	Memory	8 GB DDR3 RAM @ 1600 MHz. One DIMM Slot must be free for future upgrade
5	Motherboard	OEM Motherboard
6	Hard Disk Drive	Minimum 500 GB SATA III Hard Disk @7200 RPM or higher
7	Audio	Line/Mic In, Line-out/Speaker Out (3.5 mm)
8	Network port	10/100/1000 Mbps auto-sensing on-board integrated RJ-45 Ethernet Port
9	Wireless Connectivity	Wireless LAN - 802.11b/g/n/
1	USB Ports	Minimum 4 USB ports (out of that 2 must be in front)
1	Display Port	1 Display Port (HDMI/VGA ) port
1	Power supply	Maximum Rating 250 Watts, 80 plus certified power supply
1	Keyboard	104 keys Heavy Duty Mechanical Switch Keyboard (USB Interface) with 50 million keystrokes life per switch. Rupee Symbol to be engraved.
1	Mouse	Optical with USB interface (same make as desktop)
1	Monitor	Minimum 18.5" diagonal LED Monitor with 1366x768 or higher resolution. (Same make as desktop). Must be TCO05 certified

#	Item	Minimum Specifications
1	Operation System and Support	Pre-loaded Windows 10 Pro (or latest) Professional, licensed copy with certificate of authenticity (or equivalent authenticity information) and all necessary and latest patches and updates. Can be downgraded to Windows 7 Professional (64 bit).All Utilities and driver software, bundled in CD/DVD/Pen-drive media
1	Certification for Desktop	Energy Star 5.0 or above / BEE star certified
1	Other pre-loaded software (open source/free)	Latest version of Libre-office, Latest version of Adobe Acrobat Reader, Scanning Software (as per scanner offered). These software shall be pre-loaded (at the facility of OEM or any other location) before shipment to Authority offices/locations.

#### 5.1.4.9 Laptop

Sr No	Item	Minimum Specifications
1.	Make	Must be specified
2.	Model	Must be specified
3.	Processor	Our suggestion : Intel Core i3 with latest generation (1.9 Ghz) or higher OR AMD A10 PRO 7300 (1.9Ghz) Processor or higher OR Equivalent 64 bit x86 processor
4.	Display	Minimum 14" Diagonal TFT Widescreen with minimum 1366 x 768 resolution (16:9 ratio)
5.	Memory	4 GB DDR3 RAM @ must be free for future upgrade
6.	Hard Disk Drive	Minimum 500 GB SATA HDD @ 5400 rpm
7.	Ports	3 USB Ports 1- Gigabit LAN (RJ 45); 1- HDMI/Display port, 1- VGA, 1- headphone/Microphone;
8.	Web Camera	Built in web cam
9.	Wireless Connectivity	Wireless LAN - 802.11b/g/n/ Bluetooth 3.0
10.	Audio	Built-in Speakers

Sr No	Item	Minimum Specifications
11.	Battery backup	Minimum 4 lithium ion or lithium polymer battery with a backup of minimum 4 hours
12.	Keyboard and Mouse	84 Keys Windows Compatible keyboard, Integrated Touch Pad.
13.	Operating System	Pre-loaded Windows 8.1 (or latest) Professional 64 bit, licensed copy with certificate of authenticity (or equivalent authenticity information) and all necessary and latest patches and updates. Can be downgraded to Windows 7 Professional (64 bit).  All Utilities and driver software, bundled in CD/DVD/Pen-drive media
14.	Certification	Energy Star 5.0 or above / BEE star certified
15.	Weight	Laptop with battery (without DVD) should not weigh more than 2 Kg
16.	Accessories	Laptop carrying Back-pack. It must be from same OEM as laptop
17.	Other pre-loaded software (open source/ free)	Latest version of Libre-office, Latest version of Adobe Acrobat Reader Scanning Software (as per scanner offered). These software shall be pre-loaded (at the facility of OEM or any other location) before shipment to Authority offices/locations.

#### 5.1.4.10 Online UPS

#	Parameter	Minimum Specifications
1.	Capacity	<b>Adequate capacity to cover all above IT Components at respective location</b>
2.	Output Wave Form	<b>Pure Sine wave</b>
3.	Input Power Factor at Full Load	<b>&gt;0.90</b>
4.	Input	<b>Three Phase 3 Wire for over 10 KVA</b>
5.	Input Voltage Range	<b>305-475VAC at Full Load</b>
6.	Input Frequency	<b>50Hz +/- 3 Hz</b>
7.	Output Voltage	<b>400V AC, Three Phase for over 10 KVA UPS</b>



#	Parameter	Minimum Specifications
8.	Output Frequency	<b>50Hz+/- 0.5% (Free running); +/- 3% (Sync. Mode)</b>
9.	Inverter efficiency	<b>&gt;90%</b>
10.	Over All AC-AC Efficiency	<b>&gt;85%</b>
11.	UPS shutdown	<b>UPS should shutdown with an alarm and indication on following conditions 1)Output over voltage 2)Output under voltage 3)Battery low 4)Inverter overload 5)Over temperature 6)Output short</b>
12.	Battery Backup	<b>30 minutes in full load</b>
13.	Battery	<b>VRLA (Valve Regulated Lead Acid) SMF (Sealed Maintenance Free) Battery</b>
14.	Indicators & Metering	<b>Indicators for AC Mains, Load on Battery, Fault, Load Level, Battery Low Warning, Inverter On, UPS on Bypass, Overload, etc. Metering for Input Voltage, Output Voltage and frequency, battery voltage, output current etc.</b>
15.	Audio Alarm	<b>Battery low, Mains Failure, Over temperature, Inverter overload, Fault etc.</b>
16.	Cabinet	<b>Rack / Tower type</b>
17.	<b>Operating Temp</b>	<b>0 to 40 degrees centigrade</b>

**5.1.4.11 Fixed Dome Camera for Indoor Surveillance**

#	Parameter	Minimum Specifications or better
1.	Video Compression	H.264
2.	Video Resolution	1920 X 1080
3.	Frame rate	Min. 25 fps
4.	Image Sensor	1/3" Progressive Scan CCD / CMOS
5.	Lens Type	Varifocal, C/CS Mount, IR Correction Full HD lens compatible to camera imager
6.	Lens#	Auto IRIS 2.8-10mm
7.	Multiple Streams	Dual streaming with 2 <sup>nd</sup> stream at minimum 720P at 30fps at H.264 individually configurable
8.	Minimum Illumination	Colour: 0.1 lux, B/W: 0.01 lux (at 30 IRE)
9.	IR Cut Filter	Automatically Removable IR-cut filter
10.	Day/Night Mode	Colour, Mono, Auto
11.	S/N Ratio	≥ 50 dB
12.	Auto adjustment + Remote Control of Image settings	Colour, brightness, sharpness, contrast, white balance, exposure control, backlight compensation, Gain Control, Auto back focus
13.	Wide Dynamic Range	True WDR upto 80 db
14.	Audio	Full duplex, line in and line out, G.711, G.726
15.	Local storage	microSDXC up to 32GB (Class 10) In the event of failure of connectivity to the central server the camera shall record video locally on the SD card automatically. After the connectivity is restored these recordings shall be automatically merged with the server recording such that no manual intervention is required to transfer the SD card based recordings to server.
16.	Protocol	HTTP, HTTPS, FTP, RTSP, RTP, TCP, UDP, RTCP, DHCP, ONVIF Profile S & G
17.	Security	Password Protection, IP Address filtering, User Access Log, HTTPS encryption
18.	Intelligent Video	Motion Detection & Tampering alert
19.	Alarm I/O	Minimum 1 Input & Output contact for 3 <sup>rd</sup> part interface

#	Parameter	Minimum Specifications or better
20.	Operating conditions	0 to 50°C
21.	Casing	NEMA 4X / IP-66 rated & IK 09
22.	Certification	UL2802 / EN, CE ,FCC
23.	Power	802.3af PoE (Class 0) and 12VDC/24AC

#### 5.1.4.12 LCD 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

#### 5.1.4.12.1 Technical Specification for Data Analytics & IOT – Enterprise Service Bus Integration Capabilities

The CCC architecture proposed shall have the following layers;

1. Presentation layer
2. Application layer
3. Data analytics layer

The presentation layer consists of web view and the mobile app. The data analytics platform and the application layer work in synchronous with each other. Machine learning and business rule engine comes under the framework management tools. The external systems consists data from ERP, smart poles (WiFi, LEDs and Air quality sensor), VMS & violation analytics, environmental sensors, emergency call box, public address system & variable

display boards, smart bins, social media streams and contact centers. This whole system can be accessed either through video wall, web access or a phone/tablet.

The proposed CCC shall be built on n-tier SOA (Service Oriented Architecture) architecture. The business layer, data access layer, service layer and presentation layer forms the layers of the architecture to make the CCC robust with respect to the business functionality without compromising on the security.

All the modules communicate to each other using Web Services and Message brokers which accelerate eventual integration to any legacy systems. In case of complex environments, the Enterprise Service Bus (ESB), Message Queue for rapid internal and external integration, can handle this communication.

The system shall provide seamless and transparent integration with most popular open source and commercial Enterprise Service Bus providers.

The integrated Enterprise Service Bus (ESB) shall provide an interface for accessing the external systems like GIS, Kiosks, AMR, SCADA, Asset Management, Network Management, various sensors etc. An ESB acts as a shared messaging layer for connecting the applications and other services throughout an enterprise-computing infrastructure.

- 1) The CCC 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 CCC 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 CCC 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) CCC will monitor the KPIs for all sub systems which are integrated with it and in case of emergency or exigency or KPI breach a new incident will be generated on the CCC platform with the CC dashboarding reporting this KPI breach with a new color code. Such escalated incidents will follow a pre-defined SOP for each sub system type. In case of a dispatch the CCC should support this as an automated procedure or a manual procedure.
- 6) The proposed Command & Control Center Platform shall have the following integration functionality and modules.

#		Functionality Description
1.	Data Normalization capabilities	<p>It is envisaged that the city will implement multiple Smart City use cases over a period of time. The potential example Smart City use cases are-</p> <ul style="list-style-type: none"> <li>• Smart Outdoor Lighting</li> <li>• Smart Parking</li> <li>• Smart Traffic Management</li> <li>• Smart Energy Metering</li> <li>• Smart Water Metering</li> <li>• Public Safety and Safe City Operations</li> <li>• Connected Public Transport</li> <li>• Public Wi-Fi and Urban Service Delivery over Public Wi-Fi</li> <li>• Kiosks for Citizen Information</li> <li>• Citizen Interactive Kiosks for Urban Service Delivery</li> <li>• Environmental Monitoring</li> <li>• Smart Waste Management</li> <li>• Surveillance system including Facial Recognition, video Analytics etc.</li> <li>• And other integrations as per defined scope</li> </ul>
2.		The platform shall Connect with any external data source feeds (like social media, sensors, information systems...) using light-weight adapters (either built-in, provided by the community or custom-built)
3.		The platform shall provide real-time data transformations (for translation from one information system format to another)
4.		The platform shall provide real-time analysis of incoming data (e.g. generating a floating last 10 seconds' average of water consumption reads from smart water-meters)
5.		The platform shall provide real-time logic and routing applied to incoming data streams (e.g. create a new incident when above floating

#	Functionality Description	
		average water consumption exceeds standard deviation by more than 30%, route high & low reads to different streams for continued processing)
6.		The platform shall provide seamless integration with CCC to receive and analyze its incoming sensor data, invoke actions on it and provide full analytical data for dashboarding etc..
7.		The platform should also allow the manufacturers of the sensors to develop integrations themselves using SDKs without affecting the northbound applications and existing integration
8.		The platform should be able to normalize the data coming from different devices of same type (i.e. Different lighting sensor from different OEMs, different energy meters from different OEMs etc.) and provide secure access to that data using data API(s) to application developers.
9.		The platform should support distributed deployment of functions (workflows & policies) across city's network and compute infrastructure with centralized management and control.
10.	GIS Map Support	System should support Esri, map box, Open standard GIS etc.
11.	Location engine	<ul style="list-style-type: none"> <li>a) Map services and geospatial coordinates: provides the geographical coordinates of specific facilities, roads, and city infrastructure assets, as well as unmapped facilities</li> <li>b) Geospatial calculation: calculates distance between two, or more, locations on the map</li> <li>c) Location-based tracking: locates and traces devices on the map</li> </ul>
12.	Device engine	<ul style="list-style-type: none"> <li>a) Aggregation and abstraction of sensors: provides aggregation of sensors from diverse sensor cloud</li> <li>b) Normalization of sensor data: organizes sensor data and assigns attributes based on relations; raw data removed and passed to data engine</li> </ul>
13.	Data and Analytics engine	<ul style="list-style-type: none"> <li>a) Data archive and logging: stores data feeds from the device engine and external data sources.</li> <li>b) Analytics: provides time-shifted or offline analytics on the archived data.</li> <li>c) Reporting: delivers reports based on events triggered by device engine data and external notifications.</li> </ul>
14.	Service management	a) Data brokerage, ID Management: Performs service management.
15.	Developer Program tools	Sensor platform OEM should provide online Developer Program tools that help City to produce new applications, and/or use solution APIs to

#	Functionality Description	
		enhance or manage existing solution free of cost. OEM should have technology labs via an online public facing web interface. These labs should be available 24X7.
16.	Authentication , Authorization	System should support standard Authentication, Authorization Performs.
17.	Data plan Functionalities	Live data and visual feed from diverse sensors connected to the platform.
18.	API Repository / API Guide	Normalized APIs should be available for the listed domains (Parking, Outdoor Lighting, Traffic, Environment, Urban mobility etc.) to monitor, control sensor and/or actuators functionality to enable app developers to develop apps on the platform. For example Lighting APIs: Vendor agnostic APIs to control Lighting functionality.
19.		Platform OEM should have published the normalized APIs in their website for the listed domains ((Parking, Outdoor Lighting, Traffic, Environment, Urban mobility etc.) to allow sensor vendors and app developers to develop their connectors / adaptors to the platform.
20.	Platform upgrade and maintenance	The OEM should be able to securely access the platform remotely for platform updates / upgrades and maintenance for the given duration.
21.		Platform should be able to be deployed on a public cloud for disaster recovery.
22.	Platform functionality	API management and gateway: Provides secure API lifecycle, monitoring mechanism for available APIs.
23.		User and subscription management: Provides different tier of user categorization, authentication, authorization, and services based on the subscriptions
24.		Application management: Provides role-based access view to applications
25.		Enabling analytics: Time shifted and real-time data available for big data and analytics
26.		The platform should also be able to bring in other e-governance data (SCADA systems) as i-frames in the command and control centre dashboard
27.		All of these data should be rendered / visualized on the command and control centre dashboard.
28.	Integration capabilities	This platform is expected to integrate various urban services devices at the street layer so that urban services applications can be developed on top of this platform independent of the technology that is used in the devices.
29.		Integrate devices using their APIs in to this platform. For example, if the City wants to deploy Smart Parking solution, this platform should have

#	Functionality Description	
		the ability and provision to write adaptors which interface with the parking sensors or management software of the parking sensors to collect parking events, data and alerts and notifications from the devices and their software managers.
30.		The platform should be able to integrate any type of parking sensor irrespective of the technology used. For example, some parking sensors might use RF technology like LoRa or ZigBee to communicate the data and events, some might use GPRS or some might use Wi-Fi. Some parking sensors might use infra-red based detection, some might use magnetic field based detection or combination of the both where as some might use a video camera to detect parking occupancy. Irrespective of the technology, the platform should be able to integrate with these devices and their software managers and provide the data from such devices in a normalized and standard based data models.
31.		The same logic and requirement applies to various other urban services devices like LED control nodes, water meters, energy meters, environmental sensors, waste bin sensors, device embedded in connected vehicles etc.
32.		Enables the City and its partners to define a standard data model for each of the urban services domains (i.e. Parking, lighting, kiosks etc...)
33.		Enables City and/or its partners to write software adaptors based on the API(s) provided by device vendors and have the ability to control, monitor and collect the data from these street devices
34.	Trending Service	System should provide trends in graphical representation from data sources over a period of time. Trends should allow to monitor and analyze device performance over time.
35.	Policies and Events	System should allow policy creation to set of rules that control the behavior of infrastructure items. Each policy should a set of conditions that activate the behavior it provides. System should allow Default, Time-based, Event-based and Manual override polices creation. For example, an operator might enforce a "no parking zone" policy manually to facilitate road repairs.
36.		System should provision to defines a set of conditions that can be used to trigger an event-based policy
37.	Notifications, Alerts and Alarms	System should generate Notification, Alert and Alarm messages that should be visible within the Dashboard and the Enforcement Officer Mobile App if required.



#	Functionality Description	
38.		All system messages (notifications, alerts and alarms) should always visible from the Notifications view, which provides controls that operator can use to sort and filter the messages that it displays.
39.		Systems should deliver message to a set of subscribers. The Notification service should support min two types of notification methods – Email notification and Short Messaging Service (SMS) notification.
40.	Users and roles	Users access the perform various tasks, such as adding new locations, configuring new devices, managing adapters, and so on. However, not all users can perform all tasks. Each user should be associated with one or more roles and each role is assigned a certain set of permissions.
41.		These roles and permissions define the tasks that a user can perform. Additionally, system should assign one or more locations to each role so that the user can perform tasks at the assigned locations only.
42.		Roles and permissions define the tasks that a user can perform, such as adding users, viewing location details, exporting devices, generating reports, and so on. Each user should be associated with one or more roles and each role has an assigned set of permissions.
43.		The platform should allow different roles to be created and assign those roles to different access control policies.
44.		Since this platform is being used for managing Cities, the platform should also allow association of users and locations. For example, the platform should allow creation of locations in the system which correspond to various physical locations in the city and allow the admin to associate different users to different locations with the intent that each user can control only services for a location for which has been given access.
45.		System should support LDAP to be used as an additional data store for user management and authentication.
46.	Service Catalog Management	The Service catalog management module should allow to categorize the externalized and non-externalized services into logical groups by creating the service catalogs. In addition, system should allow manage the service catalogs by adding, modifying, or deleting the catalog details.
47.	Reports	The platform should have capability to provide access to real time data and historical data from various connected devices for reporting and analytics.

#	Functionality Description	
48.		System should allow dashboard to generate reports and have provision to add reports in favorites list
49.	Data Security	The access to data should be highly secure and efficient.
50.		Access to the platform API(s) should be secured using API keys.
51.		Software should support security standards: OAuth 2.0, HTTPS over SSL, and key management help protect the data across all domains.
52.		The analytic engine should support querying using associative query options where users selects rows and columns interactively without actually creating anything – no data models/views etc...
53.	Global Market Presence & Support System	Smart city suppliers should be adaptable to the emerging needs of cities. Suppliers should develop offerings that meet the growing interest in urban Internet of Things (IoT) applications, big data solutions, and the transformation in city approaches to energy policy, urban mobility, and city resilience.
54.	Enterprise resource planning (ERP) integration	System should allow integration of business process in ERP workflows like property tax collection etc.
55.		System should allow ERP data visualization at city dashboard
56.		The platform should have the capability to retrieve data directly from ERP systems. The APIs should be RESTful and return the data in JSON format.
57.		The platform should also have the capability to read data directly from a set of databases (HBase, MongoDB, Oracle, Cassandra, MySQL, Impala). To connect to any of the databases information on how to connect should be provided.
58.		System should be able to read data from flat CSV files.
59.	Digital billboards integration	System should share city data to Digital billboards application in API format, Digital billboards management software will do business correlation and push content for outdoor display.
60.	Analytics Engine	Analytics Engine should be an artificial intelligence-based smart city analytics platform module to maximize business value through advanced machine learning capabilities. The machine learning capabilities aid in automating policies that result in better asset and infrastructure management.

#	Functionality Description	
61.		The solution should be flexible to integrate with other city and government software applications.
62.		<p>Analytics Engine module should have below intelligence capabilities;</p> <ul style="list-style-type: none"> <li>a) Advanced Predictive Analytics should be part of the solution.</li> <li>b) The solution should be flexible to integrate with other city and government software applications</li> <li>c) The solution should be able to predict insights consuming data from city infrastructure viz., Traffic, Parking, Lighting etc.</li> <li>d) The solution should have predictions with measurable accuracy of at least &gt; 70%</li> <li>e) The solution should be able to predict and integrate with Smart City solutions helping in driving operational policies creation.</li> <li>f) The solution should be robust, secure and scalable.</li> <li>g) The solution should have a visualization platform to view historic analytics</li> </ul>
63.		<p>The application should enable the customers to discover, compare, and correlate data across heterogeneous data sources to unravel the patterns that are previously hidden. At a broader level, when you work with the application, system do the following tasks:</p> <ul style="list-style-type: none"> <li>a) Connect to a variety of data sources</li> <li>b) Analyze the result set</li> <li>c) Visualize the results</li> <li>d) Predict outcomes</li> </ul>
64.		<p>Analytics Engine should support multiple Data Sources. Min below standard data sources should be supported from day 1 –</p> <p>CSV, TSV, MS Excel, NoSQL, RDBMS</p>
65.		<p>Analytics Engine should provide analysis of data from a selected data source(s).</p> <p>Analysis enables to define arithmetic and aggregation operations that result in the desired output.</p> <p>Analytics engine should provide capability to check analysis with multiple predictive algorithms</p>
66.	Analytics Engine Visualizations	<p>Analytics Engine should provide visualizations dashboard.</p> <p>In the visualization workspace it should allow to change visual attributes of a graph.</p> <p>User should not be allowed to alter the graph/visualization definition.</p>

#	Functionality Description	
		<p>In the visualizations workspace, user should able to do the following operations:</p> <ol style="list-style-type: none"> <li>Change the graph/visualization type</li> <li>Print the graph</li> <li>Export the graph</li> <li>Narrow down on the value ranges</li> <li>Toggle the axis labels</li> <li>Integrate with other 3<sup>rd</sup> party applications seamlessly</li> </ol>
67.	Export Formats	<p>System should allow export the analysis into min following formats:</p> <ol style="list-style-type: none"> <li>XML/JSON</li> <li>Excel</li> <li>PDF</li> <li>CSV</li> </ol>
68.	Predictive Analytics	<ol style="list-style-type: none"> <li>Predictive or advanced analytics to make forecasting and prediction of unknown events. The system analytics should use techniques for data mining, statistics, modelling, machine learning and artificial intelligence to analyze data to make predictions.</li> <li>The system should use data mining, predictive modelling and analytical techniques to bring together the management, information technology, and modelling business strategies.</li> <li>The system should identify the risks based on the patterns from historical transaction data. The predictive analytics models should capture relationship among many factors to assess risks with particular set of conditions to assign score or weightage.</li> </ol>

#### 5.1.4.13 Technical Specification for E-Governance Portal

The e-Governance portal shall be integrated with the all the ERP modules of the existing ERP system. It is the responsibility of the bidder to develop the e-Governance portal and integrate the exiting ERP system with the portal.

##### 5.1.4.13.1 Web Portal

The current website of Authority needs to be replaced to a more elaborate web portal which would facilitate the two way communication between citizens and the administrations

- ❖ The basic functionalities required for the Web portal are:
  - **Information Dissemination:** The Web portal shall provide information about Chennai City (such as history, heritage details, city guide), Details of Greater Chennai Corporation (Elected Political Members, Mayor, Municipal

Commissioner of the city, Budget, Administrative Wing, Zonal Information, etc.) various Citizen Centric details/applications, grievance Redressal, Details of all Authority Officials (Emails, Employee Orders, contact information, etc.), various services provided by Authority departments, Recruitment related details, etc.

- **Multilingual:** The portal should primarily be available in Tamil & English.
- **Shall be available anytime, anywhere:** The portal shall be available 24 hours a day, 7 days a week, and accessible from anywhere in the world via the internet. While the technology shall be available round the clock, functional support might be available only during the normal working day- 9:30 to 6:30, 6 days a week
- **Shall be accessible from a variety of channels:** The portal can be accessed via a variety of established channels, including individual users (through PCs, Laptops), Citizen Civic Centers, etc. Shall exchange information & services seamlessly across various departments of Authority as well as central metadata repository as specified in RFP.
- The Web portal shall also host all the electronic forms for various services accessible to citizens from Authority. A citizen will be able to fill the form electronically (both online and offline) through internet services including Citizen Civic Centre (CCCs) outlets and submit his/her application electronically. A citizen will be able to track the status of his/her application / request at any point of time.
- System should facilitate automatic routing of the work-items/transactions to the respective Authority department officials. Such routing of work-items/transactions should be based on the following, at a minimum:
  - Automatic allocation of work-items to the employees based on FIFO mechanism
  - The role and authorization defined in the system
  - Availability and status of employees in the system (e.g. work-items shall not be routed to employees who are on leave or whose ids are temporarily or permanently deactivated)
  - Based on the defined work-flow and the designated employees
- Facility to define the workflow for each type of request / service.
- Facility to capture and to provide the workflow in the CCC/Authority offices in a comprehensive manner for all the services. Both predefined and ad hoc workflows shall be provided.
- Facility to automatically provide the status of the work item (for those work items created upon arrival of a request) through response to a request from the Citizen Civic Centers.

- Facility to manually create a work-item (by an authorized official) and assign to an individual.
- Facility to add comments / notes / documents to a work-item during processing. It should also be possible for entering profiling information or metadata needs for a particular document (in cases where applicable) as part of this facility.
- In-built business process controls to capture the validation rules defined for processing the transactions/work-items
  
- Facility to register, approve or reject documents of specified type (as per applicable Acts & Bye- Laws) by an authorized official.
- Facility to view all pending transactions, retrieve the corresponding documents, print the required pages and mark the request as pending/in process/completed as per the status of the request.
- Facility for an authorized official to view pending work-items for all individuals in his/her purview.
- Facilities for an authorized official to retrieve a work-item held by an individual (in his/her purview) and reassign it to another individual.
- Facility to automatically escalate a work-item; if it is held beyond the pre-defined period by an individual. Multiple levels of escalation must be provided. Consequently, it is also necessary to provide a facility to define the threshold time limits for each transaction or service category that will be used for the purpose of escalation. This should be a parameter that can be changed by Authority from time to time.
- Access to the records / statistics should be as per the operating span/ geography of control.
- Facility to view the archived/stored documents (within the purview of the individual) along with the notes/ comments; if any.
- After successful completion of the transaction or such other processing by Authority Office staff, make the requests and associated documents as part of the electronic repository, which can be retrieved and verified at a later date.
- Facility to return the request to citizen/individual for clarifications / corrections and keep track the payment for a given period of time; so that the applicant need not be charged for resubmission of the corrected/clarified document/request.
- Facility to process complaints filed by individuals, stake holders and businesses through the work flow functions; including ability to integrate them with the compliance management, inspection, punitive and prosecution processes.
- Facility to scan documents, convert them to specified format, allow verification / authorization and upload this as part of the electronic records, with the necessary metadata into the appropriate folder hierarchy updating any necessary indices / links consistent with the application needs.

- Integrate the email / SMS functionality into the rest of the portal system such that all the escalations, request submission, routing activities are notified to the concerned users by email and SMS.
- On submission of the form appropriate message should be generated. (Reason for rejection in case of failure and acknowledgement of form submission with unique acknowledgement number in case of successful submission)
- The acknowledgement slip should be non-editable, downloadable and printable
- The portal should have the capability to integrate with payment gateways (as per RBI Guidelines on Payment Gateways) provided/supplied by System Integrator.
- The Bidder should provide 4 or more design templates for the new Web portal for Authority from which one of the design template would be selected by Authority.

**5.1.4.13.2 Accessibility**

- Universal accessibility of the Portal through web, mobile, etc. to the entire cross-section of the target visitors including people with certain disabilities.
- Portal must be functional on as many browsers as possible without being technology or platform dependent.
- Online search result via Google or any search engine should appear first in the search results. SEO or search engine optimization is a practice to making the portal attractive to search engine.

**5.1.4.13.3 User Management**

Web portal would be accessed by Citizens. Management of users, their access rights and verifying their credentials is critical for security and effective functioning of Web Portal. Login is the process of verifying credentials of authorized users. Password management cycle further ensures that user credentials are controlled by them and updated at regular intervals. Since other external security features such as Password key, Biometrics etc. are not feasible for all users, thus password management is an integral part of computer security procedures and provides a high degree of protection for a system. User management further helps in managing user login details and other related activities performed by them after login.

S. No.	Process Detail	Responsibility
1	Citizens would access the Web Portal. First time users would have to register themselves on the portal	Citizen
2	First time citizen users would be required to create two passwords-	Citizen & SI/System Admin

S. No.	Process Detail	Responsibility
	1- Profile login password 2- Transaction Password	
3	All Employees of Authority would be given user id and password by System Administrator to login to the intranet portal for accessing corresponding departmental modules/applications.	SI/System Admin
4	System would prompt users to change transaction password at regular intervals e.g. every 45 days.	SI/System Admin
5	Users would also be allowed to change the password as and when required.	SI/System Admin
6	Web portal would automatically terminate the login session and log out the user in following scenarios- 1- No activity is performed by user after login for a specified time e.g. 10 minutes. 2- User accidentally closes the portal window during login session.	SI/System Admin
7	System administrator would have all the rights to allow, deny, and provide access rights for specific information for users at his discretion.	SI/System Admin

## 5.2 Smart Data Centre -Hosted on Cloud

### 5.2.1 Cloud Service Specification

#### 5.2.1.1 Compute

#	Requirement	Description
1.	Compute instances – <input checked="" type="checkbox"/> General Purpose <input checked="" type="checkbox"/> Memory optimized <input checked="" type="checkbox"/> Compute optimized <input checked="" type="checkbox"/> Storage optimized <input checked="" type="checkbox"/> GPU instances	Cloud provider should offer the following instance types – <input type="checkbox"/> General Purpose – optimized for generic applications and provides a balance of compute, memory, and network resources. <input type="checkbox"/> Memory optimized – optimized for memory applications <input type="checkbox"/> Compute optimized – optimized for compute applications <input type="checkbox"/> Storage optimized – include very fast/large amount of local storage for NoSQL databases and Hadoop <input type="checkbox"/> GPU – intended for graphics and general purpose GPU compute applications
2.	Compute instances – Burstable performance	Cloud provider should offer instances that provide a baseline level of CPU performance with the ability to burst above the baseline.



3	Compute instances – Dedicated	Cloud provider should offer instances that run on hardware dedicated to a single customer.
4	OS Support – Linux	Cloud provider should be able to support following Linux distributions - (Red Hat, SUSE, Ubuntu, CentOS, and Debian)
5	OS Support – Windows	Cloud provider should be able to support the last two major Windows Server versions (Windows Server 2012, Windows Server 2008)
6	Resize virtual cores, memory, storage seamlessly	Customer must be able to specify and modify server configuration (CPU, memory, storage) parameters seamlessly and without outage.
7	Local disk/Instance store	Cloud service should support local storage for compute instances to be used for temporary storage of information that changes frequently.
8	Provision multiple concurrent instances	Cloud service must offer self-service provisioning of multiple instances concurrently either through a programmatic interface (API/CLI) or through a management console.
9.	Instance affinity - logical grouping of instances within a single data center	Customer should be able to logically group instances together for applications that require low network latency and/or high network throughput.
10	Instance anti-affinity - two or more instances hosted in different data centers	Customer should be able to split and host instances across different physical data centers to ensure that a single physical failure event does not take all instances offline.
11.	Auto Scaling support	Cloud service should be able to automatically increase the number of instances during demand spikes to maintain performance and decrease capacity during lulls to reduce costs.
12	Bring your own image/Instance Import	Customer should be able to import their existing image and save it as a new, privately available image that can then be used to provision instances in the future.
13.	Export Instance Image	Cloud service must support the ability to take an existing running instance or a copy of an instance and export the instance into a VMDK or VHD image format.
14.	Instance maintenance mitigation	Cloud service must be architected in such a way to avoid instance outages or downtime when the provider is performing any kind of hardware or service maintenance.
15.	Instance failure recovery	Cloud service must be architected in such a way to automatically restart instances on a healthy host if the original physical host fails.
16.	Instance restart flexibility	Cloud provider must be able to schedule events for customer's instances, such as a reboot, stop/start, or retirement. Depending on the event, customer might be able to take action to control the timing of the event.
17.	Support for Docker containers	Cloud service should support containers, including Docker and/or other containerization platforms.
18.	Highly scalable, high performance container management service	Cloud provider should offer a highly scalable, high performance container management service.

19.	Event-driven computing that runs code in response to events	Cloud service should be able to run customer code in response to events and automatically manage the compute resources.
20.	License portability and support – Microsoft	Cloud provider should offer license portability and support for Microsoft apps like SQL Server and SharePoint Server.
21.	License portability and support – Oracle	Cloud provider should offer license portability and support for Oracle apps like Oracle Database 11g.
22.	License portability and support – SAP	Cloud provider should offer license portability and support for SAP apps like HANA.
23.	License portability and support – IBM	Cloud provider should offer license portability and support for IBM apps like DB2 and Websphere.
24.	Pay-as-you-go pricing	Cloud provider should offer a simple pay-as-you-go pricing where customers can pay for compute capacity by the hour with no long-term commitments.

### 5.2.1.2 Networking

#	Requirement	Description
27.	Multiple network interface/instance	Cloud service should be able to support multiple (primary and additional) network interfaces.
28.	Multiple IP addresses/instance	Cloud service should be able to support multiple IP addresses per instance. Use cases include hosting multiple websites on a single server and network appliances (such as load balancers) that have multiple private IP addresses for each network interface.
29.	Ability to move network interfaces and IPs between instances	Cloud service should support the ability to create a network interface, attach it to an instance, detach it from an instance, and attach it to another instance.
30.	Enhanced networking support	Cloud service should support capabilities such as single root I/O virtualization for higher performance (packets per second), lower latency, and lower jitter.
31.	Network traffic logging - Log traffic flows at network interfaces	Cloud service should support capturing information about the IP traffic going to and from network interfaces.
32.	Auto-assigned public IP addresses	Cloud service should be able to automatically assign a public IP to the instances.
33.	IP Protocol support	Cloud service should be able to support multiple IP protocols, including TCP, UDP, and ICMP protocols.
34.	Use any network CIDR, including RFC 1918	Cloud service should be able to support IP address ranges specified in RFC 1918 as well as publicly routable CIDR blocks.
35.	Static public IP addresses	Cloud provider must support IP addresses associated with a customer account, not a particular instance. The IP address should remain associated with the account until released explicitly.
36.	Auto-created default virtual private network	Cloud service should be able to create a default private network and subnet with instances launching into a default subnet

		receiving a public IP address and a private IP address.
37.	Subnets within private network	Customer should be able to create one or more subnets within private network with a single Classless Inter-Domain Routing (CIDR) block.
38.	Subnet level filtering (Network ACLs)	Cloud service should support subnet level filtering – Network ACLs that act as a firewall for associated subnets, controlling both inbound and outbound traffic at the subnet level.
39.	Ingress filtering	Cloud service should support adding or removing rules applicable to inbound traffic (ingress) to instances.
40.	Egress filtering	Cloud service should support adding or removing rules applicable to outbound traffic (egress) originating from instances.
41.	Disable source/destination checks on interfaces	Cloud service should support the ability to disable source/destination check on network interfaces. By default, compute instances perform source/destination checks.
42.	Configure proxy server (NAT instance) at network level	Cloud service should support NAT instances that can route traffic from internal-only instances to the Internet.
43.	Site-to-site managed VPN service	Cloud service should support a hardware based VPN connection between the cloud provider and customer data center.
44.	Virtual Network Peering	Cloud service should support connecting two virtual networks to route traffic between them using private IP addresses.
45.	Multiple VPN Connections per Virtual Network	Cloud service should support creating multiple VPN connections per virtual network
46.	BGP for high availability and reliable failover	Cloud provider should support Border Gateway Protocol. BGP performs a robust liveness check on the IPsec tunnel and simplifies the failover procedure that is invoked when one VPN tunnel goes down.
47.	Private connection to customer data centers	Cloud provider should support direct leased-line connections between cloud provider and a customer datacenter, office, or colocation environment, which in many cases can reduce network costs, increase bandwidth throughput, and provide a more consistent network experience than Internet-based connections.
48.	DNS based global load balancing	Cloud service should support Load balancing of instances across multiple host servers.
49.	Load balancing supports multiple routing methods	Cloud service should support multiple routing mechanism including round-robin, failover, sticky session etc.
50.	Front-end Load Balancer	Cloud service should support a front-end load balancer that takes requests from clients over the Internet and distributes them across the instances that are registered with the load balancer.
51.	Back-end Load Balancer	Cloud service should support an internal load balancer that routes traffic to instances within private subnets.
52.	Health checks - monitor the health and	Cloud service should support health checks to monitor the health and performance of resources.

	performance of application	
53.	Integration with Load Balancer	Cloud service should support integration with load balancer.
54.	Low Latency	The CSP should be able to provide a 10GB network connectivity between the servers if required.
55.	Support for storage allocated as local disk to a single VM	Cloud provider should offer persistent block level storage volumes for use with compute instances.
56.	Storage volumes > 1 TB	Cloud provider should offer block storage volumes greater than 1 TB in size.
57.	SSD backed storage media	Cloud service should support solid state drive (SSD) backed storage media that offer single digit millisecond latencies.
58.	Provisioned I/O support	Cloud service should support the needs of I/O-intensive workloads, particularly database workloads that are sensitive to storage performance and consistency in random access I/O throughput.
59.	Encryption using provider managed keys	Cloud service should support encryption of data on volumes, disk I/O, and snapshots using industry standard AES-256 cryptographic algorithm.
60.	Encryption using customer managed keys	Cloud service should support encryption using customer managed keys.
61.	Durable snapshots	Cloud service should support point-in-time snapshots. These snapshots should be incremental in nature.
62.	Ability to easily share snapshots globally	Cloud Service should support sharing of snapshots across regions making it easier to leverage multiple regions for geographical expansion, data center migration, and disaster recovery.
63.	Consistent Input Output per second (IOPS)	Cloud service should support a baseline IOPS/GB and maintain it consistently at scale
64.	Annual Failure Rates <1%	Cloud service should
65.	Scalable object storage service	Cloud provider should offer secure, durable, highly-scalable object storage for storing and retrieving any amount of data from the web.
66.	Low cost archival storage with policy support	Cloud provider should support an extremely low-cost storage service that provides durable storage with security features for data archiving and backup.
67.	Support for Server-side Encryption	Cloud service should support encryption for data at rest using 256-bit Advanced Encryption Standard (AES-256) encryption to encrypt your data.
68.	Support for Server Side Encryption with Customer-Provided Keys	Cloud service should support encryption using customer-provided keys. These keys should be used to manage both the encryption, as data is written to disks, and decryption, when data is accessed.

69.	Support for Server Side Encryption with a Key Management Service	Cloud service should support encryption using a Key Management Service that creates encryption keys, defines the policies that control how keys can be used, and audits key usage to prove they are being used correctly.
70.	Object lifecycle management	Cloud Service should support managing an object's lifecycle by using a lifecycle configuration, which defines how objects are managed during their lifetime, from creation/initial storage to deletion.
71.	Data Locality	Cloud provider should provide a strong regional isolation, so that objects stored in a region never leave the region unless customer explicitly transfers them to another region.
72.	Object change notification	Cloud service should be able to send notifications when certain events happen at the object level (addition/deletion).
73.	High-scale static web site hosting	Cloud service should be able to host a website that uses client-side technologies (such as HTML, CSS, and JavaScript) and does not require server-side technologies (such as PHP and ASP.NET).
74.	Object Versioning	Cloud Service should support versioning, where multiple versions of an object can be kept in one bucket. Versioning protects against unintended overwrites and deletions.
75.	Flexible access-control mechanisms	Cloud service should support flexible access-control policies to manage permissions for objects.
76.	Audit logs	Cloud service should be able to provide audit logs on storage buckets including details about a single access request, such as the requester, bucket name, request time, request action, response status, and error code.
77.	Multi-factor delete	Cloud service should support multi-factor delete as an additional security option for storage buckets
78.	Lower Durability offering	Cloud service should support a lower cost option for noncritical, reproducible data at lower levels of redundancy.
79.	Parallel, multipart upload	Cloud service should allow uploading a single object as a set of parts where each part is a contiguous portion of the object's data and these object parts can be uploaded independently and in any order.
80.	CDN option for users	Cloud provider should offer a service to speed up distribution of static and dynamic web content.
81.	Strong Consistency	Cloud service should support read-after-write consistency for PUT operations for new objects.
82.	Storage gateway appliance for automated enterprise backups	Cloud provider should offer a storage gateway appliance for seamlessly storing on-premises data to the cloud.

### 5.2.2 Typical Data Center Infrastructure – guidelines

- Any additional physical space required as per proposed design of SI, wherein some local storage is being envisaged for better data availability requirements, then minimal space

(to the tune 1-2 racks space) may be provisioned by authority post evaluating the design and need for the same. The bidder has to take care of the interior, electrical works DC/DR racks, IT Compute, Storage, Network, Security and Non IT components including power and cooling as a part of cloud environment.

- Indicative list of ICT equipment to be provisioned and maintained by the SI at the DC-DR cloud are given below.
- The DC-DR cloud shall necessarily be one of empaneled cloud services providers of MeitY Gol and shall DC-DR cloud environment where the CCC solution is being planned to comply with ISO27001 standards.
- The Business Continuity Planning (BCP) shall be configurable as per requirements of BCP requirements prescribed in this RFP. The mass broadcasting / messaging incase of likely disaster shall be done in accordance to guidance of police department / GoTN guidelines.

Technical Specifications for Smart Data Center and Disaster Recovery Infrastructure Components

**5.2.2.1 Data Center TOR (Top of the Rack ) Switch**

#	Parameter	Minimum Specifications
1.	Ports	<ul style="list-style-type: none"> <li>• 24 or 48 (as per density required) 1G/ 10G Ethernet ports (as per internal connection requirements) and extra 4 numbers of Uplink ports (40GE)</li> <li>• All ports can auto-negotiate between all allowable speeds, half-duplex or full duplex and flow control for half-duplex ports.</li> </ul>
2.	Switch type	Layer 3
3.	MAC	Support 32K MAC address.
4.	Backplane	Capable of providing wire-speed switching
5.	Throughput	500 Mpps or better
6.	Port Features	Must support Port Mirroring, Port Trunking and 802.3ad LACP Link Aggregation port trunks
7.	Flow Control	Support IEEE 802.3x flow control for full-duplex mode ports.
8.	Protocols	<ul style="list-style-type: none"> <li>• IPV4, IPV6</li> <li>• Support 802.1D, 802.1S, 802.1w, Rate limiting</li> <li>• Support 802.1X Security standards</li> <li>• Support 802.1Q VLAN encapsulation, IGMP v1, v2 and v3 snooping</li> <li>• Should have routing protocols like OSPFv3, BGP v4 &amp; v6 &amp; IS-IS.</li> <li>• Should support DCB (802.1Qbb &amp; 802.1qaz), FCoE Transit and iSCSI protocols.</li> </ul>

#	Parameter	Minimum Specifications
		<ul style="list-style-type: none"> <li>• 802.1p Priority Queues, port mirroring, DiffServ</li> <li>• DHCP support</li> <li>• Support up to 1024 VLANs</li> <li>• Support IGMP Snooping and IGMP Querying</li> <li>• Support Multicasting</li> <li>• Should support Loop protection and Loop detection</li> </ul>
9.	Access Control	<ul style="list-style-type: none"> <li>• Support port security</li> <li>• Support 802.1x (Port based network access control).</li> <li>• Support for MAC filtering.</li> <li>• Should support TACACS+ and RADIUS authentication</li> </ul>
10.	VLAN	<ul style="list-style-type: none"> <li>• Support 802.1Q Tagged VLAN and port based VLANs and Private VLAN</li> <li>• The switch must support dynamic VLAN Registration or equivalent</li> <li>• Dynamic Trunking protocol or equivalent</li> </ul>
11.	Protocol and Traffic	<ul style="list-style-type: none"> <li>• Network Time Protocol or equivalent Simple Network Time Protocol support</li> <li>• Switch should support traffic segmentation</li> <li>• Traffic classification should be based on user-definable application types: TOS, DSCP, Port based, TCP/UDP port number</li> </ul>
12.	Management	<ul style="list-style-type: none"> <li>• Switch needs to have a console port for management via a console terminal or PC</li> <li>• Must have support SNMP v1,v2 and v3</li> <li>• Should support 4 groups of RMON</li> <li>• 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</li> </ul>
13.	Resiliency	<ul style="list-style-type: none"> <li>• Dual load sharing AC and DC power supplies</li> <li>• Redundant variable-speed fans</li> </ul>

#### 5.2.2.2 Servers

#	Parameter	Minimum Specifications
1.	Processor	<p>Latest series/ generation of 64 bit x86 processor(s) with Ten or higher Cores</p> <p>Processor speed should be minimum 2.4 GHz</p> <p>Minimum 2 processors per each physical server</p>
2.	RAM	Minimum 64 GB Memory per physical server

#	Parameter	Minimum Specifications
3.	Internal Storage	2 x 300 GB SAS (10k rpm) hot swap disk with extensible bays
4.	Network interface	2 X 20GbE LAN ports for providing Ethernet connectivity Optional: 1 X Dual-port 16Gbps FC HBA for providing FC connectivity
5.	Power supply	Dual Redundant Power Supply
6.	RAID support	As per requirement/solution
7.	Operating System	Licensed version of 64 bit latest version of Linux/ Unix/Microsoft® Windows based Operating system)
8.	Form Factor	Rack mountable/ Blade
9.	Virtualization	Shall support Industry standard virtualization hypervisor like Hyper-V, VMWARE and Citrix.

#### 5.2.2.3 Blade Chassis Specifications

The blade chassis shall have the following minimum technical specifications:

#	Specifications
1)	Minimum 6U size, rack-mountable, capable of accommodating minimum 8 or higher hot pluggable blades
2)	Dual network connectivity of 10 G speed for each blade server for redundancy shall be provided
3)	Backplane shall be completely passive device. If it is active, dual backplane shall be provided for redundancy.
4)	Have the capability for installing industry standard flavors of Microsoft Windows, and Enterprise Red Hat Linux Oss as well as virtualization solution such as VMware.
5)	DVD ROM shall be available in chassis, can be internal or external, which can be shared by all the blades allowing remote installation of software
6)	Minimum 1 USB Ports at Blade Server or Chassis level
7)	Two hot-plug/hot-swap, redundant 10 Gbps Ethernet or FCoE module with minimum 16 ports (cumulative), having Layer 2/3 functionality
8)	Two hot-plugs/hot-swap redundant 16 Gbps Fiber Channel module for connectivity to the external Fiber channel Switch and ultimately to the storage device
9)	Hot plug/hot-swap redundant power supplies to be provided, along with power cables



10)	Power supplies shall have N+N. All power supplies modules shall be populated in the chassis.
11)	Required number of PDUs and power cables, to connect all blades, Chassis to Data Center power outlet.
12)	Hot pluggable/hot-swappable redundant cooling unit
13)	Provision of systems management and deployment tools to aid in blade server configuration and OS deployment
14)	Blade enclosure shall have provision to connect to display console/central console for local management such as troubleshooting, configuration, system status/health display.
15)	Single console for all blades in the enclosure, built-in KVM switch or Virtual KVM features over IP
16)	Dedicated management network port shall have separate path for remote management.

#### 5.2.2.4 Primary Storage

#	Parameter	Minimum Specifications
1.	Solution/ Type	<ul style="list-style-type: none"> <li>IP Based/iSCSI/FC/NFS/CIFS</li> </ul>
2.	Storage	<ul style="list-style-type: none"> <li>Storage Capacity should be minimum XX TB (usable, after configuring in offered RAID configuration)</li> <li>RAID solution offered must protect against double disc failure.</li> <li>Disks should be preferably minimum of 4 TB capacity</li> <li>To store all types of data (Data, Voice, Images, Video, etc)</li> <li>Storage system capable of scaling vertically and horizontally</li> </ul>
3.	Hardware Platform	<ul style="list-style-type: none"> <li>Rack mounted form-factor</li> <li>Modular design to support controllers and disk drives expansion</li> </ul>
4.	Controllers	<ul style="list-style-type: none"> <li>At least 2 Controllers in active/active mode</li> <li>The controllers / Storage nodes should be upgradable seamlessly, without any disruptions / downtime to production workflow for performance, capacity enhancement and software / firmware upgrades.</li> </ul>
5.	RAID support	<ul style="list-style-type: none"> <li>RAID 0, 1, 1+0, 5+0 and 6</li> </ul>
6.	Cache	<ul style="list-style-type: none"> <li>Minimum 128 GB of useable cache across all controllers. If cache is provided in additional hardware for unified storage solution, then cache must be over and above 128 GB.</li> </ul>

#	Parameter	Minimum Specifications
7.	Redundancy and High Availability	<ul style="list-style-type: none"> <li>• 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</li> </ul>
8.	Management software	<ul style="list-style-type: none"> <li>• 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.</li> <li>• Licenses for the storage management software should include disc capacity/count of the complete solution and any additional disks to be plugged in in the future, upto max capacity of the existing controller/units.</li> <li>• A single command console for entire storage system.</li> <li>• Should also include storage performance monitoring and management software</li> <li>• Should provide the functionality of proactive monitoring of Disk drive and Storage system for all possible disk failures</li> <li>• Should be able to take "snapshots" of the stored data to another logical drive for backup purposes</li> </ul>
9.	Data Protection	<p>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</p>

5.2.2.5 Server/Networking Rack Specifications

#	Parameter	Minimum Specifications
1.	Type	<ul style="list-style-type: none"> <li>• 19" 42U racks mounted on the floor</li> <li>• Floor Standing Server Rack - 42U with Heavy Duty Extruded Aluminium Frame for rigidity. Top cover with FHU provision. Top &amp; 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.</li> <li>• All racks should have mounting hardware 2 Packs, Blanking Panel.</li> <li>• Stationery Shelf (2 sets per Rack)</li> <li>• All racks must be lockable on all sides with unique key for each rack</li> <li>• Racks should have Rear Cable Management channels, Roof and base cable access</li> </ul>
2.	Wire managers	Two vertical and four horizontal
3.	Power Distribution Units	<ul style="list-style-type: none"> <li>• 2 per rack</li> <li>• Power Distribution Unit - Vertically Mounted, 32AMPs with 25 Power Outputs. (20 Power outs of IEC 320 C13 Sockets &amp; 5 Power outs of 5/15 Amp Sockets), Electronically controlled circuits for Surge &amp; Spike protection, LED readout for the total current being drawn from the channel, 32AMPS MCB, 5 KV AC isolated input to Ground &amp; Output to Ground</li> </ul>
4.	Doors	<ul style="list-style-type: none"> <li>• The racks must have steel (solid / grill / mesh) front / rear doors and side panels. Racks should NOT have glass doors / panels.</li> <li>• Front and Back doors should be perforated with at least 63% or higher perforations.</li> <li>• Both the front and rear doors should be designed with quick release hinges allowing for quick and easy detachment without the use of tools.</li> </ul>
5.	Fans and Fan Tray	<ul style="list-style-type: none"> <li>• Fan 90CFM 230V AC, 4" dia (4 Nos. per Rack)</li> <li>• 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 &amp; temperature sensor</li> </ul>

#	Parameter	Minimum Specifications
6.	Metal	Aluminium extruded profile
7.	Side Panel	Detachable side panels (set of 2 per Rack)

#### 5.2.2.6 Core Router

#	Item	Minimum Specifications
1.	Multi-Services	Should deliver multiple IP services over a flexible combination of interfaces
2.	Ports	As per overall network architecture proposed by the bidder, the router should be populated with required number of LAN/WAN ports/modules, with cable for connectivity to other network elements.
3.	Speed	As per requirement, to cater to entire bandwidth requirement of the project.
4.	Interface modules	Must support upto 10G interfaces. Must have capability to interface with variety interfaces.
5.	Protocol Support	<ul style="list-style-type: none"> <li>• Must have support for TCP/IP, PPP, Frame relay or any equivalent protocols</li> <li>• Must support VPN</li> <li>• Must have support for integration of data and voice services</li> <li>• Routing protocols of RIP, OSPF, and BGP.</li> <li>• Support IPV4 &amp; IPV6</li> <li>• Should support Multicast-only fast reroute (MoFRR) to minimize packet loss in PIM and multipoint LDP domains with dual paths available.</li> </ul>
6.	Manageability	Must be SNMP manageable
7.	Scalable	<ul style="list-style-type: none"> <li>• The router should be scalable. For each slot multiple modules should be available.</li> <li>• The chassis offered must have free slots to meet the scalability requirement of expansion of the project in the future.</li> <li>• Should support minimum 4 million ipv4 and 4 million ipv6 routes</li> <li>• should support a tleast 8000 VRF/ MPLS VPN</li> </ul>
8.	Traffic control	Traffic Control and Filtering features for flexible user control policies
9.	Bandwidth	Bandwidth on demand for cost effective connection performance enhancement
10.	Remote Access	Remote access features
11.	Redundancy	<ul style="list-style-type: none"> <li>• Redundancy in terms of Power supply(s). Power supply should be able to support fully loaded chassis</li> </ul>

#	Item	Minimum Specifications
		<ul style="list-style-type: none"> <li>All interface modules, power supplies should be hot-swappable</li> </ul>
12.	Security features	<ul style="list-style-type: none"> <li>MD5 encryption for routing protocol</li> <li>NAT</li> <li>RADIUS Authentication</li> <li>Management Access policy</li> <li>IPSec / Encryption</li> <li>L2TP</li> </ul>
13.	QOS Features	<ul style="list-style-type: none"> <li>RSVP</li> <li>Priority Queuing</li> <li>Policy based routing</li> <li>Traffic shaping</li> <li>Time-based QoS Policy</li> <li>Bandwidth Reservation / Committed Information Rate</li> </ul>

**5.2.2.7 Internet Router**

#	Item	Minimum Specifications
1.	Multi-Services	Should deliver multiple IP services over a flexible combination of interfaces
2.	Ports	As per overall network architecture proposed by the bidder, the router should be populated with required number of LAN/WAN ports/modules, with cable for connectivity to other network elements.
3.	Interface modules	Must support up to 10G interfaces as per the design. Must have capability to connect with variety of interfaces.
4.	Protocol Support	<ul style="list-style-type: none"> <li>Must have support for TCP/IP, PPP, Frame relay or any equivalent protocols</li> <li>Must support VPN</li> <li>Must have support for integration of data and voice services</li> <li>Routing protocols of RIP, OSPF, and BGP.</li> <li>Support IPV4, IPV6</li> <li>Support load balancing</li> </ul>
5.	Manageability	Must be SNMP manageable
6.	Traffic control	<ul style="list-style-type: none"> <li>Traffic Control and Filtering features for flexible user control policies</li> <li>Should support minimum 4 million IPv4 and 4 million IPv6 routes</li> </ul>

#	Item	Minimum Specifications
7.	Bandwidth	Bandwidth on demand for cost effective connection performance enhancement
8.	Remote Access	Remote access features
9.	Redundancy	<ul style="list-style-type: none"> <li>• Redundancy in terms of Power supply(s). Power supply should be able to support fully loaded chassis</li> <li>• All interface modules, power supplies should be hot-swappable</li> </ul>
10.	Security features	<ul style="list-style-type: none"> <li>• MD5 encryption for routing protocol</li> <li>• NAT</li> <li>• RADIUS/AAA Authentication</li> <li>• Management Access policy</li> <li>• IPSec / Encryption</li> <li>• L2TP</li> </ul>
11.	QOS Features	<ul style="list-style-type: none"> <li>• RSVP</li> <li>• Priority Queuing</li> <li>• Policy based routing</li> <li>• Traffic shaping</li> <li>• Time-based QoS Policy</li> <li>• Bandwidth Reservation / Committed Information Rate</li> </ul>

#### 5.2.2.8 Firewall

#	Item	Minimum Specifications
1	Physical attributes	<ul style="list-style-type: none"> <li>• Should be mountable on 19" Rack</li> <li>• Modular Chassis</li> <li>• Internal redundant power supply</li> </ul>
2	Interfaces	<ul style="list-style-type: none"> <li>• Minimum 8 x GE</li> <li>• Console Port 1 number</li> </ul>
3	Performance and Availability	<ul style="list-style-type: none"> <li>• Encrypted throughput: minimum 1000 Mbps for internet and 4000 Mbps for intranet firewall</li> <li>• Concurrent connections: up to 100,000</li> <li>• Simultaneous VPN tunnels: 2000</li> </ul>
4	Routing Protocols	<ul style="list-style-type: none"> <li>• Static Routes</li> <li>• RIPv1, RIPv2</li> <li>• OSPF</li> </ul>
5	Protocols	<ul style="list-style-type: none"> <li>• TCP/IP, PPTP</li> <li>• RTP, L2TP</li> <li>• IPSec, GRE, DES/3DES/AES</li> </ul>

#	Item	Minimum Specifications
		<ul style="list-style-type: none"> <li>• PPPoE, EAP-TLS, RTP</li> <li>• FTP, HTTP, HTTPS</li> <li>• SNMP, SMTP</li> <li>• DHCP, DNS</li> <li>• Support for Ipv6</li> </ul>
6	Other support	<ul style="list-style-type: none"> <li>• 802.1Q, NAT, PAT, IP Multicast support, Remote Access VPN, Time based Access control lists, URL Filtering, support VLAN, Radius/ TACACS</li> </ul>
7	QoS	<ul style="list-style-type: none"> <li>• QoS features like traffic prioritization, differentiated services, committed access rate. Should support for QoS features for defining the QoS policies.</li> </ul>
8	Management	<ul style="list-style-type: none"> <li>• Console, Telnet, SSHv2, Browser based configuration</li> <li>• SNMPv1, SNMPv2</li> </ul>

#### 5.2.2.9 Intrusion Prevention System

#	Item	Minimum Specifications
1.	Performance	Should have an aggregate throughput of no less than 200Mbps Total Simultaneous Sessions – 10,000
2.	Features	IPS should have Dual Power Supply IPS system should be transparent to network, not default gateway to Network IPS system should have Separate interface for secure management IPS system should be able to protect Multi Segment in the network, should be able to protect 4 segments.
3.	Real Time Protection	<ul style="list-style-type: none"> <li>• Web Protection</li> <li>• Mail Server Protection</li> <li>• Cross Site Scripting</li> <li>• SNMP Vulnerability</li> <li>• Worms and Viruses</li> <li>• Brute Force Protection</li> <li>• SQL Injection</li> <li>• Backdoor and Trojans</li> </ul>
4.	Stateful Operation	<ul style="list-style-type: none"> <li>• TCP Reassembly</li> <li>• IP Defragmentation</li> <li>• Bi-directional Inspection</li> </ul>

#	Item	Minimum Specifications
		<ul style="list-style-type: none"> <li>Forensic Data Collection</li> <li>Access Lists</li> </ul>
5.	Signature Detection	Should have provision for Real Time Updates of Signatures, IPS Should support Automatic signature synchronization from database server on web Device should have capability to define User Defined Signatures
6.	Block attacks in real time	<ul style="list-style-type: none"> <li>Drop Attack Packets</li> <li>Reset Connections</li> <li>Packet Logging</li> <li>Action per Attack</li> </ul>
7.	Alerts	<ul style="list-style-type: none"> <li>Alerting SNMP</li> <li>Log File</li> <li>Syslog</li> <li>E-mail</li> </ul>
8.	Management	<ul style="list-style-type: none"> <li>SNMP V1, 2C, 3</li> <li>HTTP, HTTPS</li> <li>SSH/ Telnet, Console</li> </ul>
9.	Security Maintenance	<ul style="list-style-type: none"> <li>IPS Should support 24/7 Security Update Service</li> <li>IPS Should support Real Time signature update</li> <li>IPS Should support Provision to add static own attack signatures</li> <li>System should show real-time and History reports of Bandwidth usage per policy</li> <li>IPS should have provision for external bypass Switch</li> </ul>

#### 5.2.2.10 Data Center Switch (1G)

(To be used for Data center LAN Switch)

#	Parameter	Minimum Specifications
1	Ports	<ul style="list-style-type: none"> <li>24 or 48 (as per requirements) 10/100/1000 Base-TX Ethernet ports and extra 2 nos of Base-SX/LX ports</li> <li>All ports can auto-negotiate between 10Mbps/ 100Mbps/ 1000Mbps, half-duplex or full duplex and flow control for half-duplex ports.</li> </ul>
2	Switch type	Layer 3
3	MAC	Support 8K MAC address.



#	Parameter	Minimum Specifications
4	Backplane	56 Gbps or more Switching fabric capacity (as per network configuration to meet performance requirements)
5	Forwarding rate	Packet Forwarding Rate should be 70.0 Mpps or better
6	Port Features	Must support Port Mirroring, Port Trunking and 802.3ad LACP Link Aggregation port trunks
7	Flow Control	Support IEEE 802.3x flow control for full-duplex mode ports.
8	Protocols	<ul style="list-style-type: none"> <li>• Support 802.1D, 802.1S, 802.1w, Rate limiting</li> <li>• Support 802.1Q VLAN encapsulation, IGMP v1, v2 and v3 snooping</li> <li>• 802.1p Priority Queues, port mirroring, DiffServ</li> <li>• Support based on 802.1p priority bits with at least 8 queues</li> <li>• DHCP support &amp; DHCP snooping/relay/optional 82/ server support</li> <li>• Shaped Round Robin (SRR) or WRR scheduling support.</li> <li>• Support for Strict priority queuing &amp; Sflow</li> <li>• Support for IPV6 ready features with dual stack</li> <li>• Support upto 255 VLANs and upto 4K VLAN IDs</li> </ul>
9	Access Control	<ul style="list-style-type: none"> <li>• Support port security</li> <li>• Support 802.1x (Port based network access control).</li> <li>• Support for MAC filtering.</li> <li>• Should support TACACS+ and RADIUS authentication</li> </ul>
10	VLAN	<ul style="list-style-type: none"> <li>• Support 802.1Q Tagged VLAN and port based VLANs and Private VLAN</li> <li>• The switch must support dynamic VLAN Registration or equivalent</li> <li>• Dynamic Trunking protocol or equivalent</li> </ul>
11	Protocol and Traffic	<ul style="list-style-type: none"> <li>• Network Time Protocol or equivalent Simple Network Time Protocol support</li> <li>• Switch should support traffic segmentation</li> <li>• Traffic classification should be based on user-definable application types: TOS, DSCP, Port based, TCP/UDP port number</li> </ul>
12	Management	<ul style="list-style-type: none"> <li>• Switch needs to have RS-232 console port for management via a console terminal or PC</li> <li>• Must have support SNMP v1,v2 and v3</li> <li>• Should support 4 groups of RMON</li> <li>• Should have accessibility using Telnet, SSH, Console</li> </ul>

#	Parameter	Minimum Specifications
		access, easier software upgrade through network using TFTP etc. Configuration management through CLI, GUI based software utility and using web interface

#### 5.2.2.11 Server Load balancer and Web Application Firewall

- Server Load Balancing Mechanism
  - Cyclic, Hash, Least numbers of users
  - Weighted Cyclic, Least Amount of Traffic
  - NT Algorithm / Private Algorithm / Customizable Algorithm / Response Time
- Redundancy Features
  - Supports Active-Active and Active-Standby Redundancy
  - Segmentation / Virtualization support along with resource allocation per segment, dedicated access control for each segment
- Routing Features
  - Routing protocols RIPv1/RIPv2/OSPF
  - Static Routing policy support
- Server Load Balancing Features
  - Server and Client process coexist
  - UDP Stateless
  - Service Failover
  - Backup/Overflow
  - Direct Server Return
  - Client NAT
  - Port Multiplexing-Virtual Ports to Real Ports Mapping
  - DNS Load Balancing
- Load Balancing Applications
  - Application/ Web Server, MMS, Streaming Media
  - DNS, FTP- ACTIVE & PASSIVE, REXEC, RSH,
  - LDAP, RADIUS
- Content Intelligent SLB
- HTTP Header Super Farm
- URL-Based SLB
- Browser Type Farm
  - Support for Global Server Load Balancing
  - Global Server Load Balancing Algorithms
  - HTTP Redirection,
  - HTTP
  - DNS Redirection/ RTSP Redirection
  - DNS Fallback Redirection, HTTP Layer 7 Redirection
- SLB should support below Management options
  - Secure Web Based Management
  - SSH

- TELNET
- SNMP v1, 2, 3 Based GUI
- Command Line

Sr. No.	Features
<b>1</b>	<b>Platform</b>
1.0	Solution can be proposed with single / multiple appliances
1.1	Must be an appliance with hardened OS
1.2	Platform should be a full proxy architecture and must perform reverse proxy for inside applications
1.3	Should have administration partitioning and segmentation / virtualization, whereby the physical device can span across multiple network segments without any inter device routing. The segmentation / virtualization feature should support the use of the same internal IP across the multiple network segments.
1.4	Should have a dedicated out-of-band Ethernet management port
1.5	Should have full support IPv6. It should support all IPv6 scenarios: a. IPv4 on the inside and IPv6 on the outside b. IPv6 on the inside and IPv4 on the outside c. IPv6 on the inside and outside
1.6	Should support VLAN, LACP & Trunking
1.7	Should have a chassis height of 1U (1 Rack Unit)
1.8	Application should support throughput of 120 Gbps for Server Load balancing
1.9	The appliance must provide appliances with minimum 24 X 10 Gbps Short Range Fiber Ports and 2 X 40 Gbps Interfaces
1.10	The solution must support to Server Load Balancing along with WAF together from same appliance
1.11	Should have a SSD with minimal capacity of 300 GB
1.12	Should have a SSD with minimal capacity of 300 GB
1.13	OS should be default deny and should be certified by ICASA
1.14	Should have a dedicated hardware for SSL Acceleration and Dedicated Hardware for compression.
1.15	Should have dual power supply

Sr. No.	Features
<b>2</b>	<b>Performance</b>
2.1	Platform should have "L7" throughput of minimum 80 Gbps
2.2	Should have capability to support up to 100 Million Concurrent Connections
2.4	Should have 80,000 TPS, where TPS = Only one HTTP transaction over each new SSL handshakes per second, without session reuse and using a 2048 bit key SSL Certificate
2.5	Should have SSL Throughput of minimum 40 Gbps
2.6	Should have compression throughput of minimum 40 Gbps
2.8	Should support configurable TCP Optimization features for client-side and server-side connection
<b>3</b>	<b>Server Load Balancing</b>
3.1	Should have application delivery features such as layer 7 load balancing, layer 7 content switch, caching, hardware based SSL offload and hardware based server side compression
3.2	Should have capability to monitor the applications using intelligent application level monitors which can be system defined, internal or external executable scripts
3.3	Should be able to tune monitoring frequency and time automatically when server is available for long time, this is to avoid monitoring load on server
3.4	Should have 2048 and 4096 bit key for SSL certificate support
3.5	Should have capability to support ECC, RSA and ECC+RSA (Hybrid) Certificates for SSL offload
3.6	Should provide static and dynamic load balancing algorithms such as round robin, weighted round robin, fastest, predictive and observed
3.7	Should be application aware and provide Full Proxy for protocols such as HTTP, HTTPS, FTP, SIP, DNS, Diameter, RADIUS etc.
3.8	Should support inspection of SSL traffic for reverse proxy and forward proxy deployment. Should also support ICAP interface for integration with external security systems.

Sr. No.	Features
	Should support IoT Device authentication over SSL and MQTT Message parsing and MQTT load balancing.
3.9	Should have HTTP 2.0 gateway in environment where the client to load balancer traffic is HTTP 2.0 and from load balancer to server is normal HTTP 1.1
<b>4</b>	<b>Web Application Firewall</b>
4.1	Should be an ICSA WAF 2.1 certified
4.2	WAF should have positive and negative security model
4.3	The proposed WAF should be equipped with a set of pre-built application specific security policies that provide out-of-the-box protection for common applications
4.4	The proposed WAF should have a mechanism to deploy preconfigured policy that can immediately secures the web application. These validated policies should require zero configuration time and serve as a starting point for more advanced policy creation, based on heuristic learning and specific application security needs for the application.
4.5	The proposed WAF should have a dynamic policy builder engine, which is responsible for automatic self-learning and creation of security policies. It should automatically build and manage security policies around newly discovered vulnerabilities without manual intervention.
4.6	The proposed WAF should at the minimum query the signature service on a daily basis and automatically downloads and apply new signatures, and all signatures must be visible to administrator for review.
4.7	The proposed WAF should defend against the OWASP Top 10 Vulnerabilities
4.8	WAF should have capability to automatically analyze attacks like Brute Force and avail CAPTCHA on the fly to users to identify bot / scripted attacks
4.9	WAF should have Proactive BOT defense and must have BOT signatures
4.10	WAF should have different policies for different web applications

Sr. No.	Features
4.11	Should be a scalable platform and support minimum 4 Gbps of WAF throughput capacity with all Signatures enabled and scanning HTTP Request and Response together
4.12	Should protect against various application attacks, including: <ul style="list-style-type: none"> <li>a. Layer 7 DoS and DDoS</li> <li>b. Brute force</li> <li>c. Cross-site scripting (XSS)</li> <li>d. Cross Site Request Forgery</li> <li>e. SQL injection</li> <li>f. Form Field and Parameter Tampering and HPP tampering</li> <li>g. Sensitive information leakage</li> <li>h. Session hijacking</li> <li>i. Buffer overflows</li> <li>j. Cookie manipulation/poisoning</li> <li>k. Various encoding attacks</li> <li>l. Broken access control</li> <li>m. Forceful browsing</li> <li>n. Hidden fields manipulation</li> <li>o. Request smuggling</li> <li>p. XML bombs/DoS</li> </ul>
4.13	Should have FTP & SMTP protection as part of WAF
4.14	Should have automatic detection of heavy URLs and protect against BOT attacks to those URLs
4.15	Should have HTTP based DDOS detection and should start automatic capturing traffic in batch mode for forensic purpose
4.16	Should support signature staging after update – so that newly added signature to a policy in block mode does not break the application. If needed this can be disabled.
<b>5</b>	<b>Device Administration</b>
5.1	Should provide HTTPS interface management for administering the device
5.2	Should provide SSH interface management for administering the device
5.3	Should provide troubleshooting and traffic analysis tool like tcpdump
5.4	Should support role based admin access with roles like no access, Guest, Operator, Application editor, Resource Administrator and Administrator

Sr. No.	Features
5.5	Should have a live dashboard with graphical reporting a. CPU Usage b. Memory Usage c. Connections Statistics d. Throughput Statistics e. Virtual Server Status f. Pool Status g. Node Status
5.6	Should provide historical graphical reporting for the last 30 days on appliance itself
5.7	Should have a built-in tool to take a snapshot of the unit for troubleshooting and analysis purpose
5.8	Vendor should provide a service to upload this snapshot and get feedback on the health of the unit & missing Hotfixes and best practices
<b>6</b>	<b>High Availability</b>
6.1	Should have active-active and active-backup high availability with TCP/IP connection mirroring as well as SSL ID mirroring. Hence old connection should not fail or forced for SSL renegotiation.
6.2	Should have transparent failover between 2 devices, the failover should be transparent to other networking devices
6.3	Should support network based failover for session mirroring, connection mirroring and heartbeat check
6.4	Should support config autosync, manual sync to and from active and backup unit
6.5	Should support the feature to force the active device to standby and back to active state; or force a device to offline mode
6.6	Should support MAC masquerading
6.7	Should support N+1 High Availability Clustering for future scalability with the ability to add heterogenous devices from the same OEM into the cluster
<b>7</b>	<b>Reporting Features</b>
7.1	Should have a Reporting Engine built-in
7.2	Should support High Speed Logging to a syslog server

Sr. No.	Features
7.3	Support for customized logging through scripts to log any parameter from L3 to L7, like Geolocation, IP addresses, client browser, client OS, etc..
7.4	Should support integration with SIEM tools like Arcsight and Splunk
7.5	Should have a log publisher to publish logs to multiple log destinations for the same application (or virtual server)
7.6	Should have a filtering capability before publishing to a log destination
<b>8</b>	<b>Others</b>
8.1	OEM should be listed in top 3 considering Gartner leader and challenger quadrant for past 5 years consecutively
8.2	Vendor should provide regular updates to geolocation database from their public downloads website

#### 5.2.2.12 Fire proof enclosure

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

<b>Capacity</b>	300 Litres
<b>Temperature to Withstand</b>	1000° C for at least 1 hour
<b>Internal Temperature</b>	30° C after exposure to high temperature For 1 hour
<b>Locking</b>	2 IO-lever high security cylindrical / Electronic lock

#### 5.2.2.13 KVM Module (If required)

#	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	USB or KVM over IP.



#	Item	Minimum Specifications
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

#### 5.2.2.14 Back-up Software

1. The software shall be primarily used to back up the necessary and relevant video feeds from storage that are marked or flagged by the Police. The other data that would require backing up would include the various databases that shall be created for the surveillance system. Details of data that would be created are available in the table at section 'Data Requirements'
2. Scheduled unattended backup using policy-based management for all Server and OS platforms
3. The software should support on-line backup and restore of various applications and Databases
4. The backup software should be capable of having multiple back-up sessions simultaneously
5. The backup software should support different types of backup such as Full back up, Incremental back up, Differential back up, Selective back up, Point in Time back up and Progressive Incremental back up and snapshots
6. The backup software should support different types of user interface such as GUI, Web-based interface

#### 5.2.2.15 Database Licenses

- a) Bidder needs to provide Licensed RDBMS, enterprise/full version as required for the proposed Surveillance System and following all standard industry norms for performance, data security, authentication and database shall be exportable in to XML.

#### 5.2.2.16 Enterprise Management System (EMS)

The Enterprise Management System (EMS) is an important requirement of this Project. Various key components of the EMS are:

- SLA & Contract management System
- Network Monitoring System
- Server Monitoring System
- Helpdesk System

Proposed EMS Solution shall be based on industry standard best practice framework such as ITIL etc.

#### *5.2.2.16.1 SLA & Contract management System*

The SLA & Contract Management solution should enable the Authority 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 Surveillance 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 Surveillance Project under discussion.
- The solution should support requirements of the auditors requiring technical audit of the whole system
- The solution must 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; provide pre-configured connectors and adapters, Ability to define Adapters to data source in a visual manner without coding.
- Support for Defining and Calculating service Credit and Penalty based on clauses in SLAs.

#### *5.2.2.16.2 Reporting*

- Ability to generate reports on penalty and credit due, to check on non-compliance of SLAs for the surveillance project
- Monetary penalties to be levied for non-compliance of SLA, thus the system must provide Service Level Performance Report over time, contract, service and more.
- 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 surveillance project
- The solution must support security for drill-down capabilities in dashboard reports ensuring visibility for only relevant personnel of the surveillance project
- Support real-time reports 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.

#### *5.2.2.16.3 Network Management System*

Solution should provide Fault, Configuration & Performance management of the entire datacentre infrastructure and should monitor IP\SNMP enabled devices such as Routers, Switches, Cameras, Online UPS, etc. Proposed Network Management shall integrate with

SLA & Contract Management system in order to supply KPI metrics like availability, utilisation in order to measure central SLA's and calculate penalties. Following are key functionalities that are required, which will help measuring SLA's as well as assist administrators to monitor network faults & performance degradations in order to reduce downtimes, increase availability and take proactive actions to remediate & restore network services.

- The proposed solution must automatically discover manageable elements connected to the infrastructure and map the connectivity between them. Solution should provide centralized monitoring console displaying network topology map from central location to Zonal / Police Station Level.
- Proposed solution should provide customizable reporting interface to create custom reports for collected data.
- The system must use advanced root-cause analysis techniques and policy-based condition correlation technology for comprehensive analysis of infrastructure faults.
- The system should be able to clearly identify configuration changes as root cause of network problems and administrators should receive an alert in case of any change made on routers spread across surveillance project.
- Network Performance management system should provide predictive performance monitoring and should be able to auto-calculate resource utilisation baselines for the entire managed systems and networks and allow user to set corresponding upper and lower threshold limits based on baseline data instead of setting up manual thresholds for monitored devices.
- The system must support the ability to create reports that allow the surveillance administrators to search all IP traffic over a specified historical period, for a variety of conditions for critical router interfaces.
- The proposed system must be capable of providing the following detailed analysis across surveillance domain:
  - Top utilised links (inbound and outbound) based on utilisation of link
  - Top protocols by volume based on utilisation of link
  - Top host by volume based on utilisation of link

#### ***5.2.2.16.4 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.

#### *5.2.2.16.5 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.

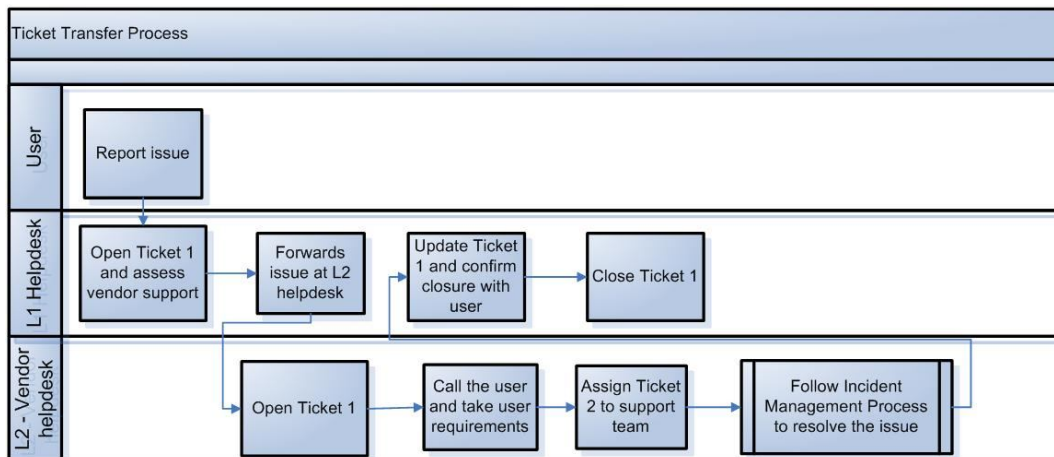
#### *5.2.2.16.6 Helpdesk Management*

It is envisaged that the centralized helpdesk, functioning as proposed below, would be managed by the Systems Integrator and shall serve following objectives:

- Act as the Point of Contact for the users of Surveillance System
- Own an Incident throughout its Lifecycle

- Communicate effectively with Police / Home Dept. Officers and IT support teams.
- Maintain high user satisfaction levels
- Maintain the SLA statistics & submit quarterly report to Police / Home Department

A general process flow for the helpdesk management is depicted in the flow-chart given as follows. Systems Integrator shall prepare a detailed Helpdesk Policy in consultation with the Chennai City Authority & its Consultant prior to the Go Live date.



System Integrator shall deploy a State-of-Art Enterprise Management System to handle the complexity of Operations & SLA Management defined in the DPR

**5.2.2.17 Link Load Balancer and DDoS**

S.No	Technical Specifications
	<b>General Requirements</b>
1	The Anti-DDoS solution should be a dedicated appliance based solution for DDoS Detection and Mitigation.
2	The solution must support stateful and statless based protection.
3	Application should support throughput of 120 Gbps for Link Load balancing
4	The appliance must provide appliances with minimum 24 X 10 Gbps Short Range Fiber Ports and 2 X 40 Gbps Interfaces
5	The appliance should have out of band management port of 1 Gigabit Ethernet Interface.
6	The solution must support to Link Load Balancing along with DDoS mitigation together from same appliance

S.No	Technical Specifications
8	The Solution must support the ability to enhance overall protection by integrating local protection with automaatated cloud-based DDoS services ans and when required.
9	The system should support the capability to perform SSL Version 3.0 /TLS (Version 1.2 & above) inspection on different module/ hardware it should not impact the core performance of DDOS device.
10	The appliances must have dual power supplies for redundancy.
11	The appliance must have a capacity to maintain logs of 30 days on SSD
12	The Appliance should support 120 Million PPS DDoS mitigation anytime.
13	The solution should support a minimum of 40 Gbps (hardware assisted) SSL decryption capacity
14	Should support hardware assisted SSL offloading capability with Minimum of 80,000 Transaction per second(TPS) or SSL Handshake per second(HPS) at 2048 bit Key size.
	<b>Functional Requirement</b>
1	DDos Protection based on IP reputation feed.
2	The solution should have GeolIP Tracking
3	The solution must be able to protect following UDP, TCP, SIP, DNS, HTTP, SSL, MQTT and other network attack targets while delivering uninterrupted service for legitimate connections:
4	The solution must be able to detect sources that send excessive amounts of traffic according to configurable thresholds, and then must provide the flexibility to place those sources on the temporary blocked hosts list (rate-base blocking)
5	The solution should support auto tuning of threshold for all DDoS vectors based on system throughput, capacity and traffic load
6	The system must support the ability to blacklist a host, country, domain, URL
7	Solution should be capable of monitoring of Internet bandwidth and signaling to cloud based on defined thresholds
	<b>Layer 3 - 4 DDoS Functionality</b>
1	The solution must be able to protect following IP based - IP Fragment, Tear Drop
2	The solution must be able to protect following TCP based - SYN, SYN-ACK, ACK and PUSH-ACK Flood, RST or FIN Flood, Fragmented ACK, Redirect Traffic Attack and Invalid TCP flags
3	The solution must be able to protect following UDP based - UDP Flood, and UDP Fragmentation, Short UDP packet
4	The solution must be able to, but not limited to, protect from following kinds of flood

S.No	Technical Specifications
4.1	ARP Flood
	ICMP v4 Flood
	ICMP v6 Flood
	IGMP Flood
	IGMP Fragment Flood
	TCP RST Flood
	TCP SYN ACK Flood
	TCP SYN Oversize
	UDP Flood
5	The solution must at least, but not limited, to detect following bad headers in IPv4 packet
5.1	Bad IP TTL Value
	Bad IP Version
	Header Length > L2 Length
	IP Error checksum
	IP Length > L2 Length
	IP Option Frames
	IP Option illegal length
	Unknown Option Type
6	The solution must at least, but not limited, to detect following bad headers in IPv6 packet
6.1	IPv6 extended headers wrong order
	Bad IPv6 Hop Count
	Bad IPv6 Version
	IPv6 duplicate extension headers
	Bad IPv6 Addr
	IPv6 Extended Header Frames
	Payload Length < L2 Length
	Too Many Extension Headers
7	The solution must be able to protect following Bad Header - DNS, ICMP, IGMP IPv4, IPv6, L2, TCP and UDP
8	The solution must support rate- limit protections for UDP flood detection, fragment flood detection, private address blocking and multicast blocking
	<b>Layer 7 DDoS Functionality</b>
1	The solution must be able to protect following HTTP based - HTTP Fragmentation, L7 DoS (Slowloris, Slow HTTP POST) and Excessive GET/POST
2	The solution must be able to protect following other Application based attacks - SIP flood or SMTP based attacks or NTP amplification/reflection or XML DoS etc.



S.No	Technical Specifications
3	The solution should have DDos Protection from active botnets
4	The solution should identify web crawlers and white list crawlers like serach engine
6	The system must support the blocking of malformed DNS requests on port 53 that do not conform to RFC standards
7	The system must be able to limit the number DNS Queries per second for following type of queries
7.1	A Query
	AAAA Query
	NS Query
	MX Query
	PTR Query
	SOA Query
	SRV Query
	TXT Query
	CNAME Query
	AXFR Query
8	The system must be able to limit SIP Traffic based on following categories
8.1	SIP ACK Method
	SIP BYE Method
	SIP Cancel Method
	SIP INVITE Method
	SIP MESSAGE Method
	SIP NOTIFY Method
	SIP OPTIONS Method
	SIP PRACK Method
	SIP PUBLISH Method
	SIP REGISTER Method
9	The system must be able to detect and drop malformed HTTP packets that does not conform to RFC standards for request headers, and then facility to blacklist the source hosts
10	The system must be able to block hosts exceeding a configurable threshold for total number of HTTP operations per second, per destination server
11	The system must provide the ability to block bot-originated traffic according to system- supplied signatures

S.No	Technical Specifications
12	The system must be able to regularly activate new defense techniques from regularly updated attack signatures that are maintained by the vendor's research team via 24x7 monitoring of the Internet to identify the most significant and recent botnets and attack strategies
13	The system must enforce correct protocol usage and block malformed SSL/TLS requests.
14	The system must detect unreasonably extended TLS/SSL headers
36	The system must detect rate based and connection exhausting attacks against SSL/TLS
37	The solution must be able to mitigate DoS vectors focusing on protocol weaknesses of HTTP Slowloris
38	The solution must be able to mitigate DoS vectors focusing on protocol weaknesses of HTTP Slow Post
39	The solution must be able to mitigate DoS vectors focusing on protocol weaknesses of HTTP such as Hash DoS or HTTP Cache Abuse DDoS
40	The solution must be able to mitigate DoS vectors focusing on protocol weaknesses of HTTP Get Flood
41	The system must allow protection parameters to be changed while a protection is running
42	The solution must be able to protect following LAND, Fake Session, Recursive GET (web scraping)
<b>Solution Management &amp; Reporting Requirements</b>	
1	The solution Graphical User Interface (GUI) must allow for multiple levels of access including administrator and operator levels. The GUI access must be via HTTPS
2	The solution GUI must include a change log that reports all relevant events that might affect its administration including user logins, configuration changes, CLI commands and solution updates
3	The solution must provide the ability to create and export diagnostics packages that contain configuration and status information to be used for troubleshooting purposes.
4	The solution must provide the ability to manage its files through the GUI, including upload, download and deletion.
5	The solution must provide a CLI interface that provides solution monitoring functions and CLI access must be provided using SSH
6	The solution must provide a alert/notification provision like Syslog, SNMP or SMTP to alert administrators on important events.
7	The solution must allow for configuration of multiple local user accounts

S.No	Technical Specifications
8	The solution must provide user- level privilege access controls that may be assigned to users or groups of users to enforce privilege separation
9	The solution must support multiple authentication mechanisms via local, RADIUS, TACACS
10	The solution must have provision to define IP Access Control lists for all remote services that are accessible
11	The solution must provide the ability to backup and restore the solution configuration.
12	The solution must provide the ability to configure scheduled automatic backups, download/upload backup files, view backups that have been created, and manually backup data
<b>Reporting</b>	
1	The solution must provide an appliance status dashboard that includes information about active alerts, all protections applied to traffic, total passed and blocked traffic, blocked hosts, traffic through the interfaces and solution CPU/Memory status
2	The solution must provide summary reporting of user defined Top IP Sources and Destinations
3	The solution must display summary reporting by Country classification
4	The solution must display statistics on the amount of dropped and passed traffic
5	The solution must provide detailed statistics and graphs for specific prefixes, showing their impact on traffic over a custom specified interval
6	The solution must display real- time protection statistics on dropped and passed traffic in bytes and packets, with rate statistics in bps and pps
7	The detailed statistics and graphs for each protection group for Servers like Web, DNS, File Servers, Custom Servers must include information on total traffic, total passed/blocked traffic, number of blocked hosts, statistics on each prevention type, traffic by URL, traffic by Domain, IP Location information, Protocol distribution, Services distribution, Web Crawlers, and statistics on top blocked hosts
8	The solution must support the generation of pdf reports containing the detailed statistics and graphs for any user defined entity from the solution
9	The solution must support the generation of e-mail reports with the detailed statistics and graphs for any user defined entity from the solution
10	The solution shall be able to perform time synchronization (ntp, etc)
11	The solution shall support monitoring using snmp version 3

S.No	Technical Specifications
12	The solution must provide built in logging to 3rd party security event tracking systems (SIEM)
	<b>Additional feature support</b>
1	The solution shall support an open API that has SOAP/XML message exchanges that allow 3rd party to fully administer the solution.
2	Should have market ready API for SDN environment integration for attack mitigation

#### 5.2.2.18 Centralised Anti-virus Solution

- a) Shall be able to scan through several types of compression formats.
- b) Must update itself over internet for virus definitions, program updates etc. (periodically as well as in push-updates in case of outbreaks)
- c) Able to perform different scan Actions based on the virus type (Trojan/ Worm, Joke, Hoax, Virus, other)
- d) Shall be able to scan only those file types which are potential virus carriers (based on true file type)
- e) Shall be able to scan for HTML, VBScript Viruses, malicious applets and ActiveX controls
- f) Shall provide Real-time product Performance Monitor and Built-in Debug and Diagnostic tools, and context- sensitive help.
- g) The solution must support multiple remote installations
- h) Shall provide for virus notification options for Virus Outbreak Alert and other configurable Conditional Notification.
- i) Should be capable of providing multiple layers of defence
- j) Shall have facility to clean, delete and quarantine the virus affected files.
- k) Should support scanning for ZIP, RAR compressed files, and TAR archive files
- l) Should support online update, where by most product updates and patches can be performed without bringing messaging server off-line.
- m) Should use multiple scan engines during the scanning process
- n) Should support in-memory scanning so as to minimize Disk IO.

- o) Should support Multi-threaded scanning
- p) Should support scanning of nested compressed files
- q) Should support heuristic scanning to allow rule-based detection of unknown viruses
- r) Updates to the scan engines should be automated and should not require manual intervention
- s) All binaries from the vendor that are downloaded and distributed must be signed and the signature verified during runtime for enhanced security
- t) Updates should be capable of being rolled back in case required
- u) File filtering should be supported by the proposed solution; file filtering should be based on true file type.
- v) Should support various types of reporting formats such as CSV, HTML and text files
- w) Shall scan at least HTTP, FTP traffic (sending & receiving) in real time and protect against viruses, worms & Trojan horse attacks and other malicious code.

#### **5.2.2.19** Directory services

- Should be compliant with LDAP v3
- Support for integrated LDAP compliant directory services to record information for users and system resources
- Should provide authentication mechanism across different client devices / PCs
- Should provide support for Group policies and software restriction policies
- Should support security features, such as Kerberos, Smart Cards, Public Key Infrastructure (PKI), etc.
- Should provide support for X.500 naming standards
- Should support that password reset capabilities for a given group or groups of users can be delegated to any nominated user
- Should support that user account creation/deletion rights within a group or groups can be delegated to any nominated user
- Should support directory services integrated DNS zones for ease of management and administration/replication.

## 5.3 Smart Sensors

### 5.3.1 Functional Specifications

- a) Smart environment sensors will gather data about pollution, temperature, rains, levels of gases in the city (pollution) and any other events on a daily basis. It is for information of citizens and administration to further take appropriate actions during the daily course / cause of any event.
- b) The environment sensors should have the following capabilities:
  - They should be rugged enough to be deployed in open air areas, on streets and parks
  - They should be able to read and report at least the following parameters: Temperature, Humidity, Ambient Light, Sound, CO, NO<sub>2</sub>, CO<sub>2</sub>, SO<sub>2</sub>.
- c) Smart environment sensors will enable citizen to keep a check on their endeavors which impact environment and enable the city to take remedial action if required. These environmental sensors can also be connected via 3G or 4G wireless network. It is not mandatory to connect all sensors via MPLS fiber network.
- d) The data should be collected in a software platform that allows third party software applications to read that data. Various environment sensors shall sense the prevailing environment conditions and send the data to the integrated control system where real time data resides and the same shall be made available to various other departments and applications for decision making.
- e) Successful bidder can also make use of the nearby variable messaging displays wherever possible.
- f) The sensor management platform should allow the configuration of the sensor to the network and also the locational details etc.
- g) Bidder needs to make relevant information available on the displays along with other environmental sensor data in consultation with Authority. If data is available in any existing external system of Authority, then the same shall be integrated by the bidder with the Command & Control System.
- h) Additionally, the bidder should install water level monitoring (flood sensors) at low lying areas of the city. These locations may differ from the locations of other environmental sensors and need to be finalized after the detailed survey of locations by the successful bidder, in consultation with Authority. The bidder should consider implementation of these sensors across the specified locations.
- i) The environment sensors will measure and log the data from locations described in the subsequent sections of the bid document.

### 5.3.2 Technical Specifications

#### 5.3.2.1 Technical Specifications – Pollution / Environmental Sensors

#	Parameter	Specification
1.	Measurement principle	<ul style="list-style-type: none"> <li>Temperature, Humidity, Ambient Light, Sound, CO, NO<sub>2</sub>, CO<sub>2</sub>, SO<sub>2</sub></li> </ul>
2.	Measurement component Measurement range	<ul style="list-style-type: none"> <li>NO<sub>2</sub>: 0 to 10 ppm</li> <li>SO<sub>2</sub> : 0 to 500 ppm</li> <li>CO : 0 to 50ppm, 5000ppm</li> <li>O<sub>3</sub>: up to 1000 ppb</li> <li>CO<sub>2</sub> : 0 to 10% / 0 to 20%</li> <li>PM 2.5: 0 to 230 micro gms / cu.m</li> <li>PM 10: 0 to 450 micro gms / cu.m</li> <li>Light: up to 10,000 Lux</li> <li>UV: up to 15 mW/ cm<sup>2</sup></li> <li>Noise: up to 120 dB (A)</li> </ul>
3.	Repeatability	<ul style="list-style-type: none"> <li>±0.5% FS</li> </ul>
4.	Temperature and Humidity Sensor	<ul style="list-style-type: none"> <li>Real-time Temperature Range: Indoor -10°C ~ +70°C (+14°F ~ +122°F)</li> <li>Real-time in Air Humidity Level Display (up to 100%)</li> </ul>
5.	Response speed	<ul style="list-style-type: none"> <li>120 seconds max. for 90% response from the analyzer inlet</li> </ul>
6.	Connectivity (Minimum)	<ul style="list-style-type: none"> <li>USB / Ethernet connectively to graphical display</li> </ul>

#### 5.3.2.2 Technical Specifications – Flood Sensors

#	Parameter	Specification
1.	Measurement principle	<ul style="list-style-type: none"> <li>Flood Sensors</li> </ul>
2.	Water levels (for flood monitoring)	<ul style="list-style-type: none"> <li>Installation of new sensors and Data integration with existing system (APIs will be provided)</li> </ul>
3.	Accuracy	<ul style="list-style-type: none"> <li>±3 mm, depending on stratification</li> </ul>

#### 5.3.2.3 Technical Specifications – Rain Gauges Sensors

#	Parameter	Specification
1.	Measurement principle	<ul style="list-style-type: none"> <li>Rainfall</li> </ul>
2.	Rain Water measurement	<ul style="list-style-type: none"> <li>Rainfall in millimetres (mm)</li> </ul>
3.	Accuracy	<ul style="list-style-type: none"> <li>± 2% at 0 mm/hr to 250 mm/hr</li> <li>± 3% at 250 mm/hr to 500 mm/hr</li> </ul>

## 5.4 Variable Messaging Display Board (VMD)

### 5.4.1 Functional Specifications

- a) VMD will be installed at identified strategic locations. The location of VMDs will be on the key junctions (mostly on the sides without obstructing the traffic) and other strategic locations with large foot fall. The VMD software application will allow user to publish specific messages for managing traffic and also general informative messages.
- b) VMD will enable Authority to communicate effectively with citizens and also improve response while dealing with exigency situations. These will also be used to regulate the traffic situations across the city by communicating right messages at the right time.
- c) The variable message display shall consist of variable message signboard with local controller, for local controls in few situations.
- d) A VMD software system shall be provided to the Command and Control Center for message preparation monitoring and control of the variable message signs. IP based Network equipment shall be provided to connect the VMD with the VMD software system.
- e) VMD software application will provide the normal operator to publish predefined sets of messages (textual / image). The application shall have an option for supervisor (someone with appropriate authority) to bypass the control during certain situations and to write in free-text mode.
- f) VMD software application will allow an operator to seamlessly toggle between multiple VMS points at each workstation in order to send specific messages to specific locations, as well as sending common message to all VMDs.
- g) VMD software application will accommodate different access rights to various control unit functionalities depending on operator status and as agreed with the client. Software should be GUI based, and capable to handle 200 VMS signage. User should be able to select desired location in Map and this should enable user to see the live status of that specific VMD.
- h) The variable messaging displays can also be used for advertisement purposes. Approximately 20% of the total running time will be utilized by Authority for its own discretion whereas the remaining time can be used by the SI for advertisement purpose.
- i) The land for VMDs will be provided to the SI at no extra cost. Also no rental/lease charges will be levied on the bidder for using the land for Variable Message Signboards.



## 5.4.2 Technical Specifications

### 5.4.2.1 Display

#	Specifications	Minimum Requirements
1.	Location	<ul style="list-style-type: none"> <li>To be installed at locations identified by Authority and the text on the sign must be readable even in broad daylight</li> </ul>
2.	Colour	<ul style="list-style-type: none"> <li>True Colour</li> </ul>
3.	Brightness & Legibility	<ul style="list-style-type: none"> <li>To be read even in broad daylight without any shade</li> <li>The displayed image shall not appear to flicker to the normal human eye</li> <li>&gt;6000 cd/m<sup>2</sup></li> </ul>
4.	Luminance Class	<ul style="list-style-type: none"> <li>L-3 as per EN 12966</li> </ul>
5.	Contrast Ratio	<ul style="list-style-type: none"> <li>R2-R3 as per EN 12966</li> </ul>
6.	Beam Width	<ul style="list-style-type: none"> <li>B6+ : Viewing angle shall ensure message readability for citizens, motorists, pedestrians, etc. on the respective locations</li> </ul>
7.	Display capability	<ul style="list-style-type: none"> <li>Fully programmable, full colour, full matrix, LED displays</li> <li>Alpha-numeric, Pictorials, Graphical &amp; video</li> </ul>
8.	Display Language	<ul style="list-style-type: none"> <li>To support both pictograms and bilingual (English and Devanagari) text</li> </ul>
9.	Display Front Panel	<ul style="list-style-type: none"> <li>It shall utilize a front face that is smooth, flat, scratch-resistant, wipe-clean</li> <li>100% anti-glare</li> </ul>
10.	Message Creation	<ul style="list-style-type: none"> <li>Through both a Central Control Room Application and a local Laptop/Device loaded with relevant software</li> </ul>
11.	Language	<ul style="list-style-type: none"> <li>Multilingual (Tamil/English) and all fonts supported by windows</li> </ul>
12.	Auto Dimming	<ul style="list-style-type: none"> <li>Auto dimming adjusts to ambient light level.</li> </ul>
13.	In built Sensor	<ul style="list-style-type: none"> <li>Photoelectric sensor</li> </ul>
14.	Storage capacity	<ul style="list-style-type: none"> <li>Minimum 60 GB</li> </ul>
15.	Display Area	<ul style="list-style-type: none"> <li><b>Double Sided</b> Display size of VMD should be two standard sizes to the tune of</li> <li>&gt; Large VMD : 4.8 x 1.9meters &amp;</li> <li>&gt; Small VMD : 3.8 x 1.9 meters</li> </ul>
16.	Number of Lines & Characters	<ul style="list-style-type: none"> <li>The number of lines and characters can be customized as per the requirement (Min 3 Lines &amp; 10 Characters)</li> </ul>
17.	Brightness & contrast	<ul style="list-style-type: none"> <li>Controlled through software from central CCC</li> </ul>

#	Specifications	Minimum Requirements
18.	Display Driving method	<ul style="list-style-type: none"> <li>Direct current control driving circuit. Driver card of display applies Direct Current Technology</li> </ul>
19.	Display Style	<ul style="list-style-type: none"> <li>Steady, flash, partial flash, right entry, left entry, top entry, bottom entry, center spread, blank, and dimming</li> </ul>
20.	Connectivity	<ul style="list-style-type: none"> <li>IP Based</li> </ul>
21.	Access Control	<ul style="list-style-type: none"> <li>Access control mechanism would be also required to establish so that the usage is regulated.</li> </ul>
22.	Integration	<ul style="list-style-type: none"> <li>Interface with GPRS or Ethernet</li> <li>Integration with Command and Communications Center and service providers for offering G2C and B2C services</li> </ul>
23.	Construction	<ul style="list-style-type: none"> <li>Mounting structure shall use minimum 6 Mtrs. high hexagonal/octagonal MS Pole or suitable structure with 5.5 mtr. Minimum vertical clearance under the VMS sign from the Road surface.</li> </ul>
24.	Battery	<ul style="list-style-type: none"> <li>230VAC+ 15%, 50Hz, Single Phase (automatically re-start in the event of an electricity supply failure)</li> <li>Batteries with solar charging options can also be recommended as back up</li> </ul>
25.	Power	<ul style="list-style-type: none"> <li>Automatic on/off operation with automatic power backup</li> </ul>
26.	Casing	<ul style="list-style-type: none"> <li>Weather-proof Display for VMS</li> <li>IP-66 rated for housing all control equipment</li> </ul>
27.	Operating conditions	0° to 55°C
28.	Message Validity	<ul style="list-style-type: none"> <li>If the controller is unable to connect to the server for the next message, it shall not display the old message, which has passed its expiry time. Instead it shall be programmed to display a default message.</li> </ul>

#### 5.4.2.2 Application Software for VMS (Control Messaging Application at Data Center)

The Application System for Controlling Messaging for VMS shall:

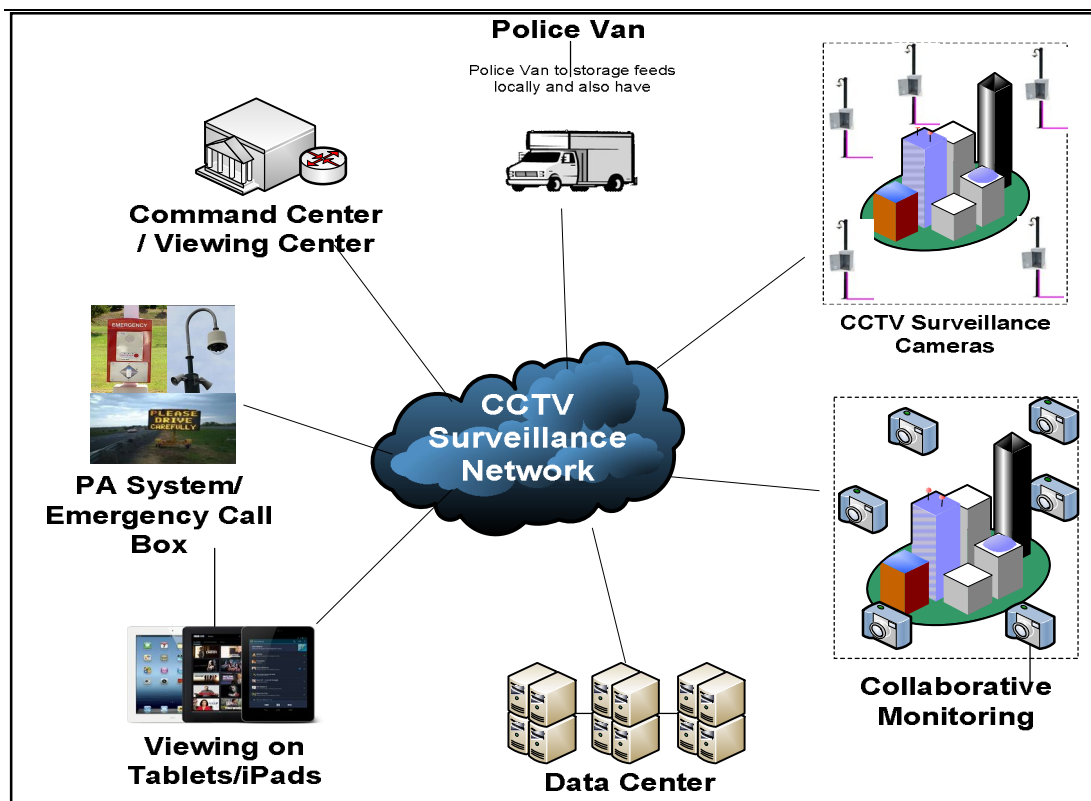
- 1) Be deployable over multiple (3 to 4) workstations.
- 2) Ensure that provision for feeding/updating the following information:
- 3) VMS messages and information
- 4) Types of possible scenarios per VMS
- 5) Types of possible messages to be displayed on each VMS during various scenarios
- 6) Ensure that the normal operator users are not able to publish any custom message and shall only display predefined sets of messages.

- 7) The application shall have an option for Supervisor (someone with appropriate authority) to bypass the control during certain situations and to write in free-text mode.
- 8) Ensure that users can publish specific messages for managing traffic and also general informative messages.
- 9) Allow an operator to seamlessly toggle between multiple VMS points at each workstation in order to send specific messages to specific locations.
- 10) Accommodate different access rights to various control unit functionalities depending on operator status and as agreed with the client.

## 5.5 City Surveillance & Disaster Management

### 5.5.1 City Surveillance

A High level system overview of the proposed CCTV Surveillance System for Chennai City is given in the diagram below:



Feed/Message to Police Van is optional

#### **5.5.1.1 Surveillance Equipment**

The project includes surveillance of about across Chennai City. These locations would get covered through different types of surveillance cameras including Fixed Box Camera and PTZ Cameras.

The Implementation vendor (SI) shall assess the feasibility to use any existing electricity, phone or advertisement poles during initial site surveys. SI shall also assess the feasibility of leveraging other structures such as areas under a bridge or billboards. For the locations identified for re-purposing the existing poles or structures, an agreement shall be signed between the SI, Authority, and other relevant stakeholders for use of the facility for the Chennai Smart City Project.

SI should ensure that proper protection is taken against power surges and ensure power stabilization to the surveillance equipment. The System Integrator would need to follow required earthing standards (e.g. IS-3043) and ensure that pole and the edge level components are protected against lightning. In addition, Junction box design should be modular and each component should be well organized and clamped inside to ensure components do not heat up or fall out on opening. For Electricity / Power, SI to bear the initial provisioning charge while recurring charge to be reimbursed by Chennai Municipal Corporation on actuals.

The proposed video surveillance system will involve setting up of IP based outdoor security cameras across various locations in the Chennai City. The video surveillance data from various cameras deployed will be stored and monitored at Police Control Center and Police shall give selective feeds from Police Control Center to Smart City Datacenter and Command and control centers. SI has to provision video storage at Smart city Datacenter also as a backup.

#### **5.5.1.2 Other Smart Safety Components**

Along with the components of the CCTV Surveillance system, the SI would be responsible to integrate the following services with the CCTV Surveillance system to build an infrastructure for a Smart city system in the Chennai Area.

#### **5.5.1.3 Information security policy, including policies on backup**

System Integrator shall be asked to prepare the Information Security Policy for the overall project, which would be reviewed & finalized by the Chennai Smart City Authority & its Consultant. It is proposed that Security policy would be submitted by the Systems Integrator within 1st quarter of the successful Final Acceptance Tests. The Systems Integrator shall obtain ISO 27001 certification for the Control Center within 2 quarters of final acceptance test. Payment from 3rd Quarter to be withheld till this certification is obtained by the successful bidder.

#### **5.5.1.4 Functional Requirement of the City Surveillance System**

Functional Requirement of the overall Surveillance System can be categorized into following components:

- Information to be Captured by Edge Devices
- Information to be Managed at the Command Center
- Command Center Requirements
- Information to be made available to different Police Personnel
- Operational Requirements
- Storage / Recording Requirements
- Other General Requirements

#### **5.5.1.5 Information to be captured by Edge Devices**

Cameras being the core of the entire Surveillance system, it is important that their selection is carefully done to ensure suitability & accuracy of the information captured on the field and is rugged, durable & compact. These cameras need to work on 24 X 7 basis and transmit quality video feeds to the centralized data center and would capture the video feeds at 1080p, 18 FPS for majority of the time and at 12 FPS for the lean period. However, Authority may take the regular review of the requirements for video resolution, FPS and may change these numbers to suit certain specific requirements (for example, there could be a situation when certain cameras are required to be viewed at higher FPS for specific period. It is estimated that not more than 0.5% of the cameras would be required to be viewed at higher FPS at a given point of time).

The complete tracking of a 'wanted' vehicle identified or flagged by Police should be possible on the GIS map.

It is recommended to clearly identify in SLAs that cameras need to transmit quality video feed (appropriately focused, clear, un blurred, jitter free, properly lit, unobstructed, etc.). Packet loss to be less than 0.5%.

#### **5.5.1.6 Information to be analyzed at the Command Centers**

The proposed Video Management System shall provide a complete end-to-end solution for security surveillance application. The Bidder has to provide VMS client software at the police Control center and the respective police station to Monitor and manage all the surveillance cameras which is part of the Smart city. Also SI has to facilitate the integration of the smart city VMS with the existing Police VMS. If there is any additional Hardware/ Software requirement for the Integration the Bidder has to specify the same in the price Bid. The control center shall allow an operator to view live / recorded video from any camera on the IP Network. The combination of control center and the IP Network would create a virtual matrix, which would allow switching of video streams around the system.

Not all the cameras would be simultaneously viewed at Command & Control Center. Command Center shall from time to time take decisions on utilization of Alerts / Exceptions / Triggers generated by cameras, and specify the client machines where these would get populated automatically.

Police personnel shall have following access to the video feeds of the cameras of their jurisdiction:

- Viewing rights to all the live Camera Feeds at the Police Control Room/ Respective Police station
- Viewing rights to the stored feeds at the Police Control Room/ Respective Police station
- Access to view Alerts / Exceptions / Triggers raised
- Trail Report on specific person / object / vehicle for a specific period / location
- Personalized Dashboard (depending upon grade of police officer)
- Accessibility to advanced analytics on recorded footages
- Provide search of recorded video. Advanced search should be possible based on various filters like alarm / event, area, camera, etc.

#### **5.5.1.7 Command Center Requirements**

- Alarm Monitor

Alarm Monitors must show the name of alarms when generated. The layout must not be restrictive.

- Guard Tours

System should allow automatic launching of Guard Tours based upon factors like Time / Date / Bookmarked event

- Customizable and programmable Event Response Mechanism

All the Event Response Mechanisms must be customizable based upon functional parameters like criticality, region, access, automatic/manual etc. (not limited to these four). SOPs for the daily incident management to be designed and approved by Police Personnel and same must be implementable in the system.

System must allow generation of reports for all Incidents based upon filters like Criticality, Current Status, Date / Time (not limited to these). System to support excel/pdf for export.

- Quick and easy integration to 3rd Party systems

System must support API based integration with other systems like eChallan, CCTNS etc. or any other 3<sup>rd</sup> Party system with allows API based integration

Other functionalities like Proper Device Grouping and User Management (including PTZ privileges) must be exportable at the access level of the user of the system for the review by the concerned authorities. Export file can be an Excel file or pdf. User must be able to export access report at his/her own level of authority.

Dashboards generated by the system (functional / technical) must be customizable based upon the user's requirements. The system must remember the edits done by the user to his/her own dashboard when he logs in next time in the system.

System should allow generation of Audit Reports for the perusal of concerned Police Authorities.

#### **5.5.1.8 Role Based Access to the Entire System**

Various users should have access to the system using single sign on and should be role based. Different roles which could be defined (to be finalized at the stage if SRS) could be Administrator, Supervisor, Officer, Operator, etc. Apart from role based access, the system should also be able to define access based on location. Other minimum features required in the Role Based authentication Systems are as follows:

- The Management Module should be able to capture basic details (including mobile number & email id) of the Police Personnel & other personnel requiring Viewing / Administration rights to the system. There should be interface to change these details, after proper authentication.
- Rights to different modules / Sub-Modules / Functionalities should be role based and proper log report should be maintained by the system for such access.
- Biometric standardized coupled with login name & password should be enabled to ensure that only the concerned personnel are able to login into the system.
- Surveillance System should have capability to map the cameras to the Police Personnel from different. There should be interface to change these mappings too.
- For PTZ cameras, there should be provision to specify hierarchy of operators / officers for control of the cameras from various locations.

#### **5.5.1.9 Storage / Recording Requirements**

It is proposed that the storage solution is modular enough to ensure compliance to the changes in storage / recording policy, to be evolved upon initial deployment of the system. As decided in the meeting of consultants & Chennai City Police Officials following storage requirements are proposed for the project:

- **The storage solution proposed is that the video feeds would be available for 30 days.** After 30 days, the video feeds would be overwritten unless it is flagged or marked by the Police for investigation or any other purpose. The video feeds of all relevant cameras capturing the incident in question would be stored until the Police deem it good for deletion.
- For incidents that are flagged by the Police or any court order, the video of the relevant portion from all relevant cameras should be stored/archived separately for investigation purposes and a committee at Authority can decide when this video feed can be deleted.
- Full audit trail of reports to be maintained for 90 days.
- The Recording Servers / System, once configured, shall run independently of the Video Management system and continue to operate if the Management system is off-line.

- The system shall support the use of separate networks, VLANs or switches for connecting the cameras to the recording servers to provide physical network separation from the clients and facilitate the use of static IP addresses for the devices.
- The system shall support H.264 or better, MPEG-4 and MJPEG compression formats for all analog cameras connected to encoders and all IP cameras connected to the system.
- The system shall record the native frame rate and resolution supplied by the camera or as configured by the operator from the System Administration Server.
- The system should not limit amount of storage to be allocated for each connected device.
- The on-line archiving capability shall be transparent and allow Clients to browse and archive recordings without the need to restore the archive video to a local hard drive for access.
- The system shall allow for the frame rate, bit rate and resolution of each camera to be configured independently for recording. The system shall allow the user to configure groups of cameras with the same frame rate, bit rate and resolution for efficient set-up of multiple cameras simultaneously.
- The system shall support Archiving or the automatic transfer of recordings from a camera's default database to another location on a time-programmable basis without the need for user action or initiation of the archiving process. Archiving shall allow the duration of the camera's recordings to exceed the camera's default database capacity. Archives shall be located on either the recording server or on a connected network drive. If the storage area on a network drive becomes unavailable for recording the system should have the ability to trigger actions such as the automatic sending of email alerts to necessary personnel.
- Bandwidth optimization
  - The Recording Server / System shall offer different codec (H.264, MJPEG, MPEG-4, etc.) and frame rate (CIF, 4CIF, QCIF) options for managing the bandwidth utilization for live viewing on the Client systems.
  - From the Client systems, the user shall have the option of having video images continually streamed or only updated on motion to conserve bandwidth between the Client systems and the Recording Server.
- The Recording Server / System shall support Camera (analogue and IP cameras) devices from various manufacturers.
- The Recording Server / System shall support the PTZ protocols of the supported devices listed by the camera OEMs.
- The system shall support full two-way audio between Client systems and remote devices.
- Failover Support



- The system shall support automatic failover for Recording Servers. This functionality shall be accomplished by Failover Server as a standby unit that shall take over in the event that one of a group of designated Recording Servers fails.
- The system shall support multiple Failover Servers for a group of Recording Servers.
- **SNMP Support**
  - The system shall support Simple Network Management Protocol (SNMP) in order for third-party software systems to monitor and configure the system.
  - The system shall act as an SNMP agent which can generate an SNMP trap as a result of rule activation in addition to other existing rule actions.

#### **5.5.1.10 Other General Requirements**

##### *5.5.1.10.1 Management / Integration functionality*

- The Surveillance System shall offer centralized management of all devices, servers and users.
- The Surveillance System should not have any limit on the number of cameras to be connected for Surveillance, Monitoring and recording. Any increase in the no. of cameras should be possible by augmentation of Hardware components.
- The Surveillance System shall support distributed viewing of any camera in the system using Video walls or big screen displays.
- The Surveillance System shall support alarm management. The alarm management shall allow for the continuous monitoring of the operational status and event-triggered alarms from system servers, cameras and other external devices.
- It should be possible to integrate the Surveillance System with 3<sup>rd</sup>-party software, to enable the users to develop customized applications for enhancing the use of video surveillance solution. For e.g., integrating alarm management to initiate SMS, E-Mail, VoIP call etc.
- The Management system shall store the overall network elements configuration in central database, either on the management server computer or on a separate DB Server on the network.
- System should be able to be integrated with Event Management / Incident Management System, if implemented by Chennai City Authority/ Chennai Municipal Corporation in future.

##### *5.5.1.10.2 System Administration functionality*

- The System Administration Server shall provide a feature-rich administration client for system configuration and day-to-day administration of the system.

- The System Administration Server shall support different logs related to the Management Server.
  - The System Log
  - The Audit Log
  - The Alert Log
  - The Event Log

- Rules

The system shall support the use of rules to determine when specific actions occur. Rules shall define what actions shall be carried out under specific conditions. The system shall support rule initiated actions such as:

- Start and stop recording
- Set non-default live frame rate
- Set non-default recording rate
- Start and stop PTZ patrolling
- Send notifications via email
- Pop-up video on designated Client Monitor recipients

#### **5.5.1.10.3 Client system**

The Client system shall provide remote users with rich functionality and features as described below.

- Viewing live video from cameras on the surveillance system
- Browsing recordings from storage systems
- Creating and switching between multiple of views.
- Viewing video from selected cameras in greater magnification and/or higher quality in a designated hotspot.
- Controlling PTZ cameras.
- Using digital zoom on live as well as recorded video.
- Using sound notifications for attracting attention to detected motion or events.
- Getting quick overview of sequences with detected motion.
- Getting quick overviews of detected alerts or events.
- Quickly searching selected areas of video recording for motion (also known as Smart Search).

#### **5.5.1.10.4 Remote Web Client**

The web-based remote client shall offer live view including PTZ control and event / output activation. The Playback function shall give the user concurrent playback of multiple recorded videos with date, alert sequence or time searching.

- a) User Authentication – The Remote Client shall support logon using the user name and password credentials.

#### **5.5.1.10.5 Matrix Monitor**

- a) Matrix Monitor – The Matrix Monitor feature shall allow distributed viewing of multiple cameras on the system on any monitor.
- b) The Matrix Monitor feature shall access the H.264/MJPEG/MPEG4 stream from the connected camera directly and not sourced through the recording server.

#### **5.5.1.10.6 Alarm Management Module**

- a) The alarm management module shall allow for continuous monitoring of the operational status and event-triggered alarms from various system servers, cameras and other devices. The alarm management module shall provide a real-time overview of alarm status or technical problems while allowing for immediate visual verification and troubleshooting.
- b) The alarm management module shall provide interface and navigational tools through the client including;
  - i. Graphical overview of the operational status and alarms from servers, network cameras and external devices including motion detectors and access control systems.
  - ii. Intuitive navigation using a map-based, hierarchical structure with hyperlinks to other maps, servers and devices or through a tree-view format.
- c) The module shall include flexible access rights and allow each user to be assigned several roles where each shall define access rights to cameras.
- d) Basic VMS should be capable to accept third party generated events / triggers

#### **5.5.1.11 Other Miscellaneous Requirements**

- System should have a facility to create CDs or other storage media for submission to Judiciary, which can be treated evidence for legal matters. Such storage media creation should be tamper proof and SI to provide appropriate technology so that integrity and quality of evidence is maintained as per requirements of the judiciary. Bidder is required to specify any additional hardware / software required for this purpose. SI will also prepare the guideline document to be followed by the Police Personnel for the retrieval of Video / images from the CCTV System so as to maintain integrity of the evidence. Such

a guideline document should include methods of retrieval of data, check-list to be followed and flowchart of the entire process to be followed.

- All the systems proposed and operationalization of Video Management System should comply with requirements of IT Acts.
- Bidder shall be required to provide a standardized Mobile Application integrate smart phones and tablets for 2-way communication with the Video Management System in a secure manner. Chennai City Authority may provide such tablets / smart phones to the designated Police Personnel. It will be responsibility of SI to configure such tablets / Smartphone with the Surveillance System and ensure that all the necessary access is given to these mobile users so that uploading of video / pictures to the surveillance system is possible.
- **Surveillance camera feeds from national highway Toll plaza, private residence, hospital places of large public gathering, Etc. needs to integrated to CCC solution**

There would be the provision for Third party audit periodically, paid by Authority separately.

#### **5.5.1.12 Video Management System**

Video management system shall constitute of a platform which will be designed for viewing, recording and replaying acquired video as part of overall project solution. This platform will be based on the Internet Protocol (IP) open platform concept. Major functionalities are described here:

##### *5.5.1.12.1 VMS Overview*

1. VMS shall be used for centralized management of all field camera devices, video servers and client users.
2. VMS server shall be deployed in a clustered server environment/Support in built for high availability and failover for directory & recording servers
3. VMS shall support a flexible rule-based system driven by schedules and events.
4. VMS shall be supported for fully distributed solution for monitoring and control function, designed for limitless multi-site and multiple server installations requiring 24/7 surveillance with support for devices from different vendors.
5. VMS shall support internet protocol (IP) cameras from major vendors.
6. The Contractor shall clearly list in their proposal the make and models that can be integrated with the VMS, additionally all the offered VMS and cameras must have Open Network Video Interface Forum (ONVIF) compliance.
7. VMS shall be enabled for any standard storage technologies and video wall system integration.
8. VMS shall be enabled for integration with any external Video Analytics Systems both edge & Server based
9. VMS shall be capable of being deployed in a virtualized server environment without loss of any functionality.

10. All CCTV cameras locations shall be overlaid in graphical map in the VMS Graphical User Interface (GUI). The cameras selection for viewing shall be possible via clicking on the camera location on the graphical map. The graphical map shall be of high resolution enabling operator to zoom-in for specific location while selecting a camera for viewing.
11. VMS shall have an administrator interface to set system parameters, manage codecs, manage permissions and manage storage.
12. VMS day to day control of cameras and monitoring on client workstations shall be controlled through the administrator interface.
13. Whilst live control and monitoring is the primary activity of the monitoring workstations, video replay shall also be accommodated on the GUI for general review and also for pre- and post-alarm recording display.
14. The solution design for the VMS shall provide flexible video signal compression, display, storage and retrieval.
15. All CCTV camera video signal inputs to the system shall be provided to various command control center(s), viewing center etc., and the transmission medium used shall best suit the relative camera deployments and access to the CCTV Network.
16. VMS shall be capable of transferring recorded images to recordable media (such as CD/DVD and/or tapes) in tamper evident and auditable form. All standard formats shall be supported including, but not limited to:
  - a) AVI files
  - b) MP4 Export or latest
17. For Video Exports with VMS's Native Format along with Watermark and Encrypted with SSL / TSL technology, one can protect the video tampering and prove that the video is not tampered
18. All streams to the above locations shall be available in real-time and at full resolution. Resolution and other related parameters shall be configurable by the administrator in order to provide for network constraints.
19. The VMS shall support field sensor settings. Each channel configured in the VMS shall have an individual setup for the following settings, the specific settings shall be determined according to the encoding device:
  - a) Brightness
  - b) Contrast
  - c) Color
  - d) Sharpness
  - e) Saturation
  - f) Hue
  - g) White balance
20. The VMS shall support the following operations:
  - a) Adding an IP device
  - b) Updating an IP device
  - c) Updating basic device parameters
  - d) Adding/removing channels

- e) Adding/removing output signals
  - f) Updating an IP channel
  - g) Removing an IP device
  - h) Enabling/disabling an IP channel
  - i) Refreshing an IP device (in case of firmware upgrade)
21. The VMS shall support retrieving data from edge storage. Thus when a lost or broken connection is restored, it shall be possible to retrieve the video from SD card and store it on central storage.
  22. The VMS shall support bookmarking the videos. Thus, allowing the users to mark incidents on live and/or playback video streams.
  23. VMS shall support automatic failover for recording. Some Critical cameras shall also be supported for Redundant (Mirrored Recording simultaneously)
  24. VMS shall support manual failover for maintenance purpose.
  25. VMS shall support access and view of cameras and views on a smartphone or a tablet (a mobile device).
  26. VMS shall support integration with the ANPR application
  27. VMS shall support integration with other online and offline video analytic applications.
  28. VMS shall be able to accept alerts from video analytics built into the cameras, other third party systems, sensors etc.
  29. VMS shall support manual failover of Directory for maintenance purpose
  30. System should support recording management to view the recordings available on a camera's local storage device (such as an SD card), and copy them to the server.
  31. The VMS shall support replacement of the edge device with another device, while maintaining past recordings according to the defined retention period and device logical entities association (triggers association, pages, etc.)
  32. The VMS shall support LoS (Level of Service) mechanism, choosing between several video streams according to its performance parameters and networking capabilities of the workstation and/or decoder.
  33. The VMS recorders' performance shall support 100% of recording channels, 30% of the channels with live monitoring and 20% of the channels with playbacks all at the same time.

#### **5.5.1.12.2 Client system**

The Client system shall provide remote users with rich functionality and features as described below.

1. Viewing live video from cameras on the surveillance system
2. Browsing recordings from storage systems
3. Creating and switching between multiple of views.
4. Viewing video from selected cameras in greater magnification and/or higher quality in a designated hotspot.
5. Using digital zoom on live as well as recorded video.
6. Using sound notifications for attracting attention to detected motion or events.
7. Getting quick overview of sequences with detected motion.

8. Getting quick overviews of detected alerts or events.
9. Quickly searching selected areas of video recording for motion (also known as Smart Search).
10. The VMS shall use its own streaming server to efficiently stream the videos.
11. When the VMS client is set to view the live videos in say 3x3, 4x4 and 5x5 grids, the VMS should display lower resolution, high frame rate video to avoid high bandwidth and CPU usage on the VMS client
12. When the user selects a particular camera, and wants to view it in full screen, the VMS should automatically show the highest quality and high frame rate video.

#### **5.5.1.12.3 Web Client**

1. The web-based remote client shall offer live view, including PTZ control (if applicable) and event / output activation. The Playback function shall give the user concurrent playback of multiple recorded videos with date, alert sequence or time searching.
2. User Authentication – The Remote Client shall support logon using the user name and password credentials

#### **5.5.1.12.4 Alarm Monitoring**

1. The VMS shall allow for continuous monitoring of the operational status and event-triggered alarms from various system servers, cameras and other devices. It shall provide a real-time overview of alarm status or technical problems while allowing for immediate visual verification and troubleshooting.
2. It shall provide interface and navigational tools through the client including;
3. Graphical overview of the operational status and alarms from servers, network cameras and external devices including motion detectors and access control systems.
4. Intuitive navigation using a map-based, hierarchical structure with hyperlinks to other maps, servers and devices or through a tree-view format.
5. It shall include flexible access rights and allow each user to be assigned several roles where each shall define access rights to cameras.
6. Basic VMS should be capable to accept third party generated events / triggers

#### **5.5.1.12.5 Other functionality**

1. The Surveillance System shall offer centralized management of all devices, servers and users.
2. The Surveillance System should not have any limit on the number of cameras to be connected for Surveillance, Monitoring and recording. Any increase in the no. of cameras should be possible by augmentation of Hardware components.
3. The Surveillance System shall support distributed viewing of any camera in the system using Video walls or big screen displays.
4. It should be possible to integrate the Surveillance System with 3<sup>rd</sup>-party software, to enable the users to develop customized applications for enhancing the use of video

surveillance solution. For e.g., integrating alarm management to initiate SMS, E-Mail, VoIP call etc.

5. System should be able to be integrated with PSIM / Incident Management System.
  6. The System Administration Server shall provide a feature-rich administration client for system configuration and day-to-day administration of the system.
  7. The System Administration Server shall support different logs related to the Management Server.
    - a) The System Log
    - b) The Audit Log
    - c) The Alert Log
    - d) The Event Log
  8. Rules: The system shall support the use of rules to determine when specific actions occur. Rules shall define what actions shall be carried out under specific conditions. The system shall support rule initiated actions such as:
    - a) Start and stop recording
    - b) Set non-default live frame rate
    - c) Send notifications via email
    - d) Pop-up video on designated Client Monitor recipients
- Security Platform shall have strong security mechanism such as the use of advance encryption, digital certificates and claims-based authentication to ensure that only authorized personnel have access to critical information, prevent man-in-the-middle attacks, and that the data is kept private.
  - System should support Report and View Open Incident Cases. This also support associating the video footages pertaining to the incident either received from City CCTV Cameras or shared by public to the police agency. This also allows viewing and downloading and delete Incident clips that are stored on the server by the administrator.

#### **5.5.1.12.6 Failover & Redundancy**

1. Synchronized Failover directory feature should be provided with the offered system to avoid the single point of failure. Also the system should sustain all its current operations i.e. recording, playback and live video even in the event of primary as well as failover directory failure. This functionality can either be loaded on any of the recording server or on a dedicated server. If offered software need dedicated server for this, then the same will be in contractor's scope. Specifications of failover administration server should be same as that of recording server except storage size.
2. Automated Failover recording should be provided to maintain the reliability of the system. In case of failure of one or more of primary recording servers simultaneously. Additional servers/storage required to meet this requirement should be in Contractors scope.
3. Redundant recording/Dual recording feature of the VMS should be supported by VMS. System administrator should get the privilege to configure this feature on any cameras simultaneously depend on the criticality of the cameras.



4. The VMS shall allow for 2-way audio communication using amplifier/call station connected the IP cameras in the field without any need of audio cabling from camera to control room

### **5.5.1.12.7 Video Analytics**

#### **5.5.1.12.7.1 General Requirements:**

1. The Video Analytics shall be designed to provide Intelligent Video Analysis for 24/7 surveillance with support for devices from different vendors.
2. Support any architecture namely distributed, centralized and hybrid
3. Support system openness without using any proprietary format
4. Support commercial-off-the-shelf computing hardware without the need of any proprietary hardware
5. Able to produce reliable analytics at lower resolutions like 4CIF resolution in order to save the computation
6. Able to process at variable resolution and frame rate when if necessary
7. It shall support open platform Video Management System (VMS).
8. It shall provide ONVIF device discovery
9. It shall get video from camera or VMS and send alarms to VMS to be viewed in VMS client
10. It shall stream the Analytics Video to VMS using open interface protocol like ONVIF.
11. It shall support multiple regions of analytics on single video feed.
12. It shall support multiple features to be enabled for each of the regions.
13. It shall support feature based scheduling so that that alarms can be enabled or disabled for a certain period of time.
14. It shall support both Virtual line and Virtual area based features. The virtual area can be of any shape and can be bound by at least 10 end points.
15. It shall support both indoor and outdoor environment.
16. It shall support setting of minimum and maximum object size for detection.
17. It shall support masking of area in a view.
18. It shall support object masking.
19. It shall support analytics capability to run both on server as well as edge (on camera).
20. It shall support simultaneous running of different features both on edge as well as server for same camera
21. It shall support camera independent licensing
22. The VMS shall provide a centralized camera tampering detection solution in real-time by automatically identifying tampering to ensure video image capture and integrity. The solution sends an alert when the following potential tampering is detected:
  - Scene too bright — e.g. flash light, direct sun, laser pointer that is pointed at the camera, causing it to become over saturated.

- Scene too dark — not enough light to see a clear image, if camera is covered.
- Camera is covered or blocked — if something is blocking or partially blocking most of the camera's field of view.
- Camera redirection detection — if camera is redirected from its' initial position of field of view (FOV).
- Unfocused or blurred view — if the camera was sprayed with rain or its focus changed.

23. Automatically search through the recorded video for the original appearance of an object in a scene.

#### **5.5.1.12.7.2 Suspicious incident detection**

1. It shall detect person loitering in a virtual area for more than a pre-defined period.
2. It shall detect crowd assembling in a pre-defined area. The count for the crowd determination should be pre-defined. It shall be able to provide live crowd count.
3. The VA shall support dense and sparse crowds for crowd counting and crowd flow detection
4. The VA shall detect object left out or abandoned in a virtual area by a person beyond a certain pre-defined period.
5. The VA shall detect object removed by a person beyond a certain pre-defined period.
6. The VA shall detect counter flow of people (such as people moving in a wrong way)
7. The VA shall be able to efficiently locate and track a specific person across time and location to minimize search time from hours to minutes when time is of the essence.
8. The VA shall be able to track individuals' movements from location to location and access all relevant associated VMS recordings
9. The VA shall support track individual algorithm to display tracked individuals path and directions on the map.
10. The VA shall support creating a composite (a human-like figure) of the suspect based on eye-witness' description. Many different options should be made available for describing hair color and style, shirts, trousers, patterns, etc.

#### **5.5.1.12.7.3 Other features**

1. It shall be able to stabilize the video when camera is shaking (such as, due to wind) and shall be able to stream the stabilized video to VMS.
2. Ability such that alerts can be searched and categorized based on this information.
  - i. Timestamp (date & time)

- ii. Alert Name
  - iii. Alert Type
  - iv. Alert Location
  - v. Text Description
  - vi. Associated Region
1. It shall provide video summary of all the alarms.
  2. It shall provide reporting option to export reports of alarms in PDF, EXCEL and Image formats and also option to schedule it.
  3. It shall support email and FTP of alarm data and also option to schedule it.
  4. It shall be able to provide comparison reports for different months and year

#### **5.5.1.12.8 Standardized Signs for CCTV Camera Locations**

It is necessary that the CCTV Camera locations put some standardized signs informing the public of the existence of CCTV cameras. This will bring about the transparency on installation of CCTV cameras and no one would be able to later complaint for breach of privacy. Following tables give draft specifications for the signage to be put at the camera locations.

#	Item	Specifications
1	Size	Board Width = 8" / 12" (For type A and B) Board Width = 12" / 18" / 24" (For type C and D)
2	Plate Material	Corrosion resistant Aluminum Alloy as per IRC 67:2001 (Code of Practice for Road signs)
3	Plate Thickness	Minimum 1.5 mm
4	Retro-Reflective sheeting for sign-plate	Weather-resistant, having colour fastness
5	Other Specifications	As per IRC 67:2001 (Code of Practice for Road signs)
6	Mounting	Can be mounted on wall or pole (appropriate mounting brackets to be provided)
7	Design	As per following signage diagrams

#### **5.5.1.12.9 Fixed Box cameras**

#	Parameter	Minimum Specifications or better
1.	Video Compression	H.264
2.	Video Resolution	1920 X 1080
3.	Frame rate	Min. 25 fps
4.	Image Sensor	1/3" Progressive Scan CCD / CMOS
5.	Lens Type	Varifocal, C/CS Mount, IR Correction Full HD lens compatible to camera imager
6.	Lens#	Auto IRIS 8 – 50 mm,
7.	Multiple Streams	Dual streaming with 2 <sup>nd</sup> stream at minimum 720P at 30fps at H.264 individually configurable
8.	Minimum Illumination	Colour: 0.1 lux, B/W: 0.01 lux (at 30 IRE)
9.	IR Cut Filter	Automatically Removable IR-cut filter
10.	Day/Night Mode	Colour, Mono, Auto
11.	S/N Ratio	≥ 50 dB
12.	Auto adjustment + Remote Control of Image settings	Colour, brightness, sharpness, contrast, white balance, exposure control, backlight compensation, Gain Control, Auto back focus
13.	Wide Dynamic Range	True WDR upto 100 db
14.	IR Illuminator	Internal /External IR illuminator with minimum 50 Mtr range
15.	Audio	Full duplex, line in and line out, G.711, G.726
16.	Local storage	microSDXC up to 64GB (Class 10) In the event of failure of connectivity to the central server the camera shall record video locally on the SD card automatically. After the connectivity is restored these recordings shall be automatically merged with the server recording such that no manual intervention is required to transfer the SD card based recordings to server.
17.	Protocol	HTTP, HTTPS, FTP, RTSP, RTP, TCP, UDP, RTCP, DHCP, ONVIF Profile S & G
18.	Security	Password Protection, IP Address filtering, User Access Log, HTTPS encryption
19.	Intelligent Video	Motion Detection & Tampering alert

#	Parameter	Minimum Specifications or better
20.	Alarm I/O	Minimum 1 Input & Output contact for 3 <sup>rd</sup> part interface
21.	Operating conditions	0 to 50°C
22.	Casing	NEMA 4X / IP-66 rated & IK 10
23.	Certification	UL2802 / EN, CE ,FCC
24.	Power	802.3af PoE (Class 0) and 12VDC/24AC

# At few places 2.8mm – 11 mm lens would be required depending upon the location of the camera and area to be covered. 2.8mm – 11mm lens requirement can be assumed as 20%. However the actual type of lens required would depend upon the field-specific user requirement & percentages may vary to some extent.

#### 5.5.1.12.10 Pan, Tilt and Zoom cameras (PTZ)

#	Parameters	Minimum Specifications or better
1.	Video Compression	H.264
2.	Video Resolution	1920 X 1080
3.	Frame rate	Min. 25 fps
4.	Image Sensor	1/3" OR 1/4" Progressive Scan CCD / CMOS
5.	Lens	Auto-focus, 4.3 – 129 mm (corresponding to 30 X
6.	Multiple Streams	Dual streaming with 2 <sup>nd</sup> stream at minimum 720P at 30fps at H.264 individually configurable
7.	Minimum Illumination	Colour: 0.05 lux, B/W: 0.01 lux (at 30 IRE, F 1.2) or better
8.	Day/Night Mode	Colour, Mono, Auto
9.	Wide Dynamic Range	True WDR upto 100 db
10.	S/N Ratio	≥ 50dB
11.	PTZ	Pan: 360° endless/continuous, 0.2 to 300°/s (auto), 0.2 to 100°/s (Manual) Tilt: 90°, 0.2 to 100°/s (Auto), 0.2 to 40°/s (Manual) 30 optical zoom and 10x digital zoom Pre-set tour 256 preset positions, Tour recording, Guard tour
12.	Auto adjustment + Remote Control of	Colour, brightness, sharpness, contrast, white balance, exposure control, backlight compensation, Gain Control, ,

#	Parameters	Minimum Specifications or better
	Image settings	Electronic Image Stabilization
13.	Protocol	HTTP, HTTPS, FTP, RTSP, RTP, TCP, UDP, RTCP, DHCP, ONVIF Profile S & G
14.	Security	Password Protection, IP Address filtering, User Access Log, HTTPS encryption
15.	IR Illuminator	Inbuilt IR illuminator with minimum 120 Mtr range
16.	Local Storage	microSDXC up to 64GB (Class 10) In the event of failure of connectivity to the central server the camera shall record video locally on the SD card automatically. After the connectivity is restored these recordings shall be automatically merged with the server recording such that no manual intervention is required to transfer the SD card based recordings to server.
17.	Intelligent Video	Motion Detection & Tampering alert
18.	Alarm I/O	Minimum 1 Input & Output contact for 3 <sup>rd</sup> part interface
19.	Operating conditions	0 to 50°C
20.	Casing	NEMA 4X / IP-66 rated & IK10
21.	Power	802.3at PoE+ (Class 4) or 24VDC/24AC
22.	Certification	UL2802 / EN, CE ,FCC

#### 5.5.1.12.11 Industrial Grade outdoor PoE switches

#	Parameter	Minimum Specifications
1.	Type	Managed Outdoor switch
2.	Ports	<ul style="list-style-type: none"> <li>• Minimum 4 10/100 TX PoE</li> <li>• May require higher port density at some locations, depending upon site conditions</li> <li>• May require fiber ports at some locations, depending upon site conditions/distances.</li> </ul>
3.	PoE Standard	IEEE 802.3af or better
4.	Protocols	<ul style="list-style-type: none"> <li>• Support 802.1Q VLAN</li> <li>• DHCP support</li> <li>• SNMP Management</li> </ul>
5.	Access Control	<ul style="list-style-type: none"> <li>• Support port security</li> </ul>

#	Parameter	Minimum Specifications
		<ul style="list-style-type: none"> <li>Support 802.1x (Port based network access control).</li> <li>Support for MAC filtering.</li> </ul>
6.	PoE Power per port	Sufficient to operate the CCTV cameras connected
7.	Rating	IP 30 or equivalent Industrial Grade Rating (This is not essential if the switch is placed in equivalent or better junction box / enclosure)
8.	Operating Temperature	0 – 50 degrees C or better

#### 5.5.1.12.12 Face Recognition System

Face Recognition System (FRS) shall be designed for identifying or verifying a person from various kinds of photo inputs from digital image file to video source. The system shall offer logical algorithms and user-friendly, simple graphical user interface making it easy to perform the facial matching.

The system shall be able to broadly match a suspect/criminal photograph with database created using photograph images available with Passport, CCTNS, and Prisons, State or National Automated Fingerprint Identification System or any other image database available with police/other entity.

The system shall be able to:

- i. Capture face images from CCTV feed and generate alerts if a blacklist match is found.
- ii. Search photographs from the database matching suspect features.
- iii. Match suspected criminal face from pre-recorded video feeds obtained from CCTVs deployed in various critical identified locations, or with the video feeds received from private or other public organization's video feeds.
- iv. Add photographs obtained from newspapers, raids, sent by people, sketches etc. to the criminal's repository tagged for sex, age, scars, tattoos, etc. for future searches.
- v. Investigate to check the identity of individuals upon receiving such requests from.

vi. Enable Handheld mobile with app to capture a face on the field and get the matching result from the backend server.

The facial recognition system shall be enabled at cameras identified by the Authority. These cameras identified shall be installed at critical locations finalized by authority

The facial recognition system in offline mode shall be provided by the SI in line with the requirement specified in the RFP.

The detailed functional requirement specification of the facial recognition system is provided in subsequent sections of this RFP.

**5.5.1.12.12.1 Face Image Data Standard**

Manual Facial recognition is not sufficient currently for de-duplication. . Computer based face recognition has reasonable accuracy under controlled conditions only. Hence for de-duplication purposes, other biometrics like finger print/iris image is also recommended.

With the objective of interoperability among various e-Governance applications, the face image data standard for Indian e-Governance Applications will adopt **ISO /IEC 19794-5:2005(E)**. While the ISO standard is broad to cover all possible applications of computer based face recognition and human visual inspection, this standard is more restrictive, as it is limited to human visual inspection.

The ISO standard specifications are tailored to meet specific needs of civilian e-Governance applications by specifying certain prescriptive values and best practices suitable in Indian context.

Standard	Description
ISO /IEC 19794-5:2005(E)	<p>This standard includes capture and storage specifications of face images for human visual inspection and verification of the individuals in Indian E-Governance applications.</p> <p>It specifies a format to store face image data within a biometric data record compliant to the Common Biometric Exchange Formats Framework (CBEFF), given in ISO 19785-1. It also includes best practices recommended for implementation of the specifications in different categories of e-Governance applications.</p> <p>The scope of this standard includes:</p> <ul style="list-style-type: none"> <li>o Characteristics of Face Image capturing device</li> <li>o Specifications of Digital Face Image &amp; Face Photograph Specifications intended only for human visual inspection and verification</li> </ul>



	<ul style="list-style-type: none"> <li>○ Scene requirements of the face images, keeping in view a future possibility of computer based face recognition</li> <li>○ Face Record Format for storing, archiving, and transmitting the information of face image within a CBEFF header data structure for the purpose of interoperability and usage in future for computer based face recognition.</li> </ul>
--	---

**5.5.1.12.13 Junction Box**

#	Parameter	Minimum Specifications
1.	Size	Suitable size as per site requirements to house the field equipment
2.	Cabinet Material	Powder coated CRCA sheet/ Stainless steel
3.	Material Thickness	Min 1.2 mm
4.	Number of Locks	Two
5.	Protection	IP 55/ NEMA 4X
6.	Mounting	On Camera pole / Ground Mounted on concrete base
7.	Form Factor	Rack mount/ Din Rail
8.	Other Features	Rain Canopy, Cable entry with glands and Fans/ any other accessories as required for operation of equipment's within junction box


**5.5.1.12.14 Field UPS**




#	Parameter	Minimum Specifications
9.	Capacity	1 KVA
10.	Input Range	Voltage Range 155-280 V on Full Load Voltage Range 110-280 V on Less than 70% Load Frequency 50 HZ ±3 HZ
11.	Output Voltage & Waveform	220V AC/ 230V AC/ 240V AC (Selectable)
12.	I/P & O/P Power Factor	0.9 or higher power factor
13.	Mains & Battery	Sealed Lead Maintenance Free VRLA type (Lead Calcium SMF batteries NOT acceptable), Mains & Battery with necessary

#	Parameter	Minimum Specifications
		indicators, alarms and protection with proper battery storage stand
14.	Frequency	50 Hz +/- 0.5% (free running), Pure Sine wave
15.	Crest Factor	min. 3:1
16.	Third Harmonic Distribution	< 3%
17.	Input Harmonic Level	< 10%
18.	Overall Efficiency	Min. 90% on Full Load;
19.	Noise Level	< 55 dB @ 1 Meter
20.	Backup	at least 60 minutes (1 hours / VAH)
21.	Warranty	5 years with UPS & battery
22.	Certification	ISO 9001:2008 & ISO 14001 certified
23.	Protection	To be provided for overload/ short circuit; overheating; input over/under voltage; output over/ under voltage.
24.	Alarms & Indications	All necessary alarms & indications essential for performance monitoring of UPS like mains fail, low battery & fault detection
25.	Interface	SNMP interface support (for remote monitoring)
26.	Galvanic Isolation	To be provided through Inbuilt transformer
27.	Compatibility	UPS to be compatible with DG Set supply and mains supply
28.	Bypass	Automatic Bypass Switch
29.	Technology	True ON-LINE (Double Conversion) with IGBT based inverter and PWM Technology
30.	Support	The system should not be an end of life / end of service product
31.	Operating Temperature	0 to 55 Degrees Centigrade

**5.5.1.12.15 Camera Poles**

#	Parameter	Minimum Specifications
1.	Pole type	Hot Dip Galvanized after Fabrication with Silver coating of 86 micron as per IS:2629; Fabrication in accordance with IS-2713 (1980)
2.	Height	<ul style="list-style-type: none"> <li>• 5 Meter OR higher, As-per-requirements for different types of cameras &amp; Site conditions.</li> <li>• Min. height of camera above the ground should be 10 feet</li> </ul>
3.	Pole Diameter	Min. 10 cm diameter pole (bidder to choose larger diameter for higher height)
4.	Bottom base plate	Minimum base plate of size 30 x 30 x 15 cms
5.	Mounting facilities	To mount CCTV cameras, Switch, etc.
6.	Foundation	<p>Casting of Civil Foundation with foundation bolts, to ensure vibration free erection (basic aim is to ensure that video feed quality is not impacted due to winds in different climatic conditions). Expected foundation depth of min. 100cms.</p> <p>Please refer to Earthing standards mentioned in Section 8.4 (pt. 4)</p>
7.	Protection	Lightning arrestors with proper grounding
8.	Sign-Board and Number-Plate	A sign board describing words such as "This area under surveillance" and with serial number of the pole.

Type	Sign Design	Remarks
A		To be used at 80% of the Places

Type	Sign Design	Remarks
B		<p>To be used at select places where text can be read. Text should be in Tamil at majority of places</p>
C		<p>This may be used on a select few places in the city, usually on the main pole of the location where multiple cameras are installed. Text should be in Tamil in majority of places.</p>
D		<p>This is an alternative to type C.</p>

### 5.5.2 Smart solutions with Artificial Intelligence at Edge Devices:

Along with the components of the CCTV Surveillance system, the SI would be responsible to integrate the following services with the CCTV Surveillance system to build an infrastructure for a Smart city system in the Chennai Area having the functional requirement to be cater through Artificial Intelligence at edge devices with continuous and deep learning capabilities for real time response and monitoring.

These use cases are to be implemented using Artificial Intelligence through various cameras, sensors etc at the edge/field devices with continuous learning capabilities, Following use cases are to be part of implementation but not limited to:

- Graffiti and Vandalism detection
- Debris and Garbage detection
- Attendance of sanitation workers on site by face recognition
- Sweeping and cleaning of streets/bins before and after
- Garbage bin, cleaned or not
- Litter detection
- Tracking of garbage truck movement and Quantity of garbage dumped at dumpsite
- Detection and Recognize the pattern of demonstration and conflicts in crowd
- Detection and classification of human, animal and vehicle
- Safety: Detection and classification based on :
  - Behavioural Biometry : Identification through multiple behaviour
  - Parking violation
  - Speeding vehicle
  - Accident detection
  - Loitering detection
  - Person climbing barricade
  - Person collapsing
  - Person/Face recognition
  - Gesture recognition : Identification through gesture change
- 'Vehicle of interest' tracking by colour, speed, number plate
- Helmet detection on two wheeler
- Unwanted/ banned vehicle detection
- Wrong way or illegal turn detection
- Toilet cleaning by detection of smell etc
- Water quality sensors at District Metered Area level
- Environmental condition detection
- Air quality detection

Edge based Analytics min specification for functional delivery:

- Deliver 5.5 teraFLOPS of FP16 performance or better
- Support Wi-Fi, Bluetooth, 3G/LTE connectivity options
- Have 100Mb/1GbE management network link
- Support 1GbE (via RJ45) or 10GbE (SFP+)

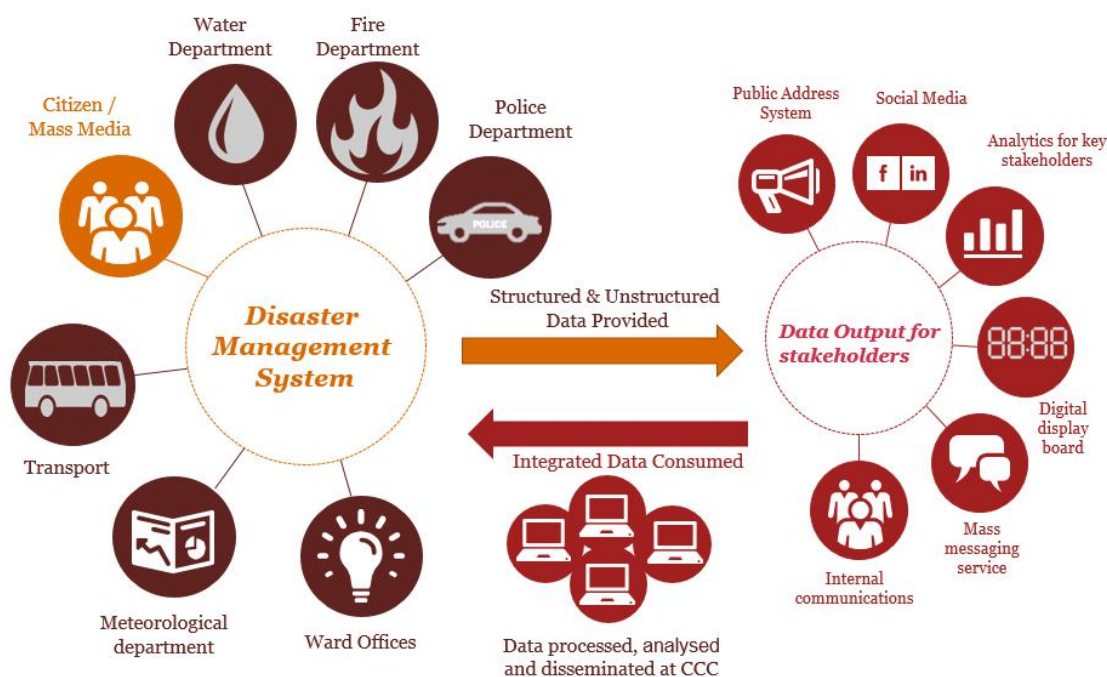
- Have operating temperature range of 0 degrees to 55 degrees to withstand outdoor operating environment and as per city conditions

Artificial Intelligence with Continuous Learning & Improvement system Specification:

- Deliver processing units' performance of 1 petaFLOPS on FP16 or better
- Have software tools for achieving the following tasks- Resource allocation, queueing of jobs, performance monitoring and creating software containers
- Support commonly used Deep Learning based AI frameworks like TensorFlow, CNTK etc.
- Have minimum 512GB system memory per system or better
- Have dual 10GbE and 4 IB EDR per system or better
- Min power consumption per system.
- Have dual 20-core Intel Xeon E5-2698 or better per system.
- At least Support parallel computing architecture.
- Support software libraries for continuous learning and improvement for betterment of Intelligent video analytics software installed in edge/field devices using Deep Learning based AI methodologies.

### 5.5.3 Disaster Management System

Disaster Management system is majorly required during Tsunami, Flood, Cyclone and Earthquake time.



- 1) Disaster Management system shall be integrated with the following system/ components/ Department;
  - a. Flood Sensors
  - b. Rainfall and Air Quality Sensors
  - c. Social Media
  - d. IMD, INCIOS department etc.
  - e. Ambulance, Hospital, Police, Traffic, GCC, Disaster Management Department and Fire department
  - f. Asset Management and Dispatch management system
  - g. ECB, PAS and the communication system (SAT phone/Radio) of the police department.
  - h. GIS

- i. All communications PA, radio, telephony to be recorded using enterprise logging solution and to be made available to the CCC operator for debriefing requirements.
- 2) The Disaster Management system shall be integrated with the GIS which will be mapped with the nearest shelter location
- 3) Sample Use Cases describing the need of integrated systems, however the authority will ask the SI to add more SOPs and use cases on need basis. SI has to do the needful support and arrangement at no additional cost:
  - *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 CCC through the available connectivity. The CCC 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 centers in the vicinity to prepare for increased number of emergency care patients.
  - Integration of **Building Management System** (BMS) database of buildings in the Area Based Development (ABD) areas to be envisaged at the CCC platform. The control system becomes critical for every building particularly places with higher population density (floating /permanent). These details w.r.t any localized disaster such as fire, etc. which would be sensed by the BMS the details may be shared to the envisaged so that Emergency Standard Operating Procedure (SOP) may be commenced. This CCC based interface will also enable periodic monitoring of the feeds and incase of malfunctioning the same may be also course corrections. In-case the State Government decides to proactive measure they can also monitor health & availability status of such control systems built in the building.
  - *Tsunami, Cyclone and Earthquake Scenario:* The Disaster Management System shall be integrated with the IMD and INCOIS for getting the alerts with respect to the change in the sea tide, wind speed at the CCC through the available connectivity. As soon as the CCC receives the emergency alert it shall trigger the variable messaging displays and public address system to warn them of possible earthquake, flooding/ cyclone in a locality. Parallely it shall alert the police department and the hospital



## 5.6 Mobile Command Centers

Mobile vans would be used as and when the situation demands to capture the real-time video feed of an incident. These will be built on 4x4 rugged vehicles and will house communications equipment that may be required to stream video feeds to Command and Control Centers. It is proposed to deploy such vans in the city cross each zone. SI shall provide the required manpower for handling the cameras & associated equipment's in the vehicle on 24 / 7 basis. Ownership of vans would be with the Police Department. Detail operational guideline document shall be prepared during implementation phase, which shall specify detail responsibilities of these resources and their Do's & Don'ts for the personnel.

Mobile vans shall have the appropriate wireless and 3G/4G connectivity to connect to the nearest Command Control Centers through the Data Centers, local storage for storing at least 24-hour video feed for 4 cameras (7 days), local computing and processing capabilities & a seating capability for minimum four people.

Indicative list of the Bill of Material for each Pre-Fabricated Mobile Vans is as follows:

- 1 rugged Laptop with 18.5" Screen (for local viewing on multiple/rugged terrains meeting Mil/ENStandards)
- Wireless and 3G/4G Connectivity
- GPS Equipment to connect to the Vehicle Tracking System
- 1 Full HD mobile PTZ Camera with inbuilt IR illuminator; 2 Fixed Box Cameras with inbuilt IR illuminator (No. of cameras could be increased to 6 in future)
- Local Storage for all cameras of Mobile Van for 24 hours (Video storage from Mobile Vans also required to be stored on Primary storage for 7 days & on Secondary Storage for 23 days at Data Centers)
- 1 IP Phone
- Local Area Network connecting Cameras, Laptop, Storage, Wireless Base Station, IP Phone and Handheld Device
- 1 Video Full HD Handheld Camera with capability to stream videos through Wi-Fi / WiMAX
- Bidder to propose a Handheld camera meeting the common benchmark specifications specified for Fixed



Illustrative Picture of Mobile Command & Control Center

Please note that the mobile van component (including all the related components) is optional, and Police Department shall decide upon its inclusion or exclusion at a later date. Police Department's decision in this regard shall be final and binding upon the Successful Bidder.

Police Department would also want to setup viewing centers where video feeds from wireless CCTV cameras can be captured. These cameras shall transmit video feeds over Wi-Fi / 3G / 4G connectivity to the temporary viewing center in the Police vans. Viewing in these Police vans will be done over Laptops. The video feeds may be stored locally in the Police van and if necessary, later archived for investigation purposes.

**5.6.1 Vehicle Top Mounted Fixed Camera**

#	Parameters	Minimum Specifications or better
1.	Video Compression	H.264
2.	Video Resolution	1920 X 1080
3.	Frame rate	Min. 25 fps
4.	Image Sensor	1/3" Progressive Scan CCD / CMOS

#	Parameters	Minimum Specifications or better
5.	Lens Type	Varifocal, C/CS Mount, IR Correction
6.	Lens#	Auto IRIS 8 – 40 mm, F1.4
7.	Minimum Illumination	Colour: 0.5 lux, B/W: 0.1 lux (at 30 IRE)
8.	IR Illuminator	Inbuilt IR Illuminator with minimum 50 mtr range
9.	IR Cut Filter	Automatically Removable IR-cut filter
10.	Day/Night Mode	Colour, Mono, Auto
11.	S/N Ratio	≥ 50 Db
12.	Auto adjustment + Remote Control of Image settings	Colour, brightness, sharpness, contrast, white balance, exposure control, backlight compensation, Gain Control, Wide Dynamic Range
13.	Audio	Audio Capture Capability
14.	Local storage	Memory card slot availability
15.	Protocol	IPV4, IPV6, HTTP, HTTPS, FTP, RTSP, RTP, TCP, UDP, RTCP, DHCP, UPnP, QoS
16.	Security	Password Protection, IP Address filtering, User Access Log, HTTPS encryption
17.	Operating conditions	0 to 50°C (temperature), 50 to 90% (humidity)
18.	Casing	NEMA 4X / IP-66 rated with vehicle mounted hardware*
19.	Certification	UL/EN, CE,FCC

### 5.6.2 Vehicle Top Mounted PTZ Camera

#	Parameters	Minimum Specifications or better
1.	Video Compression	H.264
2.	Video Resolution	1920 X 1080
3.	Frame rate	Min. 25 fps
4.	Image Sensor	1/3" Progressive Scan CMOS
5.	Lens	Auto-focus, 4.7 - 94 mm (corresponding to 20x)
6.	Minimum Illumination	Colour: 0.5 lux, B/W: 0.1 lux (at 30 IRE)

#	Parameters	Minimum Specifications or better
7.	IR Illuminator	Inbuilt IR illuminator with minimum 120 mtr range
8.	Day/Night Mode	Colour, Mono, Auto
9.	S/N Ratio	≥ 50Db
10.	PTZ	Pan: 360° endless/continuous, 0.2 to 300°/s (auto), 0.2 to 100°/s (Manual) Tilt: 90°, 0.2 to 100°/s (Auto), 0.2 to 40°/s (Manual) 20x optical zoom and 10x digital zoom 64 preset positions Auto-Tracking Pre-set tour
11.	Auto adjustment + Remote Control of Image settings	Colour, brightness, sharpness, contrast, white balance, exposure control, backlight compensation, Gain Control, Wide Dynamic Range
12.	Protocol	HTTP, HTTPS, FTP, RTSP, RTP, TCP, UDP, RTCP, DHCP, UPnP, QoS, IPV4, IPV6
13.	Security	Password Protection, IP Address filtering, User Access Log, HTTPS encryption
14.	Operating conditions	0 to 50°C (temperature), 50-90% humidity
15.	Casing	NEMA 4X / IP-66 rated with vehicle mounted hardware
16.	Certification	UL/EN,CE,FCC

### 5.6.3 In-Vehicle Fixed Camera

#	Parameters	Minimum Specifications or better
1.	Image Sensor	1/3" 2 Megapixel CCD/CMOS with dual stream
2.	Effective Pixels	1920(H)x1080(V)
3.	Scanning System	Progressive with Multiple Simultaneous Streaming
4.	Electronic Shutter Speed	Auto/Manual 1/3~1/10000
5.	Min. Illumination	Color: 0.2 Lux / F1.6, B/W: 0.01 Lux/F1.6.
6.	S/N Ratio	>50dB
7.	Day/Night	Auto(Electronic)/Color/B/W
8.	Backlight Compensation	BLC / HLC / DWDR

#	Parameters	Minimum Specifications or better	
9.	White Balance	Auto	
10.	Gain Control	Auto/Manual	
11.	Noise Reduction	Noise reduction technology for vehicular use	
12.	Local Storage	Minimum 64 GB SD Card	
13.	Focal Length	As per solutions offered.	
14.	Focus Control	Fixed lens	
15.	Mount Type	Board-in Type	
16.	Compression	H.264 / MJPEG	
17.	Resolution	1080P (1920x1080) / 720P (1280x720)/ D1(704x576) / CIF(352x288)	
18.	Frame Rate	Main Stream	1080P / 720P (1 ~ 25/30fps)
19.		Sub Stream	720p (1 ~ 25/30 fps) and below
20.	Bit Rate	H.264: 32K ~ 8192Kbps, MJPEG: 32K ~ 20480Kbps	
21.	Ethernet	RJ-45 (10/100Base-T)	
22.	Protocol	IPv4/IPv6, HTTP, HTTPS, SSL, TCP/IP, UDP, UPnP, ICMP, IGMP, SNMP, RTSP, RTP, NTP, DHCP, DNS, DDNS, IP Filter, QoS	
23.	ONVIF	ONVIF Ver. 2.0	
24.	Max. User Access	More than 10 users	
25.	Power Supply	DC 12V, PoE (802.3af)	
26.	Working Environment	-10°C ~ +60°C, 10% ~ 90%	
27.	Certification	UL/EN,CE,FCC	

#### 5.6.4 NVR for Vehicle Mounted cameras

#	Parameters	Minimum Specifications or better
1.	Channels / Ports	1080p/720p 8-Ch / Port built-in NVR-cum-Switch with Active alert mechanism

#	Parameters	Minimum Specifications or better
2.	Input	Min 8 channel IP camera inputs
3.	Output	1 channel
4.	Support for Two-way Talk	1 channel Input, 1 channel Output
5.	OSD	Camera title, Time, Video loss, Camera lock, Motion detection, Recording
6.	Video/Audio Compression	H.264 / MJPEG / PCM
7.	Resolution	1080P (1920×1080) / 720P(1280×720) / D1 (704×576 / 704×480)
8.	Record Rate	as per solutions offered
9.	Bit Rate	48~8192Kb/s
10.	Record Mode	Manual, Schedule(Regular(Continuous), MD, Alarm), Stop
11.	Record Interval	1~120 min (default: 60 min), Pre-record: 1~30 sec, Post-record: 10~300 sec
12.	Search Mode	Time/Date, Alarm, MD & Exact search (accurate to second), Smart search
13.	Playback Functions	Play, Pause, Stop, Rewind, Fast play, Slow play, Next file, Previous file, Next camera, Previous camera, Full screen, Repeat, Shuffle, Backup selection, Digital zoom
14.	Ethernet	RJ-45 port (10/100/1000M)
15.	Wireless Network	3G, 4G and Wi-Fi module option
16.	Network Functions	TCP/IP, UDP, DHCP, DNS, IP Filter, PPPOE, DDNS, FTP, Email, Alarm Server
17.	Access	For all users of the mobile van
18.	Smart Phone	Deleted
19.	Internal HDD	Minimum 2 with at least 2 extended slots
20.	USB	Minimum 1 port
21.	RS232	Deleted
22.	RS485	Deleted
23.	Working Environment	0°C to 50°C/ 0% to 90% RH

#	Parameters	Minimum Specifications or better
24.	Certification	UL/EN, CE, FCC, EN 50155/6137 or equivalent, Rugged for vehicular/mobile use.

### 5.6.5 Mobile Vans & Related Equipment's

#	Parameter	Minimum Specifications or better
1.	Mobile Van	<ul style="list-style-type: none"> <li>· 4 x 4 Vehicle</li> <li>· Cushioned seats for 5 personnel plus driver &amp; co-driver</li> <li>· Siren unit and revolving light on body roof</li> <li>· 350W LED Light</li> <li>· Observation hatch</li> <li>· Mobility : High</li> <li>· Gradeability : 20°</li> <li>· Maximum Speed : at least 100 kmph</li> <li>· Ground Clearance: 175mm or better.</li> <li>· The vehicle should be pre-fabricated with fitments for all IT equipment, and racks required.</li> </ul>
2.	Camera Lift Unit for Vehicle Mounted Cameras	<p>Bidder should provide the standard design that is suitable for the vehicle to fix the cameras to get the desired results. The standard design off-shelf is preferred and the priority is given to such design.</p> <p>Bidder should showcase the demo with the suggested unit to meet the objective of no vibration and shock requirements as defined in this document.</p>
3.	Equipment / Item Standards for Vehicle Mounted Cameras	<p><b>Any equipment / Items supplied should meet the following standards:</b></p> <ul style="list-style-type: none"> <li>· IP66; EN-50155 / 61373, IEC-60571, or equivalent</li> <li>· CE, FCC, RoHS Certified; ONVIF Profile S Compliant; vandal proof</li> <li>· ARI/JASo DO 609-75AN for cabling standards</li> <li>· AIS 052 Standard for Cable for UPS charging</li> </ul>

## 5.7 Smart Pole

### 5.7.1 Specifications

#.	Specifications
1.	Smart pole should able to meet city aesthetic requirement and it should be visually appealing. It should easily blend-in into city street pole master plan.
2.	Should be able to support 1 light arm with maximum height requirement up-to 30 meter.
3.	It should be possible to house minimum 3-4 telecom technologies (GSM, WCDMA, LTE and Wi-Fi etc.) simultaneously.
4.	Site passive infra (space and power) sharing among telecom operators is mandatory requirement.
5.	It should be possible to support LED luminaries from reputed OEMs
6.	Smart Pole shall adhere to the standards for poles (wind speed, climate, aesthetics etc.) and policies governing the Authority or as mandated by regulatory authority of Government of India and Tamilnadu.
7.	It should be possible to support connectivity for Smart pole
8.	The maximum allowed diameter (at bottom section) is 250mm
9.	All cabling, cooling/heating etc. should be via/inside the pole and it should not be visible from outside due to aesthetic and security reasons
10.	It should meet EMC requirement of telecom sites as per Indian regulations
11.	The minimum power backup requirement is minimum 2 hrs. for telecom equipment
12.	It should be possible to provide multiple color options as asked by municipality/user as per city light pole colors
13.	It should be possible to house radio units with integrated antenna, MW /optical transmission unit, SMPS (AC to DC convertor), batteries, controllers, power distribution etc. inside the smart pole
14.	It should be possible to house telecom equipment's from all reputed OEMs.
15.	It should be possible to provide light connection in daisy chain with separate MCB for lighting and telecom part
16.	There should be provision to have separate connection for light as well for telecom equipment for maintenance purpose.
17.	The paint material (to cover the RF section) should complied to RF/Telecom requirements
18.	It should be possible to color the complete body (including RF equipment camouflaging) by any paint color
19.	The camouflaging material (to cover RF equipment's) should have RF transparency with maximum 0.5db of attenuation covering all the radio frequency bands available in India



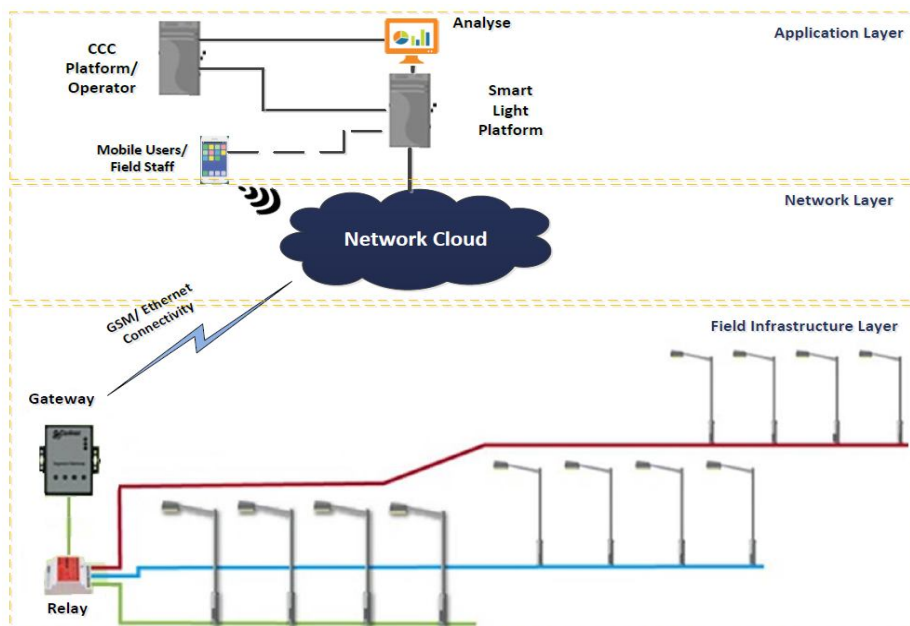
#.	Specifications
20.	The cooling/heating equipment's to cool /heat telecom equipment should be integral part of smart pole. Maximum allowable limit for cooling equipment is 100W for cooling solution, efforts should be made to reduce the power consumption as much as possible.
21.	The smart pole structure should be IP67 up-to 1 meter height from reference ground level.
22.	There should be suitable mounting options for Radio /Antenna unit mounting
23.	The ambient temperature requirement is 0-50 deg
24.	The overall power budget for smart pole should not exceed 2KW (telecom + lights)
25.	It should be possible to support 2 light arm option by smart pole
26.	Underground space should be used for telecom equipment's with suitable telecom grade enclosure box
27.	The minimum life requirement of above smart pole structure is 17 years (metal parts)
28.	The System Integrator should not use any banned /restricted material as per Indian regulations
29.	Pole hat mounting should have suitable option for GPS antenna, small MW antenna
30.	The smart pole should support Environmental sensors

## 5.7.2 LED based Smart Street light

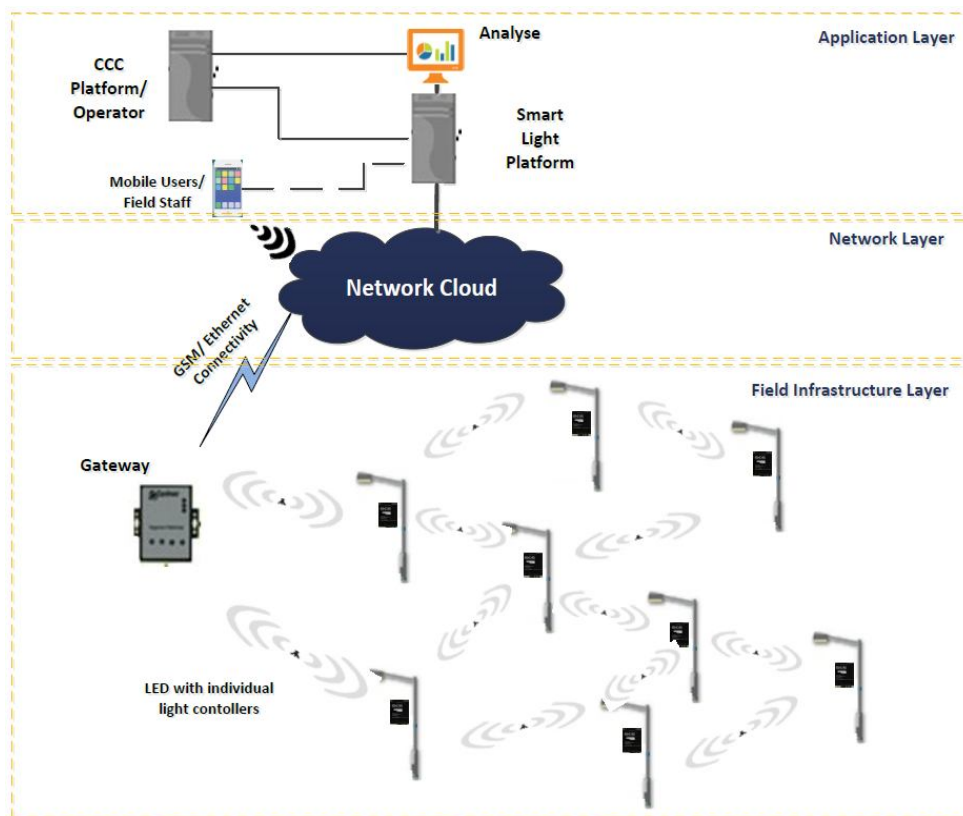
National Lighting Code by Bureau of Indian Standards (IS)- SP 72, 2010, IS 1944, IS 1977 and IEC Standards shall be complied for design and development of street lighting calculations, selection of lighting fixtures, lighting technologies, pole structure & erection, cable selection and sizing, insulation requirements, conductor specifications etc.

### 5.7.2.1 Solution Architecture

#### 5.7.2.2 Smart light with feeder panel



#### 5.7.2.3 Smart light with Individual light controllers



### 5.7.2.4 Specifications

The scope includes design, development, manufacturing, testing and supply of energy efficient luminaire complete with all accessories, LED lamps with suitable current control driver circuit including mounting bracket for street light and High mast light. The luminaire shall be suitable for rugged service under the operational and environmental conditions encountered during service.

### 5.7.2.5 Smart Street Light Solution

#	Specifications
1.	The smart street lighting system should be able to operate in any weather conditions
2.	Smart street lighting system should be able to communicate to the feeder panel.
3.	The smart street lighting system should be able to communicate to the Lighting Operations Management software hosted on the datacentre
4.	The smart street lighting system should have the capability to receive the instruction from the Lighting Operations Management software and act accordingly
5.	The smart street lighting system should be able to operate the lights switch on/off, increase/decrease luminosity (Dimming) as per the command received from the

#	Specifications
	Lighting Operations Management software. This control of smart street lights should also be available through a mobile App ( compatible with iOS, Android)
6.	The software should have the capability to apply policies to the smart lighting system. Example: set up policies like light up alternate lights during low traffic density, increase the luminosity of the lights as per the dullness of the daylight, scheduling of light functioning etc.
7.	The city administration should be able to see the real time status of the Smart Lighting System on a city map view of the Lighting Operations Management software
8.	The city administration should be able to operate the Smart Lighting System manually too.
9.	The smart lighting system should be able to communicate the system issue or failure to the Lighting Operations Management software.
10.	The smart lighting system are preferably a combination of LED lights
11.	Should enable Over the Air (OTA) firmware update

#### 5.7.2.6 LED Luminaire

#	Minimum Specifications
1.	High bright white power LEDs shall be used in the Luminaries and the wattage of these LEDs shall be >1W and <3W.
2.	Life span of LEDs used in the Luminaire shall be more than 50,000 hours at 70% light output.( Manufacture shall submit the proof-L70& TM 21 test report)
3.	Color rendering index (CRI) of the LEDs used in the luminaire shall be greater than 70.
4.	Color temperature of the proposed white color LED shall be 5000K-6500K
5.	Junction Temperature; Should be less than value at which LM80 (IS16105) data published. Should be >105 Degree C
6.	The distribution of luminaire illumination ( control of distribution) shall be based on type of roads as per BIS standard IS 1944
7.	Power Factor: 0.95
8.	Chip Efficacy: Shall be 135 lumen/watt, system lumen output at 25 degree C, supported by LM80 report shall be submitted.
9.	CRI of Luminaries: >=70 ( supported by LM80)
10.	Light Uniformity ratio ( Emin / Eavg) shall be as IS 1944 based on category of road
11.	The luminaire light output (lumen) shall be constant. The voltage variations/ fluctuations in the specified voltage range shall not impinge upon the lumen it produce maximum +/-2% is allowed throughout in the input operating voltage range

#	Minimum Specifications
12.	Operating voltage: 120 V to 270 V universal electronic driver with surge protection of 6 KV (Application IS 15885, Driver safety 16104-1/2)
13.	Total Harmonic Distortion: <10% THD Test method IEC:610003-2
14.	LEDs shall be operated at a current less than 90% of its rated current
15.	LED driver efficiency: >=350ma<=1000mA
16.	LED driver efficiency Driver (High Voltage, Low current): >85%
17.	Luminaire body temperature should not exceed 30 deg C from ambient (45 deg C) without tolerance of 10 deg. C after 24 Hrs.
18.	Heat dissipation/heat sink: Well-designed thermal management system with defined heat sink
19.	Input Current< 1000mA
20.	Should have Open Circuit protection
21.	The Luminaire shall be equipped with distortion free, clear, heat resistant, toughened, UV stabilized glass cover in the front fixed to the die cast. Aluminum frame which shall be fixed to the housing by means of stainless steel screw.
22.	The Luminaire shall be built in such a way it can withstand wind speed of 80Kmps
23.	Cover/glass without lens or with lens: Fixture cover-UV stabilized Polycarbonate/heat resistance toughened glass or equivalent will be accepted for the Luminaire without lens. For the Luminaire with lens, toughened glass be required with proper IP66 provision
24.	Frequency: 50 Hz+/-3%
25.	Operating temperature: Range -10C to +50 C
26.	Protections: IP66 for all wattage, Surge protection 6 KV, IEC61000-4-5
27.	Working humidity: 10% to 90% RH
28.	Conformation standards of Luminaire: The Luminaire should conform to IEC 60598/IS: 10322. The Luminaire should be tested as per IEC 60598-2-3:2002/IS: 10322 Part 5 sec-3 standards and following test reports should be submitted. Heat resistance test, thermal test, Ingress protection test, drop test electrical/insulation resistance test, endurance test, humidity test, photometry test (LM80 report) vibrant test.
29.	Finish: Aesthetically designed housing with corrosion resistant polyester powder coating

#	Minimum Specifications
30.	Luminaire configuration/technical requirement: Side entry type. Shall consist of separate optical and color gear compartments. It should be easy replacement in the field condition
31.	Compliance: RoHS/CE/ERTL/ERDI
32.	Surge protection: External surge protection of 10 KV to be separately installed with the each fixture
33.	Lamp starting time: Max 10 sec
34.	Overall system efficacy: >85%

#### 5.7.2.7 Feeder Panels

The System Integrator shall replace the feeder panel in non-working conditions as per the below mentioned specifications. System Integrator shall upgrade the feeder panels in working conditions (like remote transfer of data) with the below mentioned functionality.

The design and operation of feeder panels shall comply with SP 72 Part 8 of National Lighting Code 2010.

#	Specifications
1.	Principle equipment should be designed on the basis of 'Lossless Series Reactance with Secondary Compensation' technology (Auto-transformer)
2.	The efficiency of such principle equipment should not be less than 99.4% between 50% - 110% of loading
3.	Other than basic switching components, no other moving parts are allowed to be installed in the feeder panel
4.	240 VAC 50 Hz Single Phase Two Wire / 415 VAC 50 Hz Three Phase Four Wire Input
5.	Three Taps of Single / Three Phase Four Wire Outputs
6.	Standard Output Taps in each Phase at 200/205/210 VAC @ 240 VAC Nominal Input
7.	Feeder panels should have GPRS/GSM based remote streetlight monitoring system with capacity for self-protection from short-circuit, over voltage and anti-theft alert
8.	The rating of the Streetlight controller should be at least 1.3 times the lighting load as measured during the initial studies
9.	Energy Meters to be installed in separately sealable and open able compartment within the Feeder Panels as per the following specifications: <ul style="list-style-type: none"> <li>• Energy Meters should have Accuracy class of Class 1 or better;</li> <li>• Meters could be either three phase whole current or CT operated for LT as may be required based on the load connected to the feeder panel. The space to be created in the feeder panel for housing the meters should consider the same.</li> <li>• Energy Meters should be capable of logging parameters for each 15 minute</li> </ul>

#	Specifications
	<p>time block with stamping of date and time. Such data logs should be retained in the energy meters for a period of 60 days or more.</p> <ul style="list-style-type: none"> <li>• Such Energy Meters should record the following minimum parameters</li> <li>• Phase to neutral voltages <ul style="list-style-type: none"> <li>○ Phase-wise current</li> <li>○ Phase-wise power factor and frequency</li> <li>○ Total active power</li> <li>○ Total reactive power</li> <li>○ Total active energy</li> <li>○ Total reactive energy</li> <li>○ Total KVAH energy</li> </ul> </li> <li>• Meters should have requisite port (Serial port communication – RS232 or RS485) for enabling remote reading and for connection of Modem for the same <ul style="list-style-type: none"> <li>○ Energy Meter specifications should meet the minimum specifications specified by TANGEDCO and a sign-off on the same shall be obtained from TANGEDCO prior to finalizing the specifications;</li> <li>○ Energy Meters shall be tested, installed and sealed in accordance with procedures specified by TANGEDCO;</li> <li>○ A signoff from TANGEDCO on the design and specifications of the compartment in the Feeder Panel where the meters are to be housed is also recommended;</li> </ul> </li> </ul>
10.	Bidder has to install appropriate power conditioning devices to protect the new EE technologies and components of feeder panels from damage. Poor power quality is not allowed as an excuse for non-functioning of the new technologies installed under the project
11.	Fixed capacitor with appropriate capacity shall be introduced in each feeder panel to always maintain a power factor above 0.90
12.	In case of Single phase controller unit, 1 pole contactor or multiple parallel pole contactors should be used and in case of 3 phases, appropriate duty 3 pole contactor should be used. The number of contactors used should be suitable for ON/OFF/Dimmed and for changeover between full voltages to various voltage taps and interchanging between taps. The panels should be equipped with a microprocessor based Dual Channel Almanac Timer controller which should be user programmable to enable setting of ON/OFF/Dimmed times and also switching over to savings mode/bypass mode when required
13.	<p>All the principle equipment's along with input output switchgears, metering, switches (bye pass and tap changers), contactors, fuses, auto transformer coils etc. should be of reputed manufacturers and should meet best engineering practices and norms as applicable in relevant standards;</p> <ul style="list-style-type: none"> <li>• Auto transformer coil should have full current operating efficiency of better than 99%</li> <li>• The total heat dissipation from single coil should not exceed 6 watts-sec/kVA</li> </ul>

#	Specifications
	<p>under fully loaded condition</p> <ul style="list-style-type: none"> <li>• The rated current of the auto transformer should be for continuous 120% that of input rated current</li> <li>• The switched fuse units should be of 32 Amp continuous AC current capacities.</li> <li>• Fuses used should be of 20 Amp. Rating of high rupturing capacity (S/c current at least 50 kA)</li> </ul>
14.	<p>The bidders should always ensure that the System is capable to capture live data and record it at variable time-intervals. Following parameters should be recorded for every 60-120 minutes time interval:</p> <ul style="list-style-type: none"> <li>• Voltages</li> <li>• Current</li> <li>• Power Factor</li> <li>• Active Power (kW)</li> <li>• Apparent Power (kVA)</li> <li>• Metering kWh cumulative</li> <li>• Metering kVAh cumulative</li> <li>• Number of hours the lamps were glowing</li> <li>• Special emergency on/off facility with wireless control.</li> <li>• Benchmarking capacity so as to generate alert SMS for: <ul style="list-style-type: none"> <li>○ Phase-wise currents on crossing threshold values</li> <li>○ Phase-wise voltages on crossing threshold values</li> <li>○ JSCLB trips</li> <li>○ Theft alerts</li> <li>○ Group failure of lights</li> <li>○ Contactor failure</li> <li>○ No output supply</li> </ul> </li> <li>• Alert SMS shall be forwarded to five (5) phone numbers.</li> <li>• GPRS/GSM modem should be used</li> </ul>
15.	<p>Enclosure Box of feeder panels shall be IP-56 compliant and should be fabricated out of MS sheet SWG 16 / 14 duly powder coated for corrosion resistance and long life.</p> <ul style="list-style-type: none"> <li>• It should have Single Phase power socket for connecting utility tools like drill machine etc. (capacity 1phase 240Vac / 5Amp socket)</li> <li>• Utility Service Lamp inside Panel for use during maintenance work</li> <li>• Gland Plates for Cable Entry at Incomer and Outgoing</li> <li>• Auto Bypass / Tap Changing in lieu of Manual. The tap changing should be automatic between the full voltage and lower voltage for minimum two numbers selected taps.</li> </ul>
16.	<p>The bidder shall have to get the control panels fabricated from the vendor having type test certificate from CPRI for 31 MVA short-circuit rating up to 400 amp for cubical panels. The copy of the type test certificate shall also have to be produced failing which feeder panels shall not be accepted</p>



#	Specifications
17.	Design life of the control panel should be mentioned in form of MTBF (mean time between failures) and it should be minimum 15 years

#### 5.7.2.8 LED Luminaire Controller

#	Specifications
1.	Advance 32 bit Microcontroller based design.
2.	Very easy key board operation
3.	HMI LCD display. 16 character and two line type display. Which help while maintenance and reduce dependability. Contentious Scrolling display of events (Like ON time, Off time, Dimt time, Voltage, Current, Staggering time , Alarm events, Burning hours, etc.) on Single HMI LCD display to help the local monitoring of systems. Parameters can be updated from local panel. Log the alarm of last 5 events
4.	Data Measurement for Monitoring and controlling Data monitoring through Class 1 type Multi – Function Panel mounted Energy meter : By using this to measure the individual phase voltage, individual phase load amps, PF, KW, KVA, KVAR, Phase to Phase voltage, Average PF, KWH etc. ( Local display of 36 and 28 for remote display in software)
5.	Auto / Manual facility by way of contactor / relay operation for faster service mode. From local panel in manual mode it shows individual line / channel current and show no of lamp which is not working which helps to judging the problem in line (by difference of calibration current and existing line current. Judgment is possible for approximately find out no of lamps are not working
6.	Street light ON / OFF / Dim on Longitude, Latitude base sunset and sunrise time generation not by any fixed time table
7.	Door Open information
8.	Real time clock with battery with life of more than 7 years (Manufacturer provided 10 years life for the battery with the accuracy of +/- 60 second per month. Power reserve of more than 60000 hours)
9.	System parameter data protection with special RAM, which hold the parameter for more than 10 years without any power
10.	Master and user Password Protection.
11.	Inbuilt auto recovery systems for power failure which helps in streetlight operation
12.	Double Inrush current capability of electrical switch gears to support sodium vapor lamp

#### 5.7.2.9 Centralized Management Software

#	Specifications
1.	Web Base Software replaces visual inspections of individual street lighting while sitting at workstation with Internet connectivity. Also by fault alarm and monitoring of data user can judge the fault status and severity of fault

#	Specifications
2.	Remote switching through Web Base Software to override local controller
3.	User can demand any time live status of feeder pillar for current electrical and real time parameters
4.	Emergency Stop / Manual ON / Manual OFF / Test Mode of feeder pillar
5.	User can monitor and change all settable parameter setting and clock time setting
6.	Control at any level of individual Street lights. Generate electrical profile of any individual feeder pillar
7.	Unit should be directly mapped on GIS Map
8.	The software shall receive the self-generated data message from individual Feeder Pillar like, ON time, Off time, Dim time, Power Down time, Auto mode / Manual Mode, Volt Fault, Over Current Fault, Short Circuit Fault, Neutral Fault, RTC Fault, ADC Fault, Memory Fault, Low Ampere Fault, Door Open, Relay Fault, Calibration Data and acknowledgement of message demand by WEB of Parameter writing, E Stop, Test Mode, E Profile. All these messages contain all electrical parameter with real-time clock date and time
9.	The software shall generate report of any date or any date range for fault and message of individual unit or all the units. The software shall also generate Range Report for fault, Message, Voltage graph, Current Graph, Streetlight On time, VA Consumption, etc.
10.	All the data collected by the software shall be exported to work sheet format for further analysis as per requirement. The system should be able to generate graph and reports as per requirements
11.	Can be operated and viewed from anywhere in the world
12.	System should be easily expanded and maintained. The system should have the capabilities for new configurations remotely.
13.	Web Interface should give instant status of the street lights on the dynamic Google map

#### 5.7.2.10 Minimum Illumination Level

#	Type of LED Luminaries	Vertical Distance from the floor level (Meters)	Minimum Illumination Level (Lux) centre	Color of Illumination
1.	45-50W	5	(12-15)	5000K-6500K
2.	100-105W	7	(15-18)	5000K-6500K
3.	140-170W	7	(18-20)	5000K-6500K
4.	260W	7	(20-22)	5000K-6500K

5.	50W	5	(12-15)	5000K-6500K
6.	105-110W	7	(15-18)	5000K-6500K
7.	190W	7	(20-22)	5000K-6500K
8.	25-30W	5	(10-12)	5000K-6500K
9.	60W	7	(15-18)	5000K-6500K

#### 5.7.2.11 Minimum desired illumination levels during peak hours

#	Type of LED Luminaries	Type of Road	Lamp mounting height from the floor level (Meters)	Minimum Illumination Level (Lux) centre	Color of Illumination
1.	250-260W		Above 18	(20-22)	5000K-6500K
2.	190W	A1	Between 11-15	(20-22)	5000K-6500K
3.	140-170W	A1	9-15	(18-20)	5000K-6500K
4.	90-120W	A2/B1	7-9-11	(15-18)	4300K-5600K
5.	70-120W	A2/B1	7-9-11	(15-18)	4300K-5600K
6.	70-120W	B1/B2	6-7-9	(15-18)	4300K-5600K
7.	70-50W	B1/B2/C1	7-9	(12-15)	4300K-5600K
8.	45-50W	B1/B2/C1	5-7	(12-15)	4300K-5600K
9.	25-30W	B1/B2/C1	5-7	(10-12)	4300K-5600K

- Variation in illumination level shall be  $\pm 2\%$  is allowed in input voltage range from 180VAC to 250VAC.
- The illumination shall not have infra-red and ultra-violet emission. The test certificate from the NABL approved laboratory shall be submitted.
- Electronic efficiency shall be more than 85%

#### 5.7.2.12 Conformance Standards

Product Certification should be obtained from UL or CPRI or any other NABL certified lab. The following test reports should be provided:

LM-79	Luminaire efficacy (Photometry data)
LM-80	LED chip data
IP 67	Luminaire Ingress Protection

Luminaire Endurance Test	Practical testing of luminaire through 20,000 cycles
EN 60929	Performance
IEC 60598-1	General requirement and tests
IEC 61000-3-2	Limits for Harmonic current emission - THD < 10%

### 5.7.3 Public Internet Access

#### 5.7.3.1 WLAN Controller

#	Parameter	Specifications
1.	Hardware	Redundancy Features: Controller must support Active: Active and Active: Standby. Same license should be shared by both the controller.
2.		WLC should be dedicated appliance with support for up to 100 Access points. Should be in High Availability mode. Should have 2 nos. of 100/1000/10Gig ports
3.	General Feature Requirements	Full web based real time NMS system to monitor services working.
4.		Full capability for EAP/SIM, EAP/AKA etc. Mobile Data Offload to be done with Mobile Operators.
5.		To allow LSCL to download/ view performance of services utilised by subscribers with key information of Username, MAC, IP, Location, Duration, Upload/ Download & Disconnection reason
6.		Multiple payment gateway integration required so subscribers can make the payments using online/ offline mode, including prepaid mobile balance & wallet applications
7.		Advertising platform integration -AAA to support advertisements from multiple parties
8.		IOS & Android Applications to be given for seamless connectivity to network –auto detect/auto login
9.		Content delivery support
10.		Bidder should share usage data analytics from all monetization across all SSID's with LSCL on a monthly basis
11.		Ability to map SSID to VLAN

#	Parameter	Specifications
12.		WLC Should support Rogue AP detection, classification and standard WIPS signatures.
13.		Should support automatic channel selection – interference avoidance (Co-channel management, Adjacent Channel Management, Channel reuse management)
14.		Should provide Mesh capability for Mesh supported AP
15.		For smooth, seamless and easy manageability, operation, interoperability and maintenance, the bidder should offer/quote WLC & WAPs of the same make (OEM).
16.		Controller should support deep packet inspection for all user traffic across Layer 4-7 network
17.		Support 802.11a/b/g/n/ac wireless standards
18.		AP to Controller Communication
19.	Auto Deployment of APs at different locations	Access points can discover controllers on the same L2 domain without requiring any configuration on the access point.
20.		Access points can discover controllers across Layer-3 network through DHCP or DNS option
21.	Firewall & IPS	Built-in ICSA Certified Wireless Firewall in the Switch
22.		Firewall should support minimum 100000 concurrent sessions
23.		System should provide L2 / L3 stateful firewall, Role based firewall, DOS attacks and Storm control
24.		Should support Access Control Lists (ACLs).
25.		The firewall must be able to take action including allowing the traffic, denying the traffic, rejecting the traffic, routing the traffic, destination or source NAT the traffic, modify the QoS level of the traffic, and blacklist (remove from the network) the client for policy matches
26.		Should include IPS licensing for 5 years from the date of installation
27.		Should adhere to the strictest level of security standards, including 802.11i Wi-Fi Protected Access 2 (WPA2), WPA, Wired Equivalent Privacy (WEP), 802.1X with multiple

#	Parameter	Specifications
		Extensible Authentication Protocol (EAP) types, including Protected EAP (PEAP), EAP with Transport Layer Security (EAP-TLS), EAP with Tunneled TLS (EAP-TTLS).
28.	System Architecture	Centralized MAC addresses filtering
29.		Should support onboard and external DHCP server
30.		Controller should support Onboard AAA server
31.		Radio coverage algorithm must allow adjacent WAPs to operate on different channels, in order to maximize available bandwidth and avoid interference
32.		Support roaming between access points deployed on same subnet and different subnets
33.	QoS features	Per user bandwidth Rate Limiting
34.		Self-healing (on detection of RF interference or loss of RF coverage)
35.		Should support per user, per device, and per application/TCP-port prioritization
36.		Should support 802.11e WMM
37.		Support advanced multicast features with multicast rate optimization, multi-channel use and IGMP snooping
38.	RF Management	Traffic shaping capabilities to offer air-time fairness across different type of clients running different operating systems in order to prevent starvation of client throughput in particular in a dense wireless user population without the use of client specific configurations or software.
39.		Load balancing across bands and steering of dual-band capable clients from 2.4GHz to 5GHz in order to improve network performance without the use of client specific configurations or software.
40.		Allow for automatic and manual RF adjustment.
41.	Inline Security Features	Should allow authenticated client devices to roam securely from one access point to another, within or across subnets, without any perceptible delay Security during re association.

#	Parameter	Specifications
42.		Controller should support DES, 3DES and AES-128 and AES-256 encryption, with site-to-site and client-to-site VPN capabilities; should have provision to supports IPSEC tunnels
43.	Management	Command line interface to control and manage all aspects of the WLAN system from controller
44.		SNMP v3 or latest
45.		Browser-based system for total solution management including: configuration, monitoring, troubleshooting
46.		Single dashboard view of overall network, user, and security status

### 5.7.3.2 Outdoor Access Point

#	Parameters	Specifications
1.	External Protection	The Access point shall be IP66/IP67 rated for dust and water Ingress protection. Third party casing will not be accepted.
2.	Features	Must support the ability to serve clients and monitor the RF environment concurrently.
3.		Access Points proposed must include radios for both 2.4 GHz and 5 GHz.
4.		Should support mesh capabilities for temporary connectivity in areas with no Ethernet cabling.
5.		Mesh support should support QoS for voice over wireless.
6.		should support 802.11e and WMM
7.		Must support Reliable Multicast Video to maintain video quality
8.		Must support QoS and Call Admission Control capabilities.
9.		Must support IPv4 and IPv6.
10		
11		Must support telnet and/or SSH login/Console to WAPs directly for troubleshooting flexibility.
12	Ports	AP should have minimum two Auto-sensing Gigabit Ethernet port.

#	Parameters	Specifications
13		Must support Power over Ethernet.
14	Throughput	Must support data rates upto 1.3Gbps on 5Ghz radio.
15	Power	Must support Direct 100- 240 VAC / DC / PoE+ to power up access point.
16	Mobility	Minimum of 16 SSIDs available on each AP simultaneously without negatively impacting system performance
17		Access Point radio should be minimum 3X3 MIMO with minimum 3 spatial streams or more. Dual Radio capable.
18	Management	Real-time, fully integrated spectrum analyzer capabilities on the APs, that does not require dedicated sensors or separate operating system running on the AP radios.
19		The Access Point should have the technology to improve downlink performance to all mobile devices.
20	High throughput	Access Point should be 802.11ac ready from day one.
21	Diagnostics	Real time packet capture on the APs, without disconnecting clients.
22	Mounting	Access point should be supplied with OEM mounting kit and shall support pole, wall, and roof mounting options
23	Operating Temperature	The Access point shall be rated for operation over an ambient temperature range of 0° to 60°C
24	Transmit Power	Must support up to 28dbm of transmit power for 2.4 & 5Ghz radios, (limited as per Govt, of India regulation for such WAP)

### 5.7.3.3 WLAN Management System

#	Minimum Requirement
1	The system shall authenticate the City Wi-Fi users of Chennai. The system shall also provide facilities like web self-care.
2	The system shall comply to the DoT guidelines regarding provision of Wi-Fi internet



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

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

### 5.7.4 Centralised software for Smart Street Lights

#	Specifications
14.	Web Base Software replaces visual inspections of individual street lighting while sitting at workstation with Internet connectivity. Also by fault alarm and monitoring of data user can judge the fault status and severity of fault
15.	Remote switching through Web Base Software to override local controller
16.	User can demand any time live status of feeder pillar for current electrical and real time parameters
17.	Emergency Stop / Manual ON / Manual OFF / Test Mode of feeder pillar
18.	User can monitor and change all settable parameter setting and clock time setting
19.	Control at any level of individual Street lights. Generate electrical profile of any individual feeder pillar
20.	Unit should be directly mapped on GIS Map
21.	The software shall receive the self-generated data message from individual Feeder Pillar like, ON time, Off time, Dim time, Power Down time, Auto mode / Manual Mode, Volt Fault, Over Current Fault, Short Circuit Fault, Neutral Fault, RTC Fault, ADC Fault, Memory Fault, Low Ampere Fault, Door Open, Relay Fault, Calibration Data and acknowledgement of message demand by WEB of Parameter writing, E Stop, Test Mode, E Profile. All these messages contain all electrical parameter with real-time clock date and time
22.	The software shall generate report of any date or any date range for fault and message of individual unit or all the units. The software shall also generate Range Report for fault, Message, Voltage graph, Current Graph, Streetlight On time, VA Consumption, etc.
23.	All the data collected by the software shall be exported to work sheet format for further analysis as per requirement. The system should be able to generate graph and reports as per requirements
24.	Can be operated and viewed from anywhere in the world
25.	System should be easily expanded and maintained. The system should have the capabilities for new configurations remotely.
26.	Web Interface should give instant status of the street lights on the dynamic Google map

### 5.7.5 Public Address System

#### 5.7.5.1 Functional Specifications

- a) The Public Address System (PA) should be capable of addressing citizens at specific locations from the Command and Control Center.

- b) The proposed system shall contain an IP-based announcing control connected to the Command and Control Center.
- c) Public Address system shall be used at intersections, public places, market places or those critical locations as identified by Authority to make important announcements for the public. It shall be able to broadcast messages across all PA systems or specific announcement could be made to a particular location supporting single zone / multi zone operations. The system shall also deliver pre-recorded messages to the loud speakers attached to them from CD/DVD Players & Pen drives for public announcements.
- d) The system shall contain an IP-based amplifier and uses PoE power that could drive the speakers. The system shall also contain the control software that could be used to control/monitor all the components of the system that includes Controller, Calling Station & keypad, Amplifier (Mixing & Booster).
- e) The SI shall describe in detail the design, operational and physical requirements of the proposed public announcement system to demonstrate compliance with all the specified requirements of RFP.
- f) PA system's master controller should have function keys for selecting the single location, group of locations or all locations, simple operation on broadcasting to any terminal or separated zones.
- g) PA system's master controller should facilitate multiple MIC inputs and audio inputs.

#### 5.7.5.2 Technical Specifications

#	Parameter	Minimum Specifications or better
1.	PAS system	Should have the capability to control individual PAS i.e. to make an announcement at select location (1:1) or multiple locations (1: many). The PAS should also support both Live and Recorded inputs
2.	Speakers	<ul style="list-style-type: none"> <li>• Minimum 2 Speaker, to be used in different directions</li> <li>• Minimum 50 Watts of amplification</li> </ul>
3.	Connectivity	IP Based
4.	Access Control	Access control mechanism would be also required to establish so that the usage (including sound volume) is regulated.
5.	Integration	Command and Communications Center, Police Command Control Center, Traffic Control Center
6.	Battery	Internal Battery with different charging options (Solar/Mains)
7.	Power	Automatic on/off operation
8.	Casing	IP-65 rated for housing
9.	Operating conditions	0° to 50°C

## 5.7.6 Emergency Call Box

### 5.7.6.1 Functional Specifications

- a) The emergency box (or panic button) will enable citizens to establish a two way audio (microphone and speaker) & camera (video camera and a video screen) communication link with Police (or / and with Authority's Disaster Management Cell or Command and Control Center) through a press of a button.
- b) Emergency/ Panic buttons to be strategically located, suitably sized and identified/clearly labelled for "Emergency".
- c) The emergency feature must also be available within the mobile app which will enable the user to initiate a bidirectional audio call with Police /Command and Control Center.
- d) The unit shall preferably have a single button which when pressed, shall connect to Authority.

### 5.7.6.2 Technical Specifications

#	Parameter	Minimum Specifications or better
1.	Construction	Cast Iron/Steel Foundation, Sturdy Body for equipment
2.	Call Button	Watertight Push Button, Visual Feedback for button press
3.	Speaker & Microphone	VOIP Phone, Hands-free calling, Watertight and industrial grade equipment
4.	Connectivity	3G/4G/Ethernet/Fibre as per solution offered
5.	CCTV Camera	IP based, Color camera with minimum D1 resolution, Day/Night mode operations
6.	Battery	Internal Battery with different charging options
7.	Power	Automatic on/off operation
8.	Casing	IP-65 rated for housing
9.	Operating Conditions	0° to 50°C
10.	Certification	UL/CE/EN

## 5.8 ICT Enabled Smart Solid Waste/Bin Management

### 5.8.1 Overview

Authority is responsible for collection, segregation, transportation, dumping and processing of the city waste from door to door. Authority has deployed vehicles for collection of door to door waste and dumping into the bins/collection points at strategic locations. From these bins/collection point separate 4 wheelers (loaders) carries the waste to the single location

called waste processing Also, Authority has field plant. Staff which is responsible for street sweeping and collection of street waste and dumping to the nearest bins/collection points.

Currently, managing the people responsible for the activity and proper utilization of assets/resources assigned to them has become a complex job for Authority. The main problems of the existing solid waste collection process are:

1. Lack of information about the collecting time and area.
2. Lack of proper system for monitoring, tracking the vehicles and trash bin that have been collected in real time.
3. There is no estimation to the amount of solid waste inside the bin and the surrounding area due to the scattering of waste.
4. Physical visit required to verify employee performance
5. The waste keeps lying unattended for several days.
6. There is no quick response to urgent cases like truck accident, breakdown, long time idling etc.]
7. Total tonnage details of waste being dumped in dumpyard.

Authority intends to implement a GIS/GPS enabled Solid Waste Management System practices within the existing landscape to:

1. Manage routes and vehicles dynamically through an automated system.
2. Real time manage of missed garbage collection points
3. Efficient manage of waste collection bins
4. Do Route optimization which shall help in reduction of trip time, fuel saving and serving more locations
5. Reduce the human intervention in monitoring process
6. Keep history of vehicle routes, attended sites and other details
7. Integrate the dumping ground and transfer station facilities with the centralized locations
8. Reporting of vehicles, garbage collected and other SWM details to higher authorities from any location at any time
9. Monitor and track the activities of field staff force on daily basis

### **5.8.2 Scope of Work**

1. Total No. of waste collection vehicles – 50
2. Total No. of Loaders – 10

## **5.9 Parking Management System**

### **5.9.1 Project Objective**

To integrate parking related data to be integrated to CCC to have more predictive analysis by checking for any synergies of parking related data with the object of interest.

### **5.9.2 Detailed Scope of Work:**

#### **5.9.2.1 Integrations with 3<sup>rd</sup> Parking Management Solution in the City**

- a. .The solution should be able to interface to the 3<sup>rd</sup> party Parking Management solution being planned out in the Chennai City
- b. The solution shall also include data from other assets such as Parking sensors / On-street parking cameras / Kiosks for parking tickets / etc.
- c. The Solution shall be flexible to integrate with 3<sup>rd</sup> party mobility products

##### **5.9.2.1.1.1 Integration with Third Party Services and Apps**

- i. The System Integrator has to ensure that the App can integrate and interface with popular and established third party services and applications (private or public) that wish to integrate with Mobile App, upon approval from GCC.
- ii. The App should integrate with and allow payments through the selected third part shared services for Payment Gateway and e-Wallet
- iii. The App should have provisions to integrate with Emergency Response services

##### **5.9.2.1.1.2 Frequently Asked Questions (FAQs) and Contact Details of different offices of GCC**

- i. The App should have a section detailing frequently Asked Questions (FAQs) related to Smart initiatives and their related responses
- ii. The section should also provide contact information of Helpdesk Customer Service for parking problems, if any.

### **5.9.2.1.1.3 Settings**

- i. User should view version and details of the App
- ii. User should have the option to toggle between sending current GPS data to server or not
- iii. User should have the option to select a specific button on their cell phone to set as SOS short-cut, when pressed and help continuously for a certain amount of time
- iv. User should be able to toggle whether or not to send anonymous user data that can be helpful in fixing bugs or solving crashes.
- v. User should be able to select notification settings
- vi. User should be able to select app notifications to be displayed on the home/locked screen
- vii. User should have ability to enable/disable sound alerts

### **5.9.2.1.1.4 Mobile App Scope – Technical Requirements**

- i. Shall be developed in an open platform
- ii. Should be scalable and technically adaptable to future enhancements
- iii. Should be SSL (Secured Socket Layer) compliant and the System Integrator has to provide appropriate SSL certificate before the portal is made available on public domain
- iv. Should be published and released in all the major platforms including iOS, Android, Blackberry, Symbian and Windows.
- v. Should support unicode and be multilingual in at least English and Tamil
- vi. Should be easy to update as some data will be updated daily. Ability to collect data with high volume, velocity, and variety
- vii. Should track GPS location of the user device
- viii. Should provide accurate mapping and navigation services.
- ix. Collect data categorically without impacting citizen's privacy issues
- x. Command Centre should provide live feed from parking lots and number of free spaces to app



- xi. Command Centre should confirm acceptance of payment and reserve/cancel the parking lots accordingly
- xii. Command Centre should monitor GPS in an emergency and user data sent from the app if the user accepts sending of data

#### **5.9.2.1.1.5 Online Portal Scope - Technical Requirements (To be linked with GCC website/portal)**

- i. Should be based on Open Standards
- ii. Should integrate with any other portal products through open standards such as HTML, XML, RSS, web services, and WSRP
- iii. Should support encryption and compression features
- iv. Shall be OS independent. It must run on Windows, Unix, Apple and Linux operating systems
- v. Shall be browser independent and responsive to run in the same manner on leading browsers like Google Chrome, Mozilla Firefox, Safari, Internet Explorer, etc.
- vi. Shall support Unicode and be multilingual in at least English and Tamil
- vii. Shall have provision for patches, hotfixes and bug fixing solutions
- viii. Shall adhere to the best possible security standards in the industry
- ix. Shall support broad range of standards as applicable
- x. Shall support minimum Web 2.0 capabilities
- xi. Shall be SSL (Secured Socket Layer) compliant and the System Integrator has to provide SSL certificate before the portal is made available on public domain
- xii. Shall adhere to W3CAG, GIGW and G.O.I guidelines

#### **5.9.2.2 Vehicle and License Plate Image Capture**

- i. Capability to automatically capture details of vehicle license plates at every entry and exit of each parking lot
- ii. Image should be clicked at the entry point when the ticket is issued and at the exit point during payment.

- iii. Image of the license plate should be linked to the details of the corresponding ticket issued in real-time and stored in the database for one month. This information will be stored in the Central Control Centre
- iv. Daily system checks to ensure tracking of vehicles which have entered the premises but are yet to leave. Thereafter, PMGS shall generate alert, if any vehicle is overstaying in the parking lot after closing hours.
- v. Install appropriate cameras at parking lot, entry and exit of each Parking Lot in such a way that whole of the parking lot shall be covered with CCTV.

#### **5.9.2.3 Provision for Smart Card (NFC enabled Prepaid Smart Card)**

- i. Along with the paper ticket, the System Integrator shall propose a cost effective smart payment solution to include NFC enabled Prepaid Smart Card system for all users and those users opting for monthly reserved parking passes.
- ii. The NFC enabled smart card reader would be available at all Pay Stations and would automatically deduct the applicable parking charges.
- iii. NFC enabled smart card solution should be integrated with all relevant parking related information and payments back and forth with the Central Control Centre.

#### **5.9.2.4 Real-time Monitoring and Dynamic MIS Reporting**

- i. PMGS shall include central reporting system establishing the connection between the devices and sensors and the Central Control Centre
- ii. Solution shall include reporting dashboards with location specific thresholds to be set for generating customized reports
- iii. Shall be capable of monitoring the number of vehicles entering/ exiting the parking premises during any given time
- iv. IV. Shall generate real time reports for each parking spot, in each of the parking lots capturing utilization, revenues, status of assets and personnel. These reports should be available in all standard acceptable formats like .csv, .pdf, .txt, etc.

- v. Ensure analytics on the following thematic areas:
  1. Enforcement – Daily report on violations;
  2. Peak parking demand on hourly basis at each parking lot;
  3. Daily, weekly, monthly, quarterly and yearly average occupancy at each parking lot;
  4. Average time of occupancy;
  5. Revenue trends daily, weekly, monthly, quarterly and annually;

#### **5.9.2.5 Payment Mechanisms**

- i. The primary mode of payment for parking will be by pre-paid card, e-wallet, payment gateway or cash at the Pay Station, or any other appropriate mode of payment with prior approval from GCC.
- ii. For bookings through Mobile App or Smart online web-based portal application, payment will be made using e-Wallet, net banking, credit card, debit card etc. A discount of 10 percent shall be entitled to all users for payment through prepaid card, e-wallet, payment gateway etc. except cash payment.

#### **5.9.2.6 Parking Enforcement/Towing**

- a) The System Integrator shall deploy Intelligent Tow Truck (as per requirement subject to a minimum of three numbers) for towing of illegally parked vehicles, in the area defined in this Tender and shall be accompanied by GCC/Chennai Traffic police personnel. The System Integrator will tow vehicles parked in an unauthorized manner to the nearby parking space which is less utilized or at space designated for this purpose by the GCC. GCC/Chennai Traffic Police will charge penalty as well as towing charges from the owner of the vehicle. The towing charges for each vehicle will be handed over to the System Integrator as decided. Initially the numbers of Tow trucks required will be more.
- b) If the unauthorized parked vehicle is not in a position to be towed away, the System Integrator will arrange to put jammers in the wheels of the vehicle, so that GCC/traffic police personnel are able to fine the vehicle. Necessary information regarding towed vehicles will be updated on the GCC app and web portal immediately. Additionally, information regarding details of towed vehicles shall be available to users through a

dedicated helpline number. The dedicated helpline will be operated by the System Integrator.

- c) If the System Integrator fails to tow away any such vehicles parked in an unauthorized manner within thirty minutes, GCC will charge a fine from the System Integrator for each such vehicle as per applicable penalty clause.
- d) The System Integrator shall take necessary precautions while towing of vehicle with regards to safety of the vehicle. Any damage caused to vehicle during towing will be the liability of System Integrator.
- e) The System Integrator shall display live feed of video recording of cameras on crane on the web portal and also to traffic police & CCC of GCC. GPS is to be installed on each such tow truck and the online GPS information of the tow truck shall be available on GCC web portal, traffic police and GCC. Information of all clamped and tow away vehicle shall be uploaded on the app and web portal immediately.

#### **5.9.2.7 Technical Requirements:**

This section provides an overview of the technical requirements, specifications, standards and certifications:

##### **5.9.2.7.1 Integration of parking management System**

- i. Sensors should be installed in ground for detecting real-time status of the parking bay.
- ii. Ability to upgrade its firmware functionality remotely from Central Control Centre.
- iii. Ability to permit an optimal angle between the sensor output and the target.
- iv. Ability to work in all weather conditions relevant to the project site.
- v. Shall have magnetic cum optical/ magnetic cum IR technology
- vi. Shall reliably detect presence or absence of car within 20 seconds of car parking/ un-parking event occurrence.

## **6 Common guidelines / comments regarding the compliance of IT / Non-IT Equipment / Systems to be procured**

- 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.
- Any manufacturer and product name mentioned in the RFP should not be treated as a recommendation of the manufacturer / product.
- None of the IT / Non-IT equipment 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 this RFP, where-in the OEM will certify that the product is not end of life product & shall support for at least 54 months from the date of Bid Submission.
- Technical Proposal should be accompanied by OEM's product brochure / datasheet. 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.
- All equipment, parts should be Original and New.
- The User Interface of the system should be a User Friendly Graphical User Interface (GUI).
- Critical / Core components of the system should not have any requirements to have proprietary Platforms and should conform to open standards.
- For the 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. The application shall be subjected to Application security audit to ensure that the application is free from any vulnerability.
- The Successful Bidder should also propose the suitable specifications of any additional servers / other hardware, if required for the system.
- The Servers provided should meet industry standard performance parameters (such as CPU Utilization of 60% or less, disk utilization of 75% or less).
- SI is required to ensure that there is no choking point / bottleneck anywhere in the system (end-to-end) to affect the performance / SLAs.
- All the hardware and software supplied should be from the reputed Original Equipment Manufacturers (OEMs). CSCL reserves the right to ask replacement of any hardware / software if it is not from a reputed brand and conforms to all requirements specified in tender documents.

- OEMs for Servers, Enterprise Storage and Wired & Wireless LAN Access Infrastructure should be placed in Gartner MQ Leaders Segment as per latest Gartner Report OR should have double digit market share as per latest IDC Report in their respective products.
- All necessary hardware, software, licenses etc. will be in the name of GCC. In case of Custom-built bespoke application, the IPRs shall also be transferred to CSCL.
- Successful bidder shall make the details of new technologies, new hardware available in the market to CSCL. Both, CSCL and SI, in agreement, will take decision of new technology/ hardware implementation in case any new/ advanced technology comes up during the contract period.

## 7 Payment Terms & Payment Schedule

1. The request for payment shall be made to the Authority in writing, accompanied by invoices describing, as appropriate, the services performed, and by the required documents submitted pursuant to general conditions of the contract and upon fulfilment of all the obligations stipulated in the Contract.
2. Due payments shall be made promptly by the Authority, after submission of an invoice or request for payment by SI
3. The currency or currencies in which payments shall be made to the SI under this Contract shall be Indian Rupees (INR) only.
4. All remittance charges shall be borne by the SI.
5. In case of disputed items, the disputed amount shall be withheld and shall be paid only after settlement of the dispute.
6. Any penalties/ liquidated damages, as applicable, for delay and non-performance, as mentioned in this RFP document, shall be deducted from the due payments of the respective milestones.
7. Taxes, as applicable, shall be deducted / paid, as per the prevalent rules and regulations

### Payment Schedule

Payments to SI, after successful completion of the target milestones (including specified project deliverables), shall be made as under:

#	Payment Milestone	Timelines	% Payment
1	CCC Solution Design Sign-off	T + 45 days	10% of CAPEX
2	Supply & Installation of all IT & Non-IT infrastructure, at Command Communications Center (CCC).	T+150 Days	20% of CAPEX
3	Pre-Acceptance Testing by SI and submitting Readiness request for carrying out Final Acceptance Testing	T + 210 Days	20% of CAPEX
4	Final Acceptance Testing of the CCC Solution Sign-off	T+240 Days	20% of CAPEX
5	CCC Solution stabilization & Go-Live	G = T + 300 Days	25% of CAPEX
6	Quarterly Payments - Operations & Maintenance Phase for a period of 5 years	G+20Quarters	5% of OPEX per quarter (OPEX equally amortized across 20 quarters)
7	20 <sup>th</sup> Quarter – Project Closures Exit Management	G+ 20th Quarter	Remining 5% of CAPEX

#### Note:

T is the date of signing of contract

G is the date of Go Live of the CCC solution & also marks the commencement of O&M Phase (the exact date of commencement of O&M shall be decided by Authority)

## 8 Annexure 1 Matrix for Scope of Work

#	Key Activities	Deliverables	CCC	Surveillance	Sensors	Emergency Call Box	Public Address System	Digital Display Boards	e-Governance	Portal/ Mobile App
<b>Project Inception Phase</b>										
1	Project Kick Off	1. Project	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
2	Deployment of manpower	Development Plan 2. Risk Management and Mitigation Plan	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
<b>Requirement Phase</b>										
3	Assess the requirement of IT Infrastructure and Non IT Infrastructure	1. Functional Requirement Specification Document 2. System	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
4	Assessment of Business processes	Requirement Specification document	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
5	Assessment of requirement of Software requirements	3. Requirements Traceability Matrix 4. Site Survey Report	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
6	Assess the Integration requirement		Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
7	Assess the connectivity requirement all locations (including Building)		Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
8	Assessment the Network laying requirement		Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes



#	Key Activities	Deliverables	CCC	Surveillance	Sensors	Emergency Call Box	Public Address System	Digital Display Boards	e-Governance	Portal/ Mobile App
9	Assessment of training requirement		Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
<b>Design Phase</b>										
10	Formulation of Solution Architecture	1. Final Bill of Quantity	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
11	Creation of Detail Drawing	2. HLD documents	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
12	Detailed Design of Smart City Solutions	3. LLD documents	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
13	Development of test cases (Unit, System Integration and User Acceptance)	4. Application architecture documents.	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
14	Preparation of final bill of quantity and material	5. Technical Architecture documents.	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
15	SoP preparation	6. Network Architecture documents.	Yes							
		7. ER diagrams and other data modeling documents.								
		8. Logical and physical database design.								
		9. Data dictionary and data definitions.								
		10. GUI design (screen design, navigation, etc.).								
		11. Test Plans								
		12. SoPs								

#	Key Activities	Deliverables	CCC	Surveillance	Sensors	Emergency Call Box	Public Address System	Digital Display Boards	e-Governance	Portal/ Mobile App
		13. Change management Plan								
<b>Development Phase</b>										
16	Helpdesk setup	1. IT and Non IT Infrastructure Installation Report 2. Completion of UAT and closure of observations report 3. Training Completion report 4. Application deployment and configuration report	Yes			Yes			Yes	
17	Physical Infrastructure setup		Yes	Yes	Yes	Yes	Yes	Yes		
18	Procurement of Equipment , edge devices, COTS software (if any), Licenses		Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
19	IT and Non IT Infrastructure Installation		Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
20	Development, Testing and Production environment setup		Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
21	Software Application customization (if any)		Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
22	Development of Bespoke Solution (if any)		Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
23	Data Migration		Yes						Yes	
24	Integration with Third party services/application (if any)		Yes						Yes	Yes
25	Unit and User Acceptance Testing		Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
26	Implementation of	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	

#	Key Activities	Deliverables	CCC	Surveillance	Sensors	Emergency Call Box	Public Address System	Digital Display Boards	e-Governance	Portal/ Mobile App
	Solutions									
27	Preparation of User Manuals , training curriculum and training materials		Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
28	Role based training(s) on the Smart City Solutions		Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
<b>Integration Phase</b>										
29	SoP implementation	1. Integration Testing Report	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
30	Integration with GIS		Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
31	Integration of solutions with Command and Control Centre			Yes	Yes	Yes	Yes	Yes	Yes	Yes
<b>Go -Live</b>										
32	Go Live	1. Go-Live Report	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
<b>Operation and Maintenance</b>										
33	Operation and Maintenance of IT, Non IT infrastructure and Applications	1. Detailed plan for monitoring of SLAs and performance of the overall system	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
34	SLA and Performance Monitoring	2. Fortnightly Progress Report	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
35	Logging, tracking and resolution of issues.	3. Monthly SLA Monitoring Report and Exception Report	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
36	Application enhancement		Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes

#	Key Activities	Deliverables	CCC	Surveillance	Sensors	Emergency Call Box	Public Address System	Digital Display Boards	e-Governance	Portal/Mobile App
37	Patch & Version Updates	4. Quarterly security Report	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
38	Helpdesk services	5. Issues logging and resolution report	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes

## 9 Annexure 2 – RACI (Responsible, Accountable, Consulted and Informed) Matrix

#	Key Activities	Successful Bidder	GC C	SP V for GC C	CS CL	Electricity Providers	Other Utilities	Police	PM C	Existing ICT Vendors at GCC
<b>Project Inception Phase</b>										
1	Project Kick Off	R/A	C	C	I	I	I	I	C	I
2	Deployment of manpower	R/A	C	C	I	I	I	I	C	I
<b>Requirement Phase</b>										
3	Assess the requirement of IT Infrastructure and Non-IT Infrastructure	R/A	C	C	C	C	C	C	C	C
4	Assessment of Business processes	R/A	C	C	I	I	I	C	C	I
5	Assessment of requirement of Software requirements	R/A	C	C	I	I	I	C	C	I
6	Assess the Integration requirement	R/A	C	C	C	C	I	C	C	C
7	Assess the connectivity requirement all locations (including Building)	R/A	C	C	C	I	I	C	C	I
8	Assessment	C	C	C	R/A	I	I	C	C	I

#	Key Activities	Successful Bidder	GC C	SP V for GC C	CS CL	Electricity Providers	Other Utilities	Police	PM C	Existing ICT Vendors at GCC
	the Network laying requirement									
9	Assessment of training requirement	R/A	C	C	I	I	I	C	C	I
<b>Design Phase</b>										
10	Formulation of Solution Architecture	R/A	C	C	C	I	I	C	C	I
11	Creation of Detail Drawing	R/A	C	C	C	I	I	C	C	I
12	Detailed Design of Smart City Solutions	R/A	C	C	C	I	I	C	C	I
13	Development of test cases (Unit, System Integration and User Acceptance)	R/A	C	C	C	I	I	C	C	I
14	Preparation of final bill of quantity and material	R/A	C	C	C	C	I	C	C	I
15	SoP preparation	R/A	C	C	C	C	C	C	C	I
<b>Development Phase</b>										
16	Helpdesk setup	R/A	C	C	I	I	I	I	C	I
17	Physical Infrastructure setup	R/A	C	C	I	I	I	I	C	I

#	Key Activities	Successful Bidder	GC C	SP V for GC C	CS CL	Electricity Providers	Other Utilities	Police	PM C	Existing ICT Vendors at GCC
18	Procurement of Equipment , edge devices, COTS software (if any), Licenses	R/A	C	C	I	I	I	I	C	I
19	IT and Non IT Infrastructure Installation	R/A	C	C	I	I	I	I	C	I
20	Development, Testing and Production environment setup	R/A	C	C	I	I	I	I	C	I
21	Software Application customization (if any)	R/A	C	C	I	I	I	I	C	I
22	Development of Bespoke Solution (if any)	R/A	C	C	I	I	I	I	C	I
23	Data Migration	R/A	C	C	I	I	I	I	C	I
24	Integration with Third party services/application (if any)	R/A	C	C	I	I	I	I	C	I
25	Unit and User Acceptance	R/A	C	C	I	I	I	I	C	I

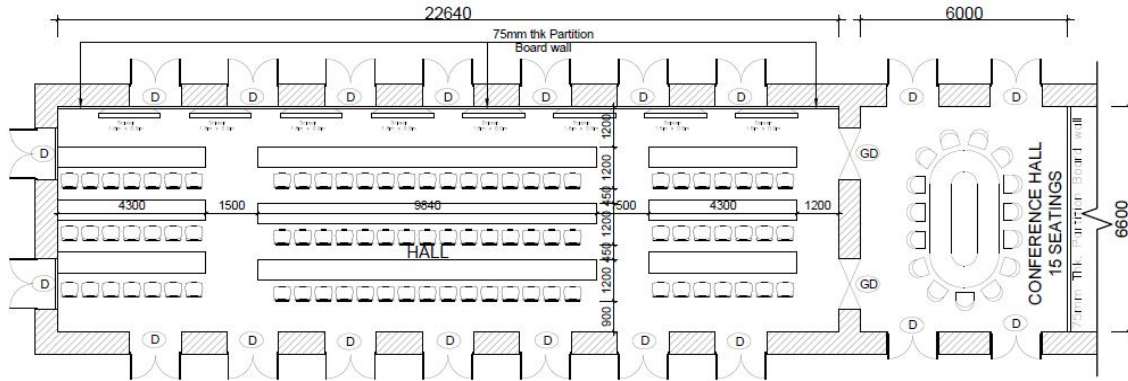
#	Key Activities	Successful Bidder	GC C	SP V for GC C	CS CL	Electricity Providers	Other Utilities	Police	PM C	Existing ICT Vendors at GCC
	Testing									
26	Implementation of Solutions	R/A	C	C	I	I	I	I	C	I
27	Preparation of User Manuals , training curriculum and training materials	R/A	C	C	I	I	I	I	C	I
28	Role based training(s) on the Smart City Solutions	R/A	C	C	I	I	I	I	C	I
<b>Integration Phase</b>										
29	SoP implementation	R/A	C	C	C	C	C	C	C	I
30	Integration with GIS	R/A	C	C	C	C	C	C	C	I
31	Integration of solutions with Command and Control Centre	R/A	C	C	C	C	C	C	C	I
<b>Go -Live</b>										
32	Go Live	R/A	C	C	I	I	I	I	C	I
<b>Operation and Maintenance</b>										
33	Operation and Maintenance of IT, Non IT infrastructure and	R/A	C	C	I	I	I	I	C	I



#	Key Activities	Successful Bidder	GC C	SP V for GC C	CS CL	Electricity Providers	Other Utilities	Police	PM C	Existing ICT Vendors at GCC
	Applications									
34	SLA and Performance Monitoring	R/A	C	C	I	I	I	I	C	I
35	Logging, tracking and resolution of issues.	R/A	C	C	I	I	I	I	C	I
36	Application enhancement	R/A	C	C	I	I	I	I	C	I
37	Patch & Version Updates	R/A	C	C	I	I	I	I	C	I
38	Helpdesk services	R/A	C	C	I	I	I	I	C	I

# 10 Annexure 3: Command & Control Center Layout

## Reference Layout of CCC Main Area



**PART OF SECOND FLOOR PLAN SHOWING  
FURNITURE LAYOUT OPTION -1**

Total No. of Seats : 87 Nos.  
Total No. of Screens : 08 Nos.

## 11 Annexure 5: List of Locations

### 11.1 List of 22 subways for surveillance

S.No	Zone/Dn.No	Name of the Subway
1	1/1	Katthivakkam High Road(ROB)
2	1/5	Manickam Nagar Subway
3	4/46	Vyasarpadi Subway(ROB)
4	5/52	MC Road Subway
5	5/60	RBI Subway
6	5/61	Gengu Reddy Subway
7	5/53	Stanley Nagar Subway(ROB)
8	6/70	Ganeshapuram Subway(ROB)
9	6/70	Perambur Highroad Subway
10	8/94	Villivakkam Redhills Subway
11	8/107	Harington Subway
12	9/109& 110	Nungambakkam Subway
13	10/134	Rangarajapuram Subway
14	10/136	Duraisamy Subway
15	10/135	Madley Subway
16	10/142	Jones Road Subway
17	10/142	Bazaar Street
18	10 & 13/ 140 & 171	Aranganathan Subway
19	12/161	Mount subway
20	12/163	Pazhavanthangal Subway
21	12/162	Thillaiganga Nagar Subway
22	12/166	Meenambakkam Subway

### 11.2 List of 100 locations for surveillance

Sl.No	Station	Name of the junction.
-------	---------	-----------------------

Sl.No	Station	Name of the junction.
1	C1 Flower Bazaar	Rattan Bazaar Rd X Evening Bazaar (MUC)
2	C2 Elephant gate	Wall Tax Road X EB Point
3	C2 Elephant gate	Wall Tax Road X Padmanabha Theatre
4	C2 Elephant gate	Wall Tax Road X Rasappa Road
5	H1 Washermenpet	BB Rd X Mint jn
6	H1 Washermenpet	Walltax Rd X Basin Bridge (Moolakothalam)
7	N3 Muthialpet	Stanley Round About
8	H1 Washermenpet	Stanley Hospital jn
9	H1 Washermenpet	MC Road X Cemetry Rd Jn
10	H1 Washermenpet	TH Rd X Cemetry Rd jn
11	H3 Tondiarpet	TH Rd X IDH jn
12	H5 New Washermenpet	TH Rd X Tollgate jn
13	H5 New Washermenpet	SN Chetty Check post
14	N1 Royapuram	SN Chetty St X Kuppam Rd jn
15	N1 Royapuram	MS Koil St X SN Chetty St (N1 PS.)
16	N1 Royapuram	MS Koil St X Cemetry Rd jn
17	K1 Sembiam	Perambur High Rd X Paper Mills Rd Jn
18	G1 Vepery	Jermaiah Road
19	G2 Periamet	V H Road X Sydenhams Road Jn (Raja Muthiah Salai)
20	G2 Periamet	Demellous Point
21	G3 Kilpauk	Orms Road X Kellys Rd Jn
22	G1 Vepery	Doveton Point
23	G3 Kilpauk	Millers Rd x Pursaiwakkam Jn
24	K7 ICF	Kellys Point
25	G3 Kilpauk	Tailers Rd X Kilpauk Garden Jn
26	G-7 Chetpet	T.P.Chattiram x Halls Road
27	G3 Kilpauk	New Avadi Rd X Kilpauk Garden Rd
28	K7 ICF	New Avadi Rd X Raju St
29	K7 ICF	New Avadi Rd 3rd Avenue
30	K7 ICF	New Avadi Rd X ICF Annexe
31	K7 ICF	ICF Point
32	K7 ICF	Konnur High Road Joint Office
33	K7 ICF	Konnur I Point
34	K7 ICF	Medavakkam Tank Road X ESI Hospital
35	V1 Villivakkam	Nathamuni Jn
36	V1 Villivakkam	CTH Rd X Singaram Pillai School Jn.(SIDCO Nagar)
37	T1 Ambattur	CTH Rd X Ambattur Telephone Exchange
38	T1 Ambattur	CTH Rd X TVS Lucas Jn
39	T1 Ambattur	CTH Rd X Korattur Jn.
40	V1 Villivakkam	200 Feet Rd X Retteri Junction
41	V1 Villivakkam	200 Feet Rd X Senthil Nagar

Sl.No	Station	Name of the junction.
42	V1 Villivakkam	200 Feet Rd X Raja Mangalam
43	V1 Villivakkam	200 Feet Rd X Thathankuppam
44	V5 Thirumangalam	Inner Ring Rd X 18th Main Rd
45	V5 Thirumangalam	Eatate Rd X Officers Rd
46	V5 Thirumangalam	Estate Rd X Park Rd
47	V5 Thirumangalam	Estate Rd X DAV School
48	V5 Thirumangalam	Estate Rd X MMM Hospital
49	V5 Thirumangalam	Estate Rd X Mangal Yeri
50	K4 Annanagar	Anna Nagar Main Rd X Iyyappan Koil (Removed)
51	K4 Annanagar	Anna Nagar Main Rd X Blue Star (Removed)
52	K4 Annanagar	Anna Nagar 2nd Avenue X 12th Main Rd Jn
53	K4 Annanagar	Anna Nagar Rountana
54	K4 Annanagar	Anna Nagar 1st Avenue XChinthamani
55	K4 Annanagar	Anna Nagar Shanthy Colony
56	K4 Annanagar	Anna Nagar K4 PS Rountana
57	F3 Nungambakkam	NM Road X Choolai Medu Jn
58	K3 Aminjikarai	NM Road X Metha Nagar Jn(Switched off)
59	R5 Virugambakkam	Kalamman koil st X Chinmaya nagar Jn
60	R5 Virugambakkam	Arcot Rd X Arunchalam Road Jn
61	R5 Virugambakkam	Arcot Rd X 80 Feet Rd
62	R5 Virugambakkam	Arcot Rd X Vembuli amman Koil Jn
63	R5 Virugambakkam	Arcot Rd X Kamaraj Salai
64	R5 Virugambakkam	Arcot Rd X Avachi School
65	R9 Valasaravakkam	Arcot Rd X Alwarthirunagar Rd Jn
66	R9 Valasaravakkam	Arcot Rd X Lamech Rd
67	R9 Valasaravakkam	Arcot Rd X Valasaravakkam Rd
68	T15 SRMC	Arcot Rd X Alappakkam jn
69	R7 KK Nagar	PT Rajan Salai X Kamarar Salai (Nagathamman Koil jn)
70	R7 KK Nagar	Anna Main Rd X Munusami Salai (Nesapakkam jn)
71	R7 KK Nagar	Anna Main Rd X PT Rajan Salai
72	S1 Mount	Butt Rd X DPO Cutting (1 Point)
73	S1 Mount	Butt Rd X DPO Cutting (2 Point)
74	S1 Mount	Army Road Jn
75	S1 Mount	IDPL (Ramapuram)
76	S1 Mount	Nanthambakkam Bridge
77	S1 Mount	Miot Hospital Jn
78	S1 Mount	Mount Poonamalli Rd X Manapakkam Road Jn.(Ramapuram)
79	S1 Mount	Mount Poonamalli Rd X L & T Jn Jn.(Ramapuram)
80	T15 SRMC	Mugalivakkam Jn
81	T15 SRMC	SRMC PC School Point
82	T15 SRMC	Porur Rountana

Sl.No	Station	Name of the junction.
83	T15 SRMC	Porur Service Road
84	R9 Valasaravakkam	Ramapuram X Arasamaram jn
85	J3 Guindy	Velachery Check post (Gurunanak College)
86	J3 Guindy	Maduvankarai Main Rd X MKN Jn
87	J3 Guindy	Velachery Main Rd X Maduvankarai Jn.
88	J7 Velachery	Velachery Vijayanagaram jn
89	J7 Velachery	Velachery Main Rd X Veeranam Rd Jn (Nalla thambi Rd )
90	J7 Velachery	Velachery 100 Feet Rd X Bye pass Rd(Maruthupandi Rd )
91	J7 Velachery	Velachery 100 Feet Rd X Lakshmi Nagar jn
92	J7 Velachery	Tharamani Rd X SRP Tools
93	J4 Kotturpuram	Madhyakailash
94	J4 Kotturpuram	Rajiv Gandhi salai X New Bridge Jn
95	J2 Adyar	Indira nagar X Ist Avenue jn (Water Tank)
96	J5 Sasthri Nagar	LB Rd X M.G Road
97	J5 Sasthri Nagar	LB Rd X Sasthri Nagar Jn
98	J5 Sasthri Nagar	MG Road X 7th Avenue Jn
99	J5 Sasthri Nagar	Besent Avenue X Thesophical Society
100	J6 Thiruanmiyur	LB Road X Indira Nagar 3rd Avenue (KALASHETRA)

### 11.3 Smart Pole Locations

S No	Location	No of Smart poles	No of Rain Gauges	No of Pollution
1.	Parks in ABD area (8 Nos)	8	1	1
2.	T Nagar Bus stand	2	1	1
3.	Mambalam railway station – both sides	2	1	1
4.	Ranganathan street	2	1	1
5.	Thiruvanmiyur beach	3	1	1
6.	Besant Nagar beach	3	1	1
7.	Marina beach	10	1	1
8.	CMBT	3	1	1
9.	Central railway station	3	1	1
10.	Egmore railway station	2	1	1
11.	Nungambakkam railway station	1	1	1
12.	Guindy railway station (covering sub-urban	2	1	1

S No	Location	No of Smart poles	No of Rain Gauges	No of Pollution
	and metro stations)			
13.	General Hospital (opposite to Central railway station)	2	1	1
14.	Alandur metro station (including covering mofussil bus stand)	2	1	1
15.	Vadapalani cross road junction	1	1	1
16.	Ashok Pillar (including covering mofussil bus stand)	2	1	1
17.	Guindy snake park	1	1	1
18.	Parrys corner / High court area	1	1	1
	<b>Total</b>	<b>50</b>	<b>18</b>	<b>18</b>

#### 11.4 Location for Flood Sensors

S.No	Zone/Dn.No	Name of the Subway
1	1/1	Katthivakkam High Road(ROB)
2	1/5	Manickam Nagar Subway
3	4/46	Vyasarpadi Subway(ROB)
4	5/52	MC Road Subway
5	5/60	RBI Subway
6	5/61	Gengu Reddy Subway
7	5/53	Stanley Nagar Subway(ROB)
8	6/70	Ganeshapuram Subway(ROB)
9	6/70	Perambur Highroad Subway
10	8/94	Villivakkam Redhills Subway
11	8/107	Harington Subway
12	9/109& 110	Nungambakkam Subway
13	10/134	Rangarajapuram Subway
14	10/136	Duraisamy Subway
15	10/135	Madley Subway

S.No	Zone/Dn.No	Name of the Subway
16	10/142	Jones Road Subway

### 11.5 Tentative location for Variable Messaging Board

S No	Location	Zone	No of Poles	Small VMS	Large VMS
1	Tiruvottiyur High Road (near bus road)	1	1	1	
2	Manali & Ennore Express Road Junction	1	1		1
3	Manali Market	2	1		1
4	NH1 and TPP road Junction	2	1		1
5	Madharvaram Junction	3	1		1
6	Moolaikadai Junction	3	1		1
7	TBD	4	1		1
8	TBD	4	1		1
9	Central railway station	5	1	1	
10	Egmore railway station	5	1	1	
11	General Hospital (opposite to Central railway station)	5	1	1	
12	Parrys corner / High court area	5	1		1
13	Ripon Building	5	1	1	
14	Secretariat	5	1	1	
15	MTH Road	7	1	1	
16	Dunlop Junction	7	1	1	
17	Koyembedu Junction	8	1		1
18	Kelleys	8	1		1
19	ega Theater	8	1		1
20	Pangal Park	9	1		1
21	Marina beach	9	2		2
22	Gemini Flyover	9	1		1
23	Luz Corner	9	1	1	
24	T Nagar Bus stand	10	1		1
25	Mambalam railway station – both sides	10	1	1	



26	Usman Road (South)	10	1		1
27	CMBT	10	1		1
28	Ashok Pillar	10	1		1
29	Porur Junction	11	1	1	
30	Vanagram	11	1	1	
31	Arcot Road	11	1	1	
32	Airport	12	1		1
33	Kattipara Junction	12	2		2
34	IRR	12	1	1	
35	Thiruvanmiyur beach	13	1		1
36	Besant Nagar beach	13	1		1
37	Adyar Junction	13	1		1
38	Little Mount - Raj Bhavan	13	1		1
39	Nandaman Junction	13	1		1
40	DG Dinakaran Salai - Music College	13	1		1
41	SRP Tools Junctions	13	1		1
42	OMR - Radial Junction	14	1		1
43	OMR - Velachery Road Junction	14	1		1
44	Velachery Tambaram Road - Palikarnai Junction	14	1		1
45	ECR	14	1		1
46	Madipakkam Medavakam Road	14	1	1	
47	TBD	15	1	1	
48	TBD	15	1	1	
	<b>Total</b>		<b>50</b>	<b>17</b>	<b>33</b>

**Request for Proposal for selection of System Integrator to “Design, Supply, Implement, Commission, Operate & Manage the Command & Control Centre” as a part of Smart City Solutions for Chennai City.**

**Volume 3: Master Service Agreement  
RfP No. S.P.D.C.No.B1/100/2016**



L I V A B I L I T Y I N D E X



## Table of Contents

<b>A. General Conditions of Contract (GCC)</b> .....	<b>4</b>
1. Definition of Terms .....	4
2. Interpretation .....	6
3. Conditions Precedent .....	6
4. Scope of work.....	7
5. Key Performance Measurements .....	7
6. Commencement and Progress .....	8
7. Standards of performance .....	8
8. Approvals and Required Consents .....	9
9. Constitution of Consortium .....	9
10. Bidder's Obligations .....	10
11. Authority's Obligations.....	17
12. Payments .....	18
13. Intellectual Property Rights.....	18
14. Taxes .....	19
15. Indemnity .....	20
16. Warranty.....	21
17. Term and Extension of the Contract .....	22
18. Dispute Resolution.....	22
19. Time is of the essence.....	24
20. Conflict of interest.....	24
21. Publicity.....	24
22. Force Majeure .....	24
23. Delivery .....	25
24. Insurance.....	25
25. Transfer of Ownership.....	27
26. Exit Management Plan .....	27
<b>B. SPECIAL CONDITIONS OF CONTRACT (SCC)</b> .....	<b>29</b>
27. Performance Security .....	29
28. Limitation of Liability: .....	29
29. Ownership and Retention of Documents.....	30
30. Information Security .....	30
31. Records of contract documents.....	31
32. Security and Safety.....	31
33. Confidentiality .....	32
34. Events of Default by SI .....	32
35. Termination .....	33
36. Consequence of Termination .....	34

37. Change Control Note (CCN) .....	35
C. SERVICE LEVELS .....	37
38. Purpose.....	37
39. Service Level Agreements & Targets .....	37
40. General principles of Service Level Agreements .....	37
41. Reporting Procedures.....	43
42. Issue Management Procedures .....	43
43. Service Level Change Control .....	44
D. ANNEXURES .....	46

## A. General Conditions of Contract (GCC)

### 1. Definition of Terms

- 1.1. **"Acceptance of System"** The system shall be deemed to have been accepted by the Authority, subsequent to its installation, rollout and deployment of trained manpower, when all the activities as defined in Scope of Work have been successfully executed and completed to the satisfaction of Authority. Refer to Section 5 of the RfP Volume II.
- 1.2. **"Applicable Law(s)"** Any statute, law, ordinance, notification, rule, regulation, judgment, order, decree, bye-law, approval, directive, guideline, policy, requirement or other governmental restriction or any similar form of decision applicable to the relevant party and as may be in effect on the date of the execution of this Agreement and during the subsistence thereof, applicable to the Project.
- 1.3. **"Authority"** means Greater Chennai Corporation /Chennai Smart City Limited. The project shall be executed in Greater Chennai and shall be owned by Greater Chennai Corporation /Chennai Smart City Limited.
- 1.4. **"Bidder"** shall mean organization/consortium submitting the proposal in response to this RfP.
- 1.5. **"SI"** means the bidder who is selected by the Authority at the end of this RfP process. The agency shall carry out all the services mentioned in the scope of work of this RfP.
- 1.6. **"Contract"** means the Contract entered into by the parties with the entire documentation specified in the RfP.
- 1.7. **"Contract Value"** means the price payable to SI under this Contract for the full and proper performance of its contractual obligations.
- 1.8. **"Commercial Off-The-Shelf (COTS)"** refers to software products that are ready-made and available for sale, lease, or license to the general public.
- 1.9. **"Data Centre Site"** means the Data Centre sites including their respective Data Centre space, wherein the delivery, installation, integration, management and maintenance services as specified under the scope of work are to be carried out for the purpose of this contract.
- 1.10. **"Document"** means any embodiment of any text or image however recorded and includes any data, text, images, sound, voice, codes, databases or any other electronic documents as per IT Act 2000.
- 1.11. **"Effective Date"** means the date on which this Contract is signed or LoA is issued by Authority, whichever is earlier and executed by the parties hereto. If this Contract is executed in parts, then the date on which the last of such Contracts is executed shall be construed to be the Effective Date.

- 1.12. **"GCC"** means General Conditions of Contract
- 1.13. **"Goods"** means all of the equipment, sub-systems, hardware, software, products accessories, software and/or other material/items which SI is required to supply, install and maintain under the contract.
- 1.14. **"[ULB HO]"** means the Greater Chennai Corporation Head Office wherein the Command and Control Centre will be located
- 1.15. Deleted
- 1.16. "Deleted"
- 1.17. **"CCC"** means **Command and Control Centre**.
- 1.18. **"Intellectual Property Rights"** means any patent, copyright, trademark, tradename, service marks, brands, proprietary information whether arising before or after the execution of this Contract and the right to ownership and registration of these rights.
- 1.19. **"Go- Live"** means commissioning of project after laying of optical fiber for Greater Chennai, installation and commencement of all smart city components, including training as per scope of work mentioned in RfP. Bidder should have the approval from Authority for user acceptance testing.
- 1.20. **"Notice"** means: a notice; or a consent, approval or other communication required to be in writing under this Contract.
- 1.21. **"OEM"** means the **Original Equipment Manufacturer of any equipment/system/software/product** which are providing such goods to the Authority under the scope of this RfP.
- 1.22. **"SI's Team"** means SI who has to provide goods & services to the Authority under the scope of this Contract. This definition shall also include any and/or all of the employees of SI, authorized service providers/partners and representatives or other personnel employed or engaged either directly or indirectly by SI for the purposes of this Contract.
- 1.23. **"Consortium"** means the entity named in the contract for any part of the work has been sublet with the consent in writing of the Authority and the heirs, legal representatives, successors and assignees of such person.
- 1.24. **"Replacement Service Provider"** means the organization replacing SI in case of contract termination for any reasons
- 1.25. **"Sub-Contractor"** shall mean the entity named in the contract for any part of the work or any person to whom any part of the contract has been sublet with the consent in writing of the Authority and the heirs, legal representatives, successors and assignees of such person.
- 1.26. **"SCC"** means Special Conditions of Contract.

- 1.27. **“Services”** means the work to be performed by the agency pursuant to this RfP and to the contract to be signed by the parties in pursuance of any specific assignment awarded by the Authority.
- 1.28. **“Server Room”** or **“Data Centre”** shall have the same meaning.

## **2. Interpretation**

- 2.1.** In this Contract unless a contrary intention is evident:
- a. the clause headings are for convenient reference only and do not form part of this Contract;
  - b. unless otherwise specified a reference to a clause number is a reference to all of its sub-clauses;
  - c. the word “include” or “including” shall be deemed to be followed by “without limitation” or “but not limited to” whether or not they are followed by such phrases;
  - d. unless otherwise specified a reference to a clause, sub-clause or section is a reference to a clause, sub-clause or section of this Contract including any amendments or modifications to the same from time to time;
  - e. a word in the singular includes the plural and a word in the plural includes the singular;
  - f. a word importing a gender includes any other gender;
  - g. a reference to a person includes a partnership and a body corporate;
  - h. a reference to legislation includes legislation repealing, replacing or amending that legislation;
  - i. Where a word or phrase is given a particular meaning it includes the appropriate grammatical forms of that word or phrase which have corresponding meanings.
  - j. In the event of an inconsistency between the terms of this Contract and the RfP and the Bid, the terms hereof shall prevail.

## **3. Conditions Precedent**

This Contract is subject to the fulfillment of the following conditions precedent by SI.

- 3.1.** Furnishing by SI, an unconditional and irrevocable Performance Bank Guarantee (PBG) (Annexure 5 (a) of the RfP Volume I) and acceptable to the Authority which would remain valid until such time as stipulated by the Authority.
- 3.2.** Obtaining of all statutory and other approvals required for the performance of the Services under this Contract. This may include approvals/clearances, wherever applicable, that may be required for execution of this contract e.g. clearances from Government authorities for importing equipment, exemption of Tax/Duties/Levies, work permits/clearances for Bidder/Bidder’s team, etc.
- 3.3.** Furnish notarized copies of any/all contract(s) duly executed by SI and its OEMs existing at the time of signing of this contract in relation to the Authority’s project.

Failure to do so within stipulated time of signing of contract would attract penalty as defined in clause 42 in this Section.

- 3.4. Furnishing of such other documents as the Authority may specify/demand.
- 3.5. The Authority reserves the right to waive any or all of the conditions specified in Clause 3 above in writing and no such waiver shall affect or impair any right, power or remedy that the Authority may otherwise have.
- 3.6. In the event that any of the conditions set forth in Clause 3 hereinabove are not fulfilled within a month from the date of this Contract, or such later date as may be mutually agreed upon by the parties, the Authority may terminate this Contract.
- 3.7. In case there is a contradiction between the sections, the below hierarchy of sections in order of precedence:
  1. Pre-bid clarification and Corrigendum, if any
  2. Volume 3 of RfP
  3. Section 1 and 2 of RfP volume II
  4. Section 4 and Annexure of RfP volume II
  5. RfP volume I

#### **4. Scope of work**

- 4.1. Scope of the work shall be as defined in **RfP Volume II** and Annexures thereto of the tender.
- 4.2. Authority has engaged SI to provide services related to implementation of ChennaiSmart City solutions using which the Authority intends to perform its business operations. SI is required to provide such goods, services and support as the Authority may deem proper and necessary, during the term of this Contract, and includes all such processes and activities which are consistent with the proposals set forth in the Bid, the Tender and this Contract and are deemed necessary by the Authority, in order to meet its business requirements (hereinafter 'scope of work').

#### **5. Key Performance Measurements**

- 5.1. Unless specified by the Authority to the contrary, SI shall deliver the goods, perform the services and carry out the scope of work in accordance with the terms of this Contract, Scope of Work and the Service Specifications as laid down under Section C (Service Level Agreement) of this section.
- 5.2. If the Contract, scheduled requirements, service specification includes more than one document, then unless the Authority specifies to the contrary, the later in time shall prevail over a document of earlier date to the extent of any inconsistency.



- 5.3. The Authority reserves the right to amend any of the terms and conditions in relation to the Contract/Service Specifications and may issue any such directions which are not necessarily stipulated therein if it deems necessary for the fulfilment of the Schedule of Requirements.

## **6. Commencement and Progress**

- 6.1. SI shall subject to the fulfillment of the conditions precedent above, commence the performance of its obligations in a manner as per the Scope of Work (RfP Volume II).
- 6.2. SI shall proceed to carry out the activities/services with diligence and expedition in accordance with any stipulation as to the time, manner, mode, and method of execution contained in this Contract.
- 6.3. SI shall be responsible for and shall ensure that all activities/services are performed in accordance with the Contract, Scope of Work and Service Specifications and that SI's Team complies with such Specifications and all other standards, terms and other stipulations/conditions set out hereunder.
- 6.4. SI shall perform the activities/services and carry out its obligations under the Contract with due diligence, efficiency and economy, in accordance with generally accepted techniques and practices used in the industry and shall observe sound management, engineering and security practices. SI shall always act, in respect of any matter relating to this Contract, as faithful advisors to the Authority and shall, at all times, support and safeguard the Authority's legitimate interests in any dealings with Third parties.

## **7. Standards of performance**

- 7.1. SI shall perform the Services and carry out its obligations under the Contract with due diligence, efficiency and economy, in accordance with generally accepted techniques and best practices used in the industry and with IT standards recognized by international professional bodies and shall observe sound management, engineering and security practices. It shall employ appropriate advanced technology and engineering practices and safe and effective equipment, machinery, material and methods. SI shall always act, in respect of any matter relating to the Contract, as faithful advisors to the Authority and shall, at all times, support and safeguard the Authority's legitimate interests in any dealings with Third Parties.

## **8. Approvals and Required Consents**

- 8.1.** The Authority shall extend necessary support to SI to obtain, maintain and observe all relevant and customary regulatory and governmental licenses, clearances and applicable approvals (hereinafter the "Approvals") necessary for SI to provide the Services. The costs of such Approvals shall be borne by SI. Both parties shall give each other all co-operation and information reasonably.
- 8.2.** The Authority shall also provide necessary support to Bidder in obtaining the Approvals. In the event that any Approval is not obtained, SI and the Authority shall co-operate with each other in achieving a reasonable alternative arrangement as soon as reasonably practicable for the Authority, to continue to process its work with as minimal interruption to its business operations as is commercially reasonable until such Approval is obtained, provided that SI shall not be relieved of its obligations to provide the Services and to achieve the Service Levels until the Approvals are obtained if and to the extent that SI 's obligations are dependent upon such Approvals.

## **9. Constitution of Consortium**

- 9.1.** For the purposes of fulfillment of its obligations as laid down under the Contract, where the Authority deems fit and unless the contract requires otherwise, Prime Bidder shall be the sole point of interface for the Authority and would be absolutely accountable for the performance of its own, the other member of Consortium and/or its Team's functions and obligations.
- 9.2.** The Consortium member has agreed that SI is the prime point of contact between the Consortium member and the Authority and it shall be primarily responsible for the discharge and administration of all the obligations contained herein and, the Authority, unless it deems necessary shall deal only with SI. SI along with all consortium members shall be jointly and solely responsible for the project execution
- 9.3.** Without prejudice to the obligation of the Consortium member to adhere to and comply with the terms of this Contract, the Consortium member has executed and submitted a Power of Attorney in favor of SI authorizing him to act for and on behalf of such member of the Consortium and do all acts as may be necessary for fulfillment of contractual obligations.
- 9.4.** The Authority reserves the right to review, approve and require amendment of the terms of the Consortium Contract or any contract or agreements entered into by and between the members of such Consortium and no such agreement/contract shall be executed, amended, modified and/or terminated without the prior written consent of the Authority. An executed copy of each of such agreements/contracts shall, immediately upon execution be submitted by SI to the Authority.

- 9.5. Where, during the term of this Contract, SI terminates any contract/arrangement or agreement relating to the performance of Services, SI shall be responsible and severally liable for any consequences resulting from such termination. SI shall in such case ensure the smooth continuation of Services by providing a suitable replacement to the satisfaction of the Authority at no additional charge and at the earliest opportunity.

## 10. Bidder's Obligations

- 10.1. SI's obligations shall include all the activities as specified by the Authority in the Scope of Work and other sections of the Tender and Contract and changes thereof to enable Authority to meet the objectives and operational requirements. It shall be SI's responsibility to ensure the proper and successful implementation, performance and continued operation of the proposed solution in accordance with and in strict adherence to the terms of his Bid, the Tender and this Contract.
- 10.2. In addition to the aforementioned, SI shall provide services to manage and maintain the said system and infrastructure as mentioned in Section 1 of RfP Volume II
- 10.3. Authority reserves the right to interview the personnel proposed that shall be deployed as part of the project team. If found unsuitable, the Authority may reject the deployment of the personnel. But ultimate responsibility of the project implementation shall lie with SI.
- 10.4. Authority reserves the right to require changes in personnel which shall be communicated to SI. SI with the prior approval of the Authority may make additions to the project team. SI shall provide the Authority with the resume of Key Personnel and provide such other information as the Authority may reasonably require. The Authority also reserves the right to interview the personnel and reject, if found unsuitable. In case of change in its team members, for any reason whatsoever, SI shall also ensure that the exiting members are replaced with at least equally qualified and professionally competent members.
- 10.5. SI shall ensure that none of the Key Personnel (refer Section 3.7.1 of the RfP Volume I proposed) and manpower exit from the project during first 6 months of the beginning of the project. In such cases of exit, a penalty of INR 2 lakhs per such replacement shall be imposed on SI.
- 10.6. SI should submit profiles of only those resources who shall be deployed on the project. Any change of resource should be approved by the Authority and compensated with equivalent or better resource. The Authority may interview the resources suggested by SI before their deployment on board. It does not apply in case of change requested by the Authority.
- 10.7. In case of change in its team members, SI shall ensure a reasonable amount of time overlap in activities to ensure proper knowledge transfer and handover/takeover of documents and other relevant materials between the outgoing and the new member.

- 10.8.** SI shall ensure that SI's Team is competent, professional and possesses the requisite qualifications and experience appropriate to the task they are required to perform under this Contract. SI shall ensure that the services are performed through the efforts of SI's Team, in accordance with the terms hereof and to the satisfaction of the Authority. Nothing in this Contract relieves SI from its liabilities or obligations under this Contract to provide the Services in accordance with the Authority's directions and requirements and as stated in this Contract and the Bid to the extent accepted by the Authority and SI shall be liable for any non-performance, non-compliance, breach or other loss and damage resulting either directly or indirectly by or on account of its Team.
- 10.9.** SI shall be fully responsible for deployment/installation/development and integration of all the software and hardware components and resolve any problems/issues that may arise due to integration of components.
- 10.10.** SI shall ensure that the OEMs supply equipment/components including associated accessories and software required and shall support SI in the installation, commissioning, integration and maintenance of these components during the entire period of contract. SI shall ensure that the COTS OEMs supply the software applications and shall support SI in the installation/deployment, integration, roll-out and maintenance of these applications during the entire period of contract. It must clearly be understood by SI that warranty and O&M of the system, products and services incorporated as part of system would commence from the day of Go-Live of system as a complete Smart city solution including all the solutions proposed. SI would be required to explicitly display that he/they have a back to back arrangement for provisioning of warranty/O&M support till the end of contract period with the relevant OEMs. The annual maintenance support shall include patches and updates the software, hardware components and other devices.
- 10.11.** All the software licenses that SI proposes should be perpetual software licenses. The software licenses shall not be restricted based on location and the Authority should have the flexibility to use the software licenses for other requirements if required.
- 10.12.** All the OEMs that Bidder proposes should have Dealer possession licenses.
- 10.13.** The Authority reserves the right to review the terms of the Warranty and Annual Maintenance agreements entered into between SI and OEMs and no such agreement/contract shall be executed, amended, modified and/or terminated without the prior written consent of the Authority. An executed copy of each of such agreements/contracts shall, immediately upon execution be submitted by SI to the Authority.
- 10.14.** SI shall ensure that none of the components and sub-components is declared end-of-sale or end-of-support by the respective OEM at the time of submission of bid. If the OEM declares any of the products/solutions end-of-sale subsequently, the SI shall ensure that the same is supported by the respective OEM for contract period.

- 10.15.** If a product is de-supported by the OEM for any reason whatsoever, from the date of Acceptance of the System till the end of contract, SI should replace the products/solutions with an alternate that is acceptable to the Authority at no additional cost to the Authority and without causing any performance degradation.
- 10.16.** The Licenses will be in the name of Authority only.
- 10.17.** SI shall ensure that the OEMs provide the support and assistance to SI in case of any problems/issues arising due to integration of components supplied by him with any other component(s)/product(s) under the purview of the overall solution. If the same is not resolved for any reason whatsoever, SI shall replace the required component(s) with an equivalent or better substitute that is acceptable to Authority without any additional cost to the Authority and without impacting the performance of the solution in any manner whatsoever.
- 10.18.** SI shall ensure that the OEMs for hardware servers/equipment supply and/or install all type of updates, patches, fixes and/or bug fixes for the firmware or software from time to time at no additional cost to the Authority.
- 10.19.** SI shall ensure that the OEMs for hardware servers/equipment or Bidder's trained engineers conduct the preventive maintenance on a Quarterly basis and break-fix maintenance in accordance with the best practices followed in the industry. SI shall ensure that the documentation and training services associated with the components shall be provided by the OEM partner or OEM's certified training partner without any additional cost to the Authority.
- 10.20.** The training has to be conducted using official OEM course curriculum mapped with the hardware/Software Product's to be implemented in the project.
- 10.21.** SI and their personnel/representative shall not alter/change/replace any hardware component proprietary to the Authority and/or under warranty or O&M of third party without prior consent of the Authority.
- 10.22.** SI shall provision the required critical spares/components at the designated Datacenter Sites/office locations of the Authority for meeting the uptime commitment of the components supplied by him.
- 10.23.** SI's representative(s) shall have all the powers requisite for the execution of scope of work and performance of services under this contract. SI's representative(s) shall liaise with the Authority's representative for the proper coordination and timely completion of the works and on any other matters pertaining to the works. SI shall extend full co-operation to Authority's representative in the manner required by them for supervision/inspection/observation of the equipment/goods/material, procedures, performance, progress, reports and records pertaining to the works. He shall also have complete charge of SI's personnel engaged in the performance of the works and to ensure compliance of rules, regulations and safety practice. He shall also cooperate with the other Service Providers/Vendors of the Authority working at the Authority's office locations & field locations and DC & DR sites.

Such Bidder's representative(s) shall be available to the Authority's Representative at respective Datacenter during the execution of works.

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

**10.25.** SI is expected to set up a project office in Chennai City. The technical manpower deployed on the project should work from the same office. However, some resources may be required to work from the client office during the contract period.

**10.26. Access to Sites**

**10.26.1.** Sites would include Server Room, Command and Communications Centre

**10.26.2.** The Authority's representative upon receipt of request from SI intimating commencement of activities at various locations shall give to SI access to as much of the Sites as may be necessary to enable SI to commence and proceed with the installation of the works in accordance with the program of work. Any reasonable proposal of SI for access to Site to proceed with the installation of work in accordance with the program of work shall be considered for approval and shall not be unreasonably withheld by the Authority. Such requests shall be made to the Authority's representative in writing at least 7 days prior to start of the work.

**10.26.3.** At the site locations, the Authority's representative shall give to SI access to as much as may be necessary to enable SI to commence and proceed with the installation of the works in accordance with the program of work or for performance of Facilities Management Services.

**10.27. Start of Installation**

**10.27.1.** Bidder shall co-ordinate with the Authority and stakeholders for the complete setup of sites before commencement of installation of other areas as mentioned in Section 5: of the RFP Volume II document.

**10.27.2.** As per TRAI guidelines, resale of bandwidth connectivity is not allowed. In such a case tripartite agreement should be formed between Authority, selected Bidder and Internet Service Provider(s).

**10.27.3.** The plan and design documents thus developed shall be submitted by SI for approval by the Authority.

**10.27.4.** After obtaining the approval from the Authority, SI shall commence the installation.

## **10.28. Reporting Progress**

- 10.28.1.** SI shall monitor progress of all the activities related to the execution of this contract and shall submit to the Authority, progress reports with reference to all related work, milestones and their progress during the implementation phase.
- 10.28.2.** Formats for all above mentioned reports and their dissemination mechanism shall be discussed and finalized along with project plan. The Authority on mutual agreement between both parties may change the formats, periodicity and dissemination mechanism for such reports.
- 10.28.3.** Periodic meetings shall be held between the representatives of the Authority and SI once in every 15 days during the implementation phase to discuss the progress of implementation. After the implementation phase is over, the meeting shall be held as an ongoing basis, as desired by Authority, to discuss the performance of the contract.
- 10.28.4.** SI shall ensure that the respective solution teams involved in the execution of work are part of such meetings.
- 10.28.5.** Several review committees involving representative of the Authority and senior officials of SI shall be formed for the purpose of this project. These committees shall meet at intervals, as decided by the Authority later, to oversee the progress of the implementation.
- 10.28.6.** All the goods, services and manpower to be provided/deployed by SI under the Contract and the manner and speed of execution and maintenance of the work and services are to be conducted in a manner to the satisfaction of Authority's representative in accordance with the Contract.
- 10.28.7.** The Authority reserves the right to inspect and monitor/assess the progress/performance of the work/services at any time during the course of the Contract. The Authority may demand and upon such demand being made, SI shall provide documents, data, material or any other information which the Authority may require, to enable it to assess the progress/performance of the work/service.
- 10.28.8.** At any time during the course of the Contract, the Authority shall also have the right to conduct, either itself or through another agency as it may deem fit, an audit to monitor the performance by SI of its obligations/functions in accordance with the standards committed to or required by the Authority and SI undertakes to cooperate with and provide to the Authority/any other agency appointed by the Authority, all Documents and other details as may be required by them for this purpose. Such audit shall not include Bidder's books of accounts.

- 10.28.9.** Should the rate of progress of the works or any part of them at any time fall behind the stipulated time for completion or is found to be too slow to ensure completion of the works by the stipulated time, or is in deviation to Tender requirements/standards, the Authority's representative shall so notify SI in writing.
- 10.28.10.** SI shall reply to the written notice giving details of the measures he proposes to take to expedite the progress so as to complete the works by the prescribed time or to ensure compliance to RfP requirements. SI shall not be entitled to any additional payment for taking such steps. If at any time it should appear to the Authority or Authority's representative that the actual progress of work does not conform to the approved plan SI shall produce at the request of the Authority's representative a revised plan showing the modification to the approved plan necessary to ensure completion of the works within the time for completion or steps initiated to ensure compliance to the stipulated requirements
- 10.28.11.** The submission seeking approval by the Authority or Authority's representative of such plan shall not relieve SI of any of his duties or responsibilities under the Contract.
- 10.28.12.** In case during execution of works, the progress falls behind schedule or does not meet the Tender requirements, SI shall deploy extra manpower/resources to make up the progress or to meet the RfP requirements. Plan for deployment of extra man power/resources shall be submitted to the Authority for its review and approval. All time and cost effect in this respect shall be borne, by SI within the contract value.

**10.29. Knowledge of Server Room, Command and Control Centre.**

- 10.29.1.** SI shall be granted access to the Server Room, Command and Control Centre, for inspection by the Authority before commencement of installation. The plan shall be drawn mutually at a later stage.
- 10.29.2. SI shall be deemed to have knowledge of the Server Room, Command and Control Centre, and its surroundings and information available in connection therewith and to have satisfied itself the form and nature thereof including, the data contained in the Bidding Documents, the physical and climatic conditions, the quantities and nature of the works and materials necessary for the completion of the works, the means of access, etc. and in general to have obtained itself all necessary information of all risks, contingencies and circumstances affecting his obligations and responsibilities therewith under the Contract and his ability to perform it. However, if during pre-installation survey/during delivery or installation, SI detects physical conditions and/or obstructions affecting the work, SI shall take all measures to overcome them.



### **10.30. Project Plan**

- 10.30.1.** Within 15 calendar days of effective date of the contract/Issuance of LoA, SI shall submit to the Authority for its approval a detailed Project Plan with details of the Project showing the sequence, procedure and method in which he proposes to carry out the works. The Plan so submitted by SI shall conform to the requirements and timelines specified in the Contract. The Authority and SI shall discuss and agree upon the work procedures to be followed for effective execution of the works, which SI intends to deploy and shall be clearly specified. The Project Plan shall include but not limited to project organization, communication structure, proposed staffing, roles and responsibilities, processes and tool sets to be used for quality assurance, security and confidentiality practices in accordance with industry best practices, project plan and delivery schedule in accordance with the Contract. Approval by the Authority's Representative of the Project Plan shall not relieve SI of any of his duties or responsibilities under the Contract.
- 10.30.2.** If SI's work plans necessitate a disruption/shutdown in Authority's operation, the plan shall be mutually discussed and developed so as to keep such disruption/shutdown to the barest unavoidable minimum. Any time and cost arising due to failure of SI to develop/adhere such a work plan shall be to his account.

### **10.31. Adherence to safety procedures, rules regulations and restriction**

- 10.31.1.** SI's Team shall comply with the provision of all laws including labor laws, rules, regulations and notifications issued there under from time to time. All safety and labor laws enforced by statutory agencies and by Authority shall be applicable in the performance of this Contract and Bidder's Team shall abide by these laws.
- 10.31.2.** Access to the Server Room, Command and Communications Centre shall be strictly restricted. No access to any person except the essential members of SI's Team who are authorized by the Authority and are genuinely required for execution of work or for carrying out management/maintenance shall be allowed entry. Even if allowed, access shall be restricted to the pertaining equipment of the Authority only. SI shall maintain a log of all activities carried out by each of its team personnel.
- 10.31.3.** No access to any staff of bidder, except the essential staff who has genuine work-related need, should be given. All such access should be logged in a loss free manner for permanent record with unique biometric identification of the staff to avoid misrepresentations or mistakes
- 10.31.4.** SI shall take all measures necessary or proper to protect the personnel, work and facilities and shall observe all reasonable safety rules and instructions. SI's Team shall adhere to all security

requirement/regulations of the Authority during the execution of the work. Authority's employee also shall comply with safety procedures/policy.

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

## **10.32. Statutory Requirements**

- 10.32.1. During the tenure of this Contract nothing shall be done by SI or his team including consortium in contravention of any law, act and/or rules/regulations, there under or any amendment thereof governing inter-alia customs, stowaways, foreign exchange etc. and shall keep Authority indemnified in this regard.

## **11. Authority's Obligations**

- 11.1.** Authority or his/her nominated representative shall act as the nodal point for implementation of the contract and for issuing necessary instructions, approvals, commissioning, acceptance certificates, payments etc. to SI.
- 11.2.** Authority shall ensure that timely approval is provided to SI as and when required, which may include approval of project plans, implementation methodology, design documents, specifications, or any other document necessary in fulfillment of this contract.
- 11.3.** The Authority's representative shall interface with SI, to provide the required information, clarifications, and to resolve any issues as may arise during the execution of the Contract. Authority shall provide adequate cooperation in providing details, coordinating and obtaining of approvals from various governmental agencies, in cases, where the intervention of the Authority is proper and necessary.
- 11.4.** Authority may provide on Bidder's request, particulars/information/or documentation that may be required by SI for proper planning and execution of work and for providing services covered under this contract and for which SI may have to coordinate with respective vendors.
- 11.5.** Authority shall provide to SI only sitting space and basic infrastructure not including, stationery and other consumables at the Authority's office locations.
- 11.6.** Authority reserves the right to procure the hardware including devices on quarterly basis in first year based on actual deployment and O&M shall be applicable whenever the devices are procured and deployed till end of the contract.
- 11.7. Site Not Ready:** Authority hereby agrees to make the project sites ready as per the agreed specifications, within the agreed timelines. Authority agrees that SI shall not be in any manner liable for any delay arising out of Authority's failure to make the site ready within the stipulated period.

## **12. Payments**

- 12.1.** Authority shall make payments to SI at the times and in the manner set out in the Payment schedule as specified Payment Milestones in RfP Volume II subject to the penalties as mentioned under Clause 42 of Section C- Service Levels of Volume 3. Authority shall make all efforts to make payments to SI within 45 days of receipt of invoice(s) and all necessary supporting documents.
- 12.2.** All payments agreed to be made by Authority to SI in accordance with the Bid shall be inclusive of all statutory levies, duties, taxes and other charges whenever levied/applicable, if any, and Authority shall not be liable to pay any such levies/other charges under or in relation to this Contract and/or the Services.
- 12.3.** No invoice for extra work/change order on account of change order shall be submitted by SI unless the said extra work/change order has been authorized/approved by the Authority in writing in accordance with Change Control Note (Annexure I of this section of the RfP)
- 12.4.** In the event of Authority noticing at any time that any amount has been disbursed wrongly to SI or any other amount is due from SI to the Authority, the Authority may without prejudice to its rights recover such amounts by other means after notifying SI or deduct such amount from any payment falling due to SI. The details of such recovery, if any, shall be intimated to SI. SI shall receive the payment of undisputed amount under subsequent invoice for any amount that has been omitted in previous invoice by mistake on the part of the Authority or SI.
- 12.5.** All payments to SI shall be subject to the deductions of tax at source under Income Tax Act, and other taxes and deductions as provided for under any law, rule or regulation. All costs, damages or expenses which Authority may have paid or incurred, for which under the provisions of the Contract, SI is liable, the same shall be deducted by Authority from any dues to SI. All payments to SI shall be made after making necessary deductions as per terms of the Contract and recoveries towards facilities, if any, provided by the Authority to SI on chargeable basis.

## **13. Intellectual Property Rights**

- 13.1.** Retention of Ownership except for the rights expressly granted to the Licensee under this Agreement, the Licensor shall retain all right, title and interest in and to the Licensed Technology, including all worldwide Technology and intellectual property and proprietary rights.
- 13.2.** Preservation of Notice Licensee shall not remove, efface or obscure any copyright notices or other proprietary notices or legends from any Licensed Technology or materials provided under this Agreement, and shall reproduce all such notices and legends when incorporating Licensed Technology or materials into any Integrated Products.

- 13.3.** SI must ensure that while using any software, hardware, processes, document or material in the course of performing the Services, it does not infringe the Intellectual Property Rights of any person/Company. SI shall keep the Authority indemnified against all costs, expenses and liabilities howsoever, arising out any illegal or unauthorized use (piracy) or in connection with any claim or proceedings relating to any breach or violation of any permission/license terms or infringement of any Intellectual Property Rights by SI or SI's Team during the course of performance of the Services. SI's liability is excluded regarding any claim based on any of the following (a) anything Authority provides which is incorporated into the Solution; (b) the Authority's modification of the solution; (c) the combination, operation, or use of the solution with other materials, if the third party claim has been caused by the combination, operation or use of the solution
- 13.4. Authority shall own and have a right in perpetuity to use all newly created Intellectual Property Rights which have been developed solely during execution of this Contract, including but not limited to all processes, products, specifications, reports and other documents which have been newly created and developed by SI solely during the performance of Services and for the purposes of inter-alia use or sub-license of such Services under this Contract. SI undertakes to disclose all such Intellectual Property Rights arising in performance of the Services to the Authority, execute all such agreements/documents and obtain all permits and approvals that may be necessary in regard to the Intellectual Property Rights of the Authority.
- 13.5.** If Authority desires, SI shall be obliged to ensure that all approvals, registrations, licenses, permits and rights etc. which are inter-alia necessary for use of the goods supplied/installed by SI, the same shall be acquired in the name of the Authority, prior to termination of this Contract and which may be assigned by the Authority to SI for the purpose of execution of any of its obligations under the terms of the Bid, Tender or this Contract. However, subsequent to the term of this Contract, such approvals, registrations, licenses, permits and rights etc. shall endure to the exclusive benefit of the Authority.
- 13.6.** SI shall not copy, reproduce, translate, adapt, vary, modify, disassemble, decompile or reverse engineer or otherwise deal with or cause to reduce the value of the Materials except as expressly authorized by Authority in writing

## **14. Taxes**

- 14.1.** SI shall bear all personnel taxes levied or imposed on its personnel, or any other member of SI's Team, etc. on account of payment received under this Contract. SI shall bear all corporate taxes, levied or imposed on SI on account of payments received by it from the Authority for the work done under this Contract.
- 14.2.** SI shall bear all taxes and duties etc. levied or imposed on SI under the Contract including but not limited to Sales Tax, Customs duty, Excise duty, Octroi, Service Tax, VAT, Works Contracts Tax and all Income Tax levied under Indian Income Tax Act – 1961 or any amendment thereof during the entire contract period, i.e., on account of material supplied and services rendered and payments received by

him from the Authority under the Contract. It shall be the responsibility of SI to submit to the concerned Indian authorities the returns and all other connected documents required for this purpose. SI shall also provide the Authority such information, as it may be required in regard to SI's details of payment made by the Authority under the Contract for proper assessment of taxes and duties. The amount of tax withheld by the Authority shall at all times be in accordance with Indian Tax Law and the Authority shall promptly furnish to SI original certificates for tax deduction at source and paid to the Tax Authorities.

- 14.3.** SI agrees that he shall comply with the Indian Income Tax Act in force from time to time and pay Indian Income Tax, as may be imposed/levied on them by the Indian Income Tax Authorities, for the payments received by them for the works under the Contract
- 14.4.** SIs shall fully familiarize themselves about the applicable domestic taxes (such as value added or sales tax, service tax, income taxes, duties, fees, levies, etc.) on amounts payable by the Authority under the Agreement. All such taxes must be included by Bidders in the financial proposal. (Bidder to find out applicable taxes for the components being proposed.)
- 14.5.** Should SI fail to submit returns/pay taxes in times as stipulated under applicable Indian/State Tax Laws and consequently any interest or penalty is imposed by the concerned authority, SI shall pay the same. SI shall indemnify Authority against any and all liabilities or claims arising out of this Contract for such taxes including interest and penalty by any such Tax Authority may assess or levy against the Authority/Prime Bidder.
- 14.6.** Supplies of materials from abroad are exempted from levy of Sales Tax/VAT on works/works Contract tax (Central or state). However, the Sales Tax/VAT on works (central or state) if levied on supplies made from indigenous vendors for the works shall be borne by SI within the Contract Price. Service Tax/Terminal Sales Tax/Works Contract Tax, etc., if any applicable, shall be payable extra, at actuals by the Authority in accordance with the conditions of the Contract and upon submission of proof of payment of such taxes.
- 14.7.** The Authority shall if so required by applicable laws in force, at the time of payment, deduct income tax payable by SI at the rates in force, from the amount due to SI and pay to the concerned tax authority directly.

## **15. Indemnity**

- 15.1.** SI shall indemnify the Authority from and against any costs, loss, damages, expense, claims including those from third parties or liabilities of any kind howsoever suffered, arising or incurred inter alia during and after the Contract period out of:
  - a. any negligence or wrongful act or omission by SI or any third party associated with SI in connection with or incidental to this Contract; or

- b. any breach of any of the terms of SI's bid as agreed, the RfP and this Contract by SI
  - c. any infringement of patent, trademark/copyright or industrial design rights arising from the use of the supplied goods and related services or any part thereof
- 15.2.** SI shall also indemnify the Authority against any privilege, claim or assertion made by a third party with respect to right or interest in, ownership, mortgage or disposal of any asset, property etc.
- 15.3.** Regardless of anything contained (except for SI's liability for bodily injury and/or damage to tangible and real property for which it is legally liable and its liability for patent and copyright infringement in accordance with the terms of this Agreement) the total liability of SI, is restricted to the total value of the contract and SI is not responsible for any third party claims.

## **16. Warranty**

- 16.1.** A comprehensive warranty applicable on goods supplied under this contract shall be provided for the period of contract from the date of acceptance of respective system by the Authority.
- 16.2.** Technical Support for Software applications shall be provided by the respective OEMs for the period of contract. The Technical Support should include all upgrades, updates and patches to the respective Software applications.
- 16.3.** The SI warrants that the Goods supplied under the Contract are new, non-refurbished, unused and recently manufactured; shall not be nearing End of sale/End of support; and shall be supported by the SI and respective OEM along with service and spares support to ensure its efficient and effective operation for the entire duration of the contract.
- 16.4.** The SI warrants that the goods supplied under this contract shall be of the highest grade and quality and consisted with the established and generally accepted standards for materials of this type. The goods shall be in full conformity with the specifications and shall operate properly and safely. All recent design improvements in goods, unless provided otherwise in the Contract, shall also be made available.
- 16.5.** The SI further warrants that the Goods supplied under this Contract shall be free from all encumbrances and defects/faults arising from design, material, manufacture or workmanship (except insofar as the design or material is required by the Authority's Specifications) or from any act or omission of the SI, that may develop under normal use of the supplied Goods in the conditions prevailing at the respective Datacenter/Server Room Sites.
- 16.6.** The Authority shall promptly notify the SI in writing of any claims arising under this warranty.

- 16.7. Upon receipt of such notice, the SI shall, with all reasonable speed, repair or replace the defective Goods or parts thereof, without prejudice to any other rights which the Authority may have against the SI under the Contract.
- 16.8. If the SI, having been notified, fails to remedy the defect(s) within a reasonable period, the Authority may proceed to take such remedial action as may be necessary, at the SI's risk and expense and without prejudice to any other rights which the Authority may have against the SI under the Contract.
- 16.9. Any OEM specific warranty terms that do not conform to conditions under this Contract shall not be acceptable.

## 17. Term and Extension of the Contract

- 17.1. The Contract period shall commence from the date of signing of contract or Issuance of LoA, whichever is earlier, and shall remain valid for 60 Months from the date of Go Live of the system.
- 17.2. If the delay occurs due to circumstances beyond control of SI such as strikes, lockouts, fire, accident, defective materials, delay in approvals or any cause whatsoever beyond the reasonable control of SI, a reasonable extension of time shall be granted by the Authority.
- 17.3. The Authority shall reserve the sole right to grant any extension to the term abovementioned and shall notify in writing to SI, at least 3 (three) months before the expiration of the Term hereof, whether it shall grant SI an extension of the Term. The decision to grant or refuse the extension shall be at the Authority's discretion and such extension of the contract, if any, shall be as per terms agreed mutually between the Authority and SI.
- 17.4. Where the Authority is of the view that no further extension of the term be granted to SI, the Authority shall notify SI of its decision at least 3 (three) months prior to the expiry of the Term. Upon receipt of such notice, SI shall continue to perform all its obligations hereunder, until such reasonable time beyond the Term of the Contract within which, the Authority shall either appoint an alternative agency/SI or create its own infrastructure to operate such Services as are provided under this Contract.

## 18. Dispute Resolution

- 18.1. In case, a dispute is referred to arbitration, the arbitration shall be under the **Indian Arbitration and Conciliation Act, 1996** and any statutory modification or re-enactment thereof.
- 18.2. If during the subsistence of this Contract or thereafter, any dispute between the Parties hereto arising out of or in connection with the validity, interpretation, implementation, material breach or any alleged material breach of any provision of this Contract or regarding any question, including as to whether the

termination of this Contract by one Party hereto has been legitimate, the Parties hereto shall endeavor to settle such dispute amicably and/or by Conciliation to be governed by the Arbitration and Conciliation Act, 1996 or as may be agreed to between the Parties. The attempt to bring about an amicable settlement is considered to have failed as soon as one of the Parties hereto, after reasonable attempts; which attempt shall continue for not less than thirty (30) days, gives thirty (30) day notice to refer the dispute to arbitration to the other Party in writing.

- 18.3.** The Arbitration proceedings shall be governed by the Arbitration and Conciliation Act, 1996.
- 18.4.** The Arbitration proceedings shall be held in Chennai, Tamilnadu State, India.
- 18.5.** The Arbitration proceeding shall be governed by the substantive laws of India.
- 18.6.** The proceedings of Arbitration shall be in English language.
- 18.7.** Except as otherwise provided elsewhere in the contract if any dispute, difference, question or disagreement arises between the parties hereto or their respective representatives or assignees, at any time in connection with construction, meaning, operation, effect, interpretation or out of the contract or breach thereof the same shall be referred to a Tribunal of three (3) Arbitrators, constituted as per the terms of and under the (Indian) Arbitration and Conciliation Act, 1996. Each party to the contract shall appoint/nominate one Arbitrator each, the two Arbitrators so appointed/nominated by the Parties herein shall together choose the third Arbitrator, who shall be the Presiding Arbitrator of the Tribunal. The consortium of the three Arbitrators shall form the Arbitral Tribunal.
- 18.8.** In case, a party fails to appoint an arbitrator within 30 days from the receipt of the request to do so by the other party or the two Arbitrators so appointed fail to agree on the appointment of third Arbitrator within 30 days from the date of their appointment upon request of a party, the Chief Justice of the Tamilnadu High Court or any person or institution designated by him shall appoint the Arbitrator/Presiding Arbitrator upon request of one of the parties.
- 18.9.** Any letter, notice or other communications dispatched to SI relating to either arbitration proceeding or otherwise whether through the post or through a representative on the address last notified to the Authority by SI shall be deemed to have been received by SI although returned with the remarks, refused 'undelivered' where about not known or words to that effect or for any other reasons whatsoever
- 18.10.** If the Arbitrator so appointed dies, resigns, incapacitated or withdraws for any reason from the proceedings, it shall be lawful for the Authority to appoint another person in his place in the same manner as aforesaid. Such person shall proceed with the reference from the stage where his predecessor had left if both parties consent for the same; otherwise, he shall proceed de novo.



**18.11.** It is a term of the contract that the party invoking arbitration shall specify all disputes to be referred to arbitration at the time of invocation of arbitration and not thereafter.

**18.12.** It is also a term of the contract that neither party to the contract shall be entitled for any interest on the amount of the award.

**18.13.** The Arbitrator shall give reasoned award and the same shall be final, conclusive and binding on the parties.

**18.14.** The fees of the arbitrator, costs and other expenses incidental to the arbitration proceedings shall be borne equally by the parties.

## **19. Time is of the essence**

**19.1.** Time shall be of the essence in respect of any date or period specified in this Contract or any notice, demand or other communication served under or pursuant to any provision of this Contract and in particular in respect of the completion of the activities by SI by the specified completion date.

## **20. Conflict of interest**

**20.1.** SI shall disclose to the Authority in writing, all actual and potential conflicts of interest that exist, arise or may arise (either for SI or SI's Team) in the course of performing the Services as soon as practical after it becomes aware of that conflict.

## **21. Publicity**

**21.1.** SI shall not make or permit to be made a public announcement or media release about any aspect of this Contract unless the Authority first gives SI its written consent.

## **22. Force Majeure**

**22.1.** Force Majeure shall not include any events caused due to acts/omissions of SI resulting in a breach/contravention of any of the terms of the Contract and/or SI's Bid. It shall also not include any default on the part of SI due to its negligence or failure to implement the stipulated/proposed precautions, as were required to be taken under the Contract.

**22.2.** The failure or occurrence of a delay in performance of any of the obligations of either party shall constitute a Force Majeure event only where such failure or delay could not have reasonably been foreseen i.e. war, or hostility, acts of the public enemy, civil commotion, sabotage, fires, floods, explosions, epidemics, quarantine restriction, strikes, lockouts or act of God (hereinafter referred to as events) , or where despite the presence of adequate and stipulated safeguards the

failure to perform obligations has occurred at any location in scope. In such an event, the affected party shall inform the other party in writing within five days of the occurrence of such event. Any failure or lapse on the part of SI in performing any obligation as is necessary and proper, to negate the damage due to projected force majeure events or to mitigate the damage that may be caused due to the above mentioned events or the failure to provide adequate disaster management/recovery or any failure in setting up a contingency mechanism would not constitute force majeure, as set out above.

- 22.3.** In case of a Force Majeure, all Parties shall endeavor to agree on an alternate mode of performance in order to ensure the continuity of service and implementation of the obligations of a party under the Contract and to minimize any adverse consequences of Force Majeure.

## **23. Delivery**

- 23.1.** SI shall bear the cost for packing, transport, insurance, storage and delivery of all the goods for "Selection of agency for implementation of Chennai Smart City" at all locations identified by the Authority in Chennai.
- 23.2.** The Goods and manpower supplied under this Contract shall conform to the standards mentioned in the RfP, and, when no applicable standard is mentioned, to the authoritative standards; such standard shall be approved by Authority.
- 23.3.** SI shall only procure the hardware and software after approvals from a designated Committee/Authority.

## **24. Insurance**

- 24.1.** The Goods supplied under this Contract shall be comprehensively insured by SI at his own cost, against any loss or damage, for the entire period of the contract. SI shall submit to the Authority, documentary evidence issued by the insurance company, indicating that such insurance has been taken.
- 24.2.** SI shall bear all the statutory levies like customs, insurance, freight, etc. applicable on the goods and also the charges like transportation charges, octroi, etc. that may be applicable till the goods are delivered at the respective sites of installation shall also be borne by SI.
- 24.3.** SI shall take out and maintain at its own cost, on terms and conditions approved by the Authority, insurance against the risks, and for the coverage's, as specified below;
- a. At the Authority's request, shall provide evidence to the Authority showing that such insurance has been taken out and maintained and that the current premiums therefore have been paid.
  - b. Employer's liability and workers' compensation insurance in respect of the Personnel of the Company, in accordance with the relevant provisions of the

Applicable Law, as well as, with respect to such Personnel, any such life, health, accident, travel or other insurance as may be appropriate

## **25. Transfer of Ownership**

- 25.1.** SI must transfer all titles to the assets and goods procured for the purpose of the project to the Authority at the time of Acceptance of System. This includes all licenses, titles, source code, certificates, hardware, devices, equipment's etc. related to the system designed, developed, installed and maintained by SI. SI is expected to provide source code, transfer IPR and ownership right of only those solutions which would be customized by bidder for the use of Chennai Smart City Corporation Limited. For any pre-existing work, SI and Chennai Smart City Corporation Limited shall be held jointly responsible and its use in any other project by SI shall be decided on mutual consent.
- 25.2.** Forthwith upon expiry or earlier termination of the Contract and at any other time on demand by the Authority, SI shall deliver to the Authority all Documents provided by or originating from the Authority and all Documents produced by or from or for SI in the course of performing the Services, unless otherwise directed in writing by the Authority at no additional cost. SI shall not, without the prior written consent of the Authority store, copy, distribute or retain any such Documents.

## **26. Exit Management Plan**

- 26.1.** An Exit Management plan shall be furnished by SI in writing to the Authority within 90 days from the date of signing the Contract, which shall deal with at least the following aspects of exit management in relation to the contract as a whole and in relation to the Project Implementation, and Service Level monitoring.
- i. A detailed program of the transfer process that could be used in conjunction with a Replacement Service Provider including details of the means to be used to ensure continuing provision of the services throughout the transfer process or until the cessation of the services and of the management structure to be used during the transfer;
  - ii. Plans for provision of contingent support to Project and Replacement Service Provider for a reasonable period after transfer.
  - iii. Exit Management plan in case of normal termination of Contract period
  - iv. Exit Management plan in case of any eventuality due to which Project is terminated before the contract period.
  - v. Exit Management plan in case of termination of SI
- 26.2.** Exit Management plan at the minimum adhere to the following:
- i. Three (3) months of the support to Replacement Service Provider post termination of the Contract
  - ii. Complete handover of the Planning documents, bill of materials, functional requirements specification, technical specifications of all equipments, change requests if any, sources codes, wherever applicable, reports, documents and other relevant items to the Replacement Service Provider/Authority

iii. Certificate of Acceptance from authorized representative of Replacement Service Provider issued to SI on successful completion of handover and knowledge transfer

**26.3.** In the event of termination or expiry of the contract, Project Implementation, or Service Level monitoring, both Bidder and Authority shall comply with the Exit Management Plan.

**26.4.** During the exit management period, SI shall use its best efforts to deliver the services.

## **B. SPECIAL CONDITIONS OF CONTRACT (SCC)**

### **27. Performance Security**

**27.1.** SI shall furnish Performance Security to the Authority at the time of signing the Contract which shall be equal to 10% of the value of the Contract and shall be in the form of a **Bank Guarantee Bond** from a Nationalized/Scheduled Bank in the Performa given in Annexure 5 (a) RfP volume I within 15 days after issuance of Letter of Acceptance (LoA) which would be valid up to a period of six months after the contract completion period.

**27.2.** SI shall be required to submit **five** Bank Guarantees of equal amount totaling 10% of the value of the Contract. The Authority shall return 1<sup>st</sup> Bank Guarantee after 2 years of signing of contract and successful project execution, 2<sup>nd</sup> Bank Guarantee after 3 years of contract signing and successful project execution, 3<sup>rd</sup> Bank Guarantee after 4 years of contract signing and successful project execution and the 4<sup>th</sup> and 5<sup>th</sup> Bank Guarantee one year after successful completion of the contract.

### **27.3. Liquidated Damages**

**27.4.** If SI fails to supply, install or maintain any or all of the goods as per the contract, within the time period(s) specified in the RfP Vol II, the Authority without prejudice to its other rights and remedies under the Contract, deduct from the Contract price, as liquidated damages, a sum equivalent to 0.1 % per week or part thereof of contract value for a milestone/quarter.

**27.5.** The deduction shall not in any case exceed **10 % of the contract value**.

**27.6.** The Authority may without prejudice to its right to effect recovery by any other method, deduct the amount of liquidated damages from any money belonging to SI in its hands (which includes the Authority's right to claim such amount against SI's Bank Guarantee) or which may become due to SI. Any such recovery or liquidated damages shall not in any way relieve SI from any of its obligations to complete the Work or from any other obligations and liabilities under the Contract.

**27.7.** Delay not attributable to SI shall be considered for exclusion for the purpose of computing liquidated damages.

### **28. Limitation of Liability:**

Limitation of Bidder's Liability towards the Authority:

**28.1.** Neither Party shall be liable to the other Party for any indirect or consequential loss or damage (including loss of revenue and profits) arising out of or relating to the Contract.

- 28.2.** Except in case of gross negligence or willful misconduct on the part of SI or on the part of any person or company acting on behalf of SI in carrying out the Services,

SI, with respect to damage caused by SI to Authority's property, shall not be liable to Authority:

- (i) for any indirect or consequential loss or damage; and
  - (ii) For any direct loss or damage that exceeds (A) the total payments payable under the Contract to SI hereunder, or (B) the proceeds SI may be entitled to receive from any insurance maintained by SI to cover such a liability, whichever of (A) or (B) is higher.
- 28.3.** This limitation of liability shall not affect SI liability, if any, for damage to Third Parties caused by SI or any person or company acting on behalf of SI in carrying out the Services.

## **29. Ownership and Retention of Documents**

- 29.1.** The Authority shall own the Documents, prepared by or for SI arising out of or in connection with the Contract.
- 29.2.** Forthwith upon expiry or earlier termination of this Contract and at any other time on demand by the Authority, SI shall deliver to the Authority all documents provided by or originating from the Authority and all documents produced by or for SI in the course of performing the Services, unless otherwise directed in writing by the Authority at no additional cost. SI shall not, without the prior written consent of the Authority store, copy, distribute or retain any such documents.

## **30. Information Security**

- 30.1.** SI shall not carry any written/printed document, layout diagrams, CD, hard disk, storage tapes, other storage devices or any other goods/material proprietary to Authority into/out of any location without written permission from the Authority.
- 30.2.** SI shall not destroy any unwanted documents, defective tapes/media present at any location on their own. All such documents, tapes/media shall be handed over to the Authority.
- 30.3.** All documentation and media at any location shall be properly identified, labeled and numbered by SI. SI shall keep track of all such items and provide a summary report of these items to the Authority whenever asked for.
- 30.4.** Access to Authority's data and systems, Internet facility by SI at any location shall be in accordance with the written permission by the Authority. The Authority shall allow SI to use facility in a limited manner subject to availability. It is the

responsibility of SI to prepare and equip himself in order to meet the requirements.

- 30.5. SI must acknowledge that Authority's business data and other Authority proprietary information or materials, whether developed by Authority or being used by Authority pursuant to a license agreement with a third party (the foregoing collectively referred to herein as "proprietary information") are confidential and proprietary to Authority; and SI along with its team agrees to use reasonable care to safeguard the proprietary information and to prevent the unauthorized use or disclosure thereof, which care shall not be less than that used by SI to protect its own proprietary information. SI recognizes that the goodwill of Authority depends, among other things, upon SI keeping such proprietary information confidential and that unauthorized disclosure of the same by SI or its team could damage the goodwill of Authority, and that by reason of SI's duties hereunder. SI may come into possession of such proprietary information, even though SI does not take any direct part in or furnish the services performed for the creation of said proprietary information and shall limit access thereto to employees with a need to such access to perform the services required by this agreement. SI shall use such information only for the purpose of performing the said services.
- 30.6. SI shall, upon termination of this agreement for any reason, or upon demand by Authority, whichever is earliest, return any and all information provided to SI by Authority, including any copies or reproductions, both hardcopy and electronic.
- 30.7. By virtue of the Contract, SI team may have access to personal information of the Authority and/or a third party. The Authority has the sole ownership of and the right to use, all such data in perpetuity including any data or other information pertaining to the citizens that may be in the possession of SI team in the course of performing the Services under the Contract

### **31. Records of contract documents**

- 31.1. SI shall at all-time make and keep sufficient copies of the process manuals, operating procedures, specifications, Contract documents and any other documentation for him to fulfil his duties under the Contract.
- 31.2. SI shall keep on the Site at least three copies of each and every specification and Contract Document, in excess of his own requirement and those copies shall be available at all times for use by the Authority's Representative and by any other person authorized by the Authority's Representative.

### **32. Security and Safety**



- 32.1.** SI shall comply with the directions issued from time to time by the Authority and the standards related to the security and safety, in so far as it applies to the provision of the Services.
- 32.2.** SI shall upon reasonable request by the Authority, or its nominee(s) participate in regular meetings when safety and information technology security matters are reviewed.

### **33. Confidentiality**

- 33.1.** SI shall not, either during the term or after expiration of this Contract, disclose any proprietary or confidential information relating to the Services/Contract and/or Authority's business/operations, information, Application/software, hardware, business data, architecture schematics, designs, storage media and other information/documents without the prior written consent of the Authority.
- 33.2.** The Authority reserves the right to adopt legal proceedings, civil or criminal, against SI in relation to a dispute arising out of breach of obligation by SI under this clause.
- 33.3.** SI shall do everything reasonably possible to preserve the confidentiality of the Confidential Information including execution of a confidentiality agreement with the Authority to the satisfaction of the Authority.
- 33.4.** SI shall notify the Authority promptly if it is aware of any disclosure of the Confidential Information otherwise than as permitted by the Contract or with the authority of the Authority.
- 33.5.** SI shall be liable to fully recompense the Authority for any loss of revenue arising from breach of confidentiality.

### **34. Events of Default by SI**

The failure on the part of SI to perform any of its obligations or comply with any of the terms of this Contract shall constitute an Event of Default on the part of SI. The events of default are but not limited to:

- 34.1.** SI/Bidder's Team has failed to perform any instructions or directives issued by the Authority which it deems proper and necessary to execute the scope of work or provide services under the Contract, or
- 34.2.** SI/Bidder's Team has failed to confirm/adhere to any of the key performance indicators as laid down in the Key Performance Measures/Service Levels, or if SI has fallen short of matching such standards/benchmarks/targets as the Authority may have designated with respect to the system or any goods, task or service, necessary for the execution of the scope of work and performance of services under this Contract. The above mentioned failure on the part of SI may be in

terms of failure to adhere to performance, quality, timelines, specifications, requirements or any other criteria as defined by the Authority;

- 34.3.** SI has failed to remedy a defect or failure to perform its obligations in accordance with the specifications issued by the Authority, despite being served with a default notice which laid down the specific deviance on the part of SI/SI's Team to comply with any stipulations or standards as laid down by the Authority; or
- 34.4.** SI/SI's Team has failed to adhere to any amended direction, instruction, modification or clarification as issued by the Authority during the term of this Contract and which the Authority deems proper and necessary for the execution of the scope of work under this Contract.
- 34.5.** SI/SI's Team has failed to demonstrate or sustain any representation or warranty made by it in this Contract, with respect to any of the terms of its Bid, the RfP and this Contract.
- 34.6.** There is a proceeding for bankruptcy, insolvency, winding up or there is an appointment of receiver, liquidator, assignee, or similar official against or in relation to SI.
- 34.7.** SI/Bidder's Team has failed to comply with or is in breach or contravention of any applicable laws.

Where there has been an occurrence of such defaults inter alia as stated above, the Authority shall issue a notice of default to SI, setting out specific defaults/deviances/omissions/non-compliances/non-performances and providing a notice of thirty (30) days to enable such defaulting party to remedy the default committed.

Where despite the issuance of a default notice to SI by the Authority, SISI fails to remedy the default to the satisfaction of the Authority, the Authority may, where it deems fit, issue to the defaulting party another default notice or proceed to contract termination.

## **35. Termination**

The Authority may, terminate this Contract in whole or in part by giving SI a prior and written notice indicating its intention to terminate the Contract under the following circumstances:

- 35.1.** Where the Authority is of the opinion that there has been such Event of Default on the part of SI/SI's Team which would make it proper and necessary to terminate this Contract and may include failure on the part of SI to respect any of its commitments with regard to any part of its obligations under its Bid, the RfP or under this Contract.

- 35.2.** Where it comes to the Authority's attention that SI (or SI's Team) is in a position of actual conflict of interest with the interests of the Authority, in relation to any of terms of SI's Bid, the RfP or this Contract.
- 35.3.** Where SI's ability to survive as an independent corporate entity is threatened or is lost owing to any reason whatsoever, including inter-alia the filing of any bankruptcy proceedings against SI, any failure by SI to pay any of its dues to its creditors, the institution of any winding up proceedings against SI or the happening of any such events that are adverse to the commercial viability of SI. In the event of the happening of any events of the above nature, the Authority shall reserve the right to take any steps as are necessary, to ensure the effective transition of the sites pilot site to a successor agency, and to ensure business continuity.
- 35.4.** Termination for Insolvency: The Authority may at any time terminate the Contract by giving written notice to SI, without compensation to SI, if SI becomes bankrupt or otherwise insolvent, provided that such termination shall not prejudice or affect any right of action or remedy which has accrued or shall accrue thereafter to the Authority.
- 35.5.** SI may, subject to approval by the Authority, terminate this Contract before the expiry of the term by giving the Authority a prior and written notice at least 3 months in advance indicating its intention to terminate the Contract.

## **36. Consequence of Termination**

- 36.1.** In the event of termination of the Contract due to any cause whatsoever, whether consequent to the stipulated Term of the Contract or otherwise the Authority shall be entitled to impose any such obligations and conditions and issue any clarifications as may be necessary to ensure an efficient transition and effective business continuity of the project which SI shall be obliged to comply with and take all available steps to minimize loss resulting from that termination/breach, and further allow and provide all such assistance to the Authority and/or the successor agency/service provider, as may be required, to take over the obligations of SI in relation to the execution/continued execution of the requirements of the Contract.
- 36.2.** Where the termination of the Contract is prior to its stipulated term on account of a Default on the part of SI or due to the fact that the survival of SI as an independent corporate entity is threatened/has ceased, or for any other reason, whatsoever, the Authority, through unilateral re-determination of the consideration payable to SI, shall pay SI for that part of the Services which have been authorized by the Authority and satisfactorily performed by SI up to the date of termination. Without prejudice to any other rights, the Authority may retain such amounts from the payment due and payable by the Authority to SI as may be required to offset any losses caused to the Authority as a result of any act/omissions of SI. In case of any loss or damage due to default on the part of SI in performing any of its obligations with regard to executing the Schedule of Requirements under the contract, SI shall compensate the Authority for any such

loss, damages or other costs, incurred by the Authority. Additionally, members of its team shall perform all its obligations and responsibilities under the Contract in an identical manner as were being performed before the collapse of SI as described above in order to execute an effective transition and to maintain business continuity. All third parties shall continue to perform all/any functions as stipulated by the Authority and as may be proper and necessary to execute the Schedule of Requirements under the Contract in terms of SI's Bid, the Bid Document and the Contract

- 36.3.** Nothing herein shall restrict the right of the Authority to invoke the Bank Guarantee and other Guarantees furnished hereunder and pursue such other rights and/or remedies that may be available to the Authority under law.
- 36.4.** The termination hereof shall not affect any accrued right or liability of either Party nor affect the operation of the provisions of the Contract that are expressly or by implication intended to come into or continue in force on or after such termination.

**37. Change Control Note (CCN)**

- 37.1.** This applies to and describes the procedure to be followed in the event of any proposed change to contract, site Implementation, and Service levels. Such change shall include, but shall not be limited to, changes in the scope of services provided by SI and changes to the terms of payment.
- 37.2.** Change requests in respect of the contract, the site implementation, or the Service levels shall emanate from the Parties' representative who shall be responsible for obtaining approval for the change and who shall act as its sponsor throughout the Change Control Process and shall complete Part A of the CCN (Annex I, Section 3 of the RfP). CCNs shall be presented to the other Party's representative who shall acknowledge receipt by signature of the authorized representative of the Authority.
- 37.3.** SI and the Authority while preparing the CCN, shall consider the change in the context of whether the change is beyond the scope of Services including ancillary and concomitant services required. The CCN shall be applicable for the items which are beyond the stated/implied scope of work as per the RfP document.
- 37.4.** SI shall assess the CCN and complete Part B of the CCN. In completing Part B of the CCN SI/Lead Bidder shall provide as a minimum:
- a description of the change;
  - a list of deliverables required for implementing the change;
  - a timetable for implementation;
  - an estimate of any proposed change; or any relevant acceptance criteria;
  - an assessment of the value of the proposed change;
  - Material evidence to prove that the proposed change is not already covered within the scope of the RfP, Agreement and Service Levels.

- 37.5.** Prior to submission of the completed CCN to the Authority or its nominated agencies, SI shall undertake its own internal review of the proposal and obtain all necessary internal approvals. As a part of this internal review process, SI shall consider the materiality of the proposed change in the context of the Agreement, the sites, Service levels affected by the change and the total effect that may arise from implementation of the change.
- 37.6.** Each Party shall be responsible for its own costs incurred in the quotation, preparation of CCNs and in the completion of its obligations described in this process provided SI meets the obligations as set in the CCN. In the event SI is unable to meet the obligations as defined in the CCN then the cost of getting it done by third party shall be borne by SI. Change requests and CCNs shall be reported monthly to each Party's representative who shall prioritize and review progress.

## **C. SERVICE LEVELS**

### **38. Purpose**

- 38.1.** The purpose is to define the levels of service provided by SI to the Authority for the duration of the contract. The benefits of this are:
- 38.2.** Start a process that applies to Authority and SI attention to some aspect of performance, only when that aspect drops below the threshold defined by the Authority.
- 38.3.** Help the Authority control the levels and performance of SI's services.
- 38.4.** The Service Levels are between the Authority and SI.

### **39. Service Level Agreements & Targets**

- 39.1.** This section is agreed to by Authority and SI as the key performance indicator for the project. This may be reviewed and revised according to the procedures detailed in Clause 45 SLA Change Control.
- 39.2.** The following section reflects the measurements to be used to track and report system's performance on a regular basis. The targets shown in the following tables are for the period of contact.
- 39.3.** The procedures in Clause 45 shall be used if there is a dispute between Authority and SI on what the permanent targets should be.

### **40. General principles of Service Level Agreements**

The Service Level agreements have been logically segregated in the following categories:

#### **40.1. Liquidated Damages**

The liquidated damages shall come into effect once the notification of Award has been issued by the Authority. It would be mainly applicable on the implementation phase of the project.

#### **40.2. Service Level Agreements**

- Service Level Agreement (SLA) shall become the part of contract between Chennai Smart City and the successful bidder. SLA defines the terms of the successful bidder's responsibility in ensuring the timely delivery of the deliverables and the correctness of the same based on the agreed Performance Indicators as detailed in this section.

- The successful bidder has to comply with service level requirements to ensure adherence to project timelines, quality and availability of services, throughout the period of this contract i.e. during implementation phase and for a period of five (5) years. The successful bidder has to supply appropriate software/hardware/automated tools as may be required to monitor and submit reports of all the SLAs mentioned in this section.
- For purposes of the SLA, the definitions and terms as specified in the document along with the following terms shall have the meanings set forth below:
  - "Total Time" - Total number of hours in the quarter (or the concerned period) being considered for evaluation of SLA performance.
  - "Uptime" – Time period for which the specified services/outcomes are available in the period being considered for evaluation of SLA. Formulae for calculation of Uptime:  $\text{Uptime (\%)} = \{1 - [(\text{Downtime}) / (\text{Total time-scheduled maintenance time})]\} * 100$
  - "Downtime"- Time period for which the specified services/components/outcomes are not available in the concerned period, being considered for evaluation of SLA, which would exclude downtime owing to Force Majeure & Reasons beyond control of the successful bidder.
  - "Scheduled Maintenance Time" - Time period for which the specified services/components with specified technical and service standards are not available due to scheduled maintenance activity. The successful bidder is required to take at least 10 days prior approval from Chennai Smart City Ltd for any such activity. The scheduled maintenance should be carried out during non-peak hours (like post mid-night, and should not be for more than 4 hours. Such planned downtime would be granted max 4 times a year.
- "Incident" - Any event/abnormalities in the service being rendered, that may lead to disruption in normal operations and services to the end user.
- "Response Time" - Time elapsed from the moment an incident is reported in the Helpdesk over phone or by any applicable mode of communication, to the time when a resource is assigned for the resolution of the same.
- "Resolution Time" - Time elapsed from the moment incident is reported to Helpdesk either in person or automatically through system, to the time by which the incident is resolved completely and services as promised are restored.

#### **40.3. Pre-Implementation SLAs**

- These SLAs shall be used to evaluate the timelines for completion of deliverables that are listed in the deliverable.
- These SLAs for completion of individual milestones listed in the implementation schedule. For delay of every week in completion & submission of the deliverable mentioned in the section of deliverables & timeline e, the selected bidder would be charged with a penalty as follows:

Delay (Weeks)	Penalty (INR)
1 week of delay for completion of scope for any smart element	0.1% of capex of respective smart element value
For every subsequent week	0.15% of capex of respective smart element value

- In case the penalties for the selected bidder reaches 10% of the capex value in the form of penalty, cumulative of penalties for all smart elements, at any point of time during the duration of pre- implementation phase, GMVC reserves the right to invoke the termination clause.

#### 40.4. Post-Implementation SLAs

- These SLAs shall be used to evaluate the performance of the services on monthly basis.
- Penalty levied for non- performance as per SLA requirements shall be deducted through subsequent payments due from Chennai Smart City Ltd or through the Performance Bank Guarantee.
- The SLA parameters shall be measured for each of the sub systems’ SLA parameter requirements and measurement methods, through appropriate SLA Measurement tools. All such required tools should be provided by the successful bidder. GMVC will have the authority to audit these tools for accuracy and reliability.
- The upper limit of penalty would be capped at 10% of the opex value for each quarter. In case the calculated penalty crosses 10% penalty of the opex value in 2 subsequent quarters, GMVC reserves the right to invoke the termination clause.
- SLAs for street IT infrastructure such as surveillance cameras, RLVD cameras, ANPR cameras, environment sensors, weather sensors, emergency call box, public address system, and digital display boards.

#	Uptime SLA (Monthly)	Penalty Clause
1	Uptime >= 99.5%	No Deduction
2	Uptime < 99.5%	(99.5%- Uptime %) of monthly Operational Expense for the component. For example if uptime of component is 95%, then penalty imposed will be 99%-95% i.e. 4% of operational expense.

- Uptime definition: All devices have to be working and deliver the desired results. The no. of hours that the particular device/equipment does not work will be treated as down time. Uptime shall be calculated as  $Uptime (\%) = \{1 - [(Downtime) / (Total\ time - scheduled\ maintenance\ time)]\} * 100$ . For ex, if 10 nos. of Sensors for Digital display are deployed at various locations, and 2 device/units does not work for 5 Hrs, the total non-working device hours will



be 10 unit hours ( and the uptime would be  $\{1-(10/(10*90*24))\}$ , 10 being the number of units, for 90 days on 24 hours basis.

- The penalties would be levied for every unit down time hour.
- SLA and Penalty for Helpdesk Response and Resolution time

#	Parameter	Penalty Clause
1	For $\leq 1\%$ of the calls not getting responded in less than or equal to 60 seconds per quarter	No Deduction
2	For $> 1\%$ of the calls not getting responded in less than or equal to 60 seconds per quarter	0.5% of the monthly opex value

- SLA for Change Requests or enhancements

#	Parameter	Metric	Frequency	Penalty
1	Criticality of Change – <b>Low</b>	$< T$ , where T is the timeframe for completion of the Change request as agreed upon by Chennai Smart City Ltd and successful bidder	Weekly per Occurrence	1 % of change request value per week for the first two weeks for each occurrence, 2 % of change request value per week for every subsequent week, subject to a maximum of 10% post which Chennai Smart City Ltd may invoke annulment of the contract.
2	Criticality of Change – <b>Medium</b>	$< T$ , where T is the timeframe for completion of the Change request as agreed upon by Chennai Smart City Ltd and successful bidder	Weekly per Occurrence	1.5 % of change request value per week for the first two weeks for each occurrence, 2.5 % of change request value per week for every subsequent week, subject to a maximum of 10% post which Chennai Smart City Ltd may invoke annulment of

#	Parameter	Metric	Frequency	Penalty
3	Criticality of Change – <b>High</b>	< T weeks, where T is the timeframe for completion of the Change request as agreed upon by Chennai Smart City Ltd and successful bidder	Weekly per Occurrence	the contract. 2 % of change request value per week for the first two weeks for each occurrence, 3 % of change request value per week for every subsequent week, subject to a maximum of 10% post which Chennai Smart City Ltd may invoke annulment of the contract.

- SLA for issue resolution

#	Parameter	Metric	Frequency	Penalty
1	Severity 1 Issue	Resolution Time: <= 8 Hrs from the time the call is logged by end user.	Daily	0.1% of monthly opex value per week for the first two weeks for each occurrence, 0.2% of monthly opex value per week for every subsequent week, subject to a maximum of 10% post which Chennai Smart City Ltd may invoke annulment of the contract.
2	Severity 2 Issue	Resolution Time: <= 4 Days from the time the call is logged by end user.	Daily	0.1% of monthly opex value per week for the first two weeks for each occurrence, 0.2% of monthly opex value per week for every subsequent week, subject to a maximum of 10% post which Chennai Smart City Ltd may invoke annulment of the contract.
3	Severity 3 Issue	Resolution Time: <= 10 Days from the time the call is logged by end user.	Daily	0.1% of monthly opex value per week for the first two weeks for each occurrence, 0.2% of monthly opex value per week for every subsequent week, subject to a maximum of 10% post which Chennai Smart City Ltd may invoke annulment of the contract.

4	Severity 4 Issue	Resolution Time: <= 20 Days from the time the call is logged by end user.	Daily	0.1% of monthly opex value per week for the first two weeks for each occurrence, 0.2% of monthly opex value per week for every subsequent week, subject to a maximum of 10% post which Chennai Smart City Ltd may invoke annulment of the contract.
---	------------------	--	-------	---

- Miscellaneous SLAs

#	Parameter	Metric	Frequency	Penalty
1	Compliance in document versioning and maintenance (FRS, SRS, Business Blue Prints, User Training Manual etc.), application version control, updates & patches etc.	100% as per requirement timelines	Daily per occurrence	Rs.10,000 per occurrence per day of delay.
2	Manpower Availability & Readiness	100% as per requirement timelines	Daily	Rs 10,000 per day in casethere is shortage in manpower deployment or lack of adequate skills
3	Scheduled downtime for System Maintenance per week	<= 2 times per month	Per Occurrence	Rs. 1,00,000 per occurrence for unscheduled downtime or scheduled downtimes exceeding the specified metric.
4	Resource Replacement	Within 7 days of exit of resource (in case of Chennai Smart City Ltd initiated or supplier initiated)	Per Occurrence	Rs. 5,000.00 per day of unavailability of resource
5	Application Security	Cyber Crime/Hacking/Data Theft/Fraud attributable to the service provider	Per Occurrence	Depending on the type of incident and its impact, a Penalty of 10% on the entire contract value or in case of severe issue (as defined by Chennai Smart City Ltd) such breach may lead to

				termination of contract
--	--	--	--	-------------------------

**Definitions:**

- Severity 1: Command and Communication Centre or ERP or Smart City applications down for more than 70% users.
- Severity 2: Command and Communication Centre or ERP or Smart City applications down for more than 30% users.
- Severity 3: Modules of Command and Communication Centre or ERP not functional for users.
- Severity 4: Minor functionality issues with Command and Communication Centre or ERP or Smart City applications
- Response Time: Response time is defined as the time the support vendor takes to respond from the time that ticket was raised.
- Resolution Time: Resolution time is defined as the time the vendor takes to resolve the issue or provide acceptable workaround for the issue.

**40.5. Conditions for No Penalties**

- Penalties shall not be levied on the Bidder in the following cases:
  - There is a force majeure event effecting the SLA which is beyond the control of the successful bidder. Force Majeure events shall be considered in line with the clause mentioned RfP.
  - The non-compliance to the SLA has been due to reasons beyond the control of the successful bidder.
  - Theft cases by default/vandalism would not be considered as “beyond the control of bidder”. Hence, the Bidder should be taking adequate anti-theft measures, spares strategy, Insurance as required to maintain the desired Required SLA.

**41. Reporting Procedures**

- 41.1** SI representative shall prepare and distribute Service level performance reports in a mutually agreed format by the 5th working day of subsequent month. The reports shall include “actual versus target” Service Level Performance, a variance analysis and discussion of appropriate issues or significant events. Performance reports shall be distributed to Authority management personnel as directed by Authority.
- 41.2** Also, SI may be required to get the Service Level performance report audited by a third-party Auditor appointed by the Authority.

**42. Issue Management Procedures**

**42.1 General**

This process provides an appropriate management structure for the orderly consideration and resolution of business and operational issues in the event that quick consensus is not reached between Authority and Bidder.

Implementing such a process at the beginning of the outsourcing engagement significantly improves the probability of successful issue resolution. It is expected that this pre-defined process shall only be used on an exception basis if issues are not resolved at lower management levels.

## 42.2 Issue Management Process

**42.3** Either Authority or SI may raise an issue by documenting the business or technical problem, which presents a reasonably objective summary of both points of view and identifies specific points of disagreement with possible solutions.

**42.4** Any unresolved issues/disputes concerning the Project/Contract between the Parties shall first be referred in writing to the Project Manager for his consideration and resolution. If the Project Manager is unable to resolve any issue/dispute within 5 days of reference to them, the Project Manager shall refer the matter to the Program Management Committee. If the Program Management Committee is unable to resolve the issues/disputes referred to them within 15 days the unresolved issue/dispute shall be referred to Steering Committee/high powered committee/Project Implementation Committee for resolution. The Steering Committee within 30 days of reference to them shall try to resolve the issue/dispute.

**42.5** If the Steering Committee fails to resolve a dispute as per the above clause, the same shall be referred to arbitration. The arbitration proceedings shall be carried out as per the Arbitration procedures mentioned in Clause 18 of this section of RfP.

## 43. Service Level Change Control

### 43.1 General

It is acknowledged that this **Service levels may change as Authority's business needs evolve over the course of the contract period**. As such, this document also defines the following management procedures:

- a. A process for negotiating changes to the Service Levels
- b. An issue management process for documenting and resolving particularly difficult issues.
- c. Authority and Bidder management escalation process to be used in the event that an issue is not being resolved in a timely manner by the lowest possible level of management.

Any changes to the levels of service provided during the term of this Agreement shall be requested, documented and negotiated in good faith by both parties. Either party can request a change.

**43.2 Service Level Change Process:** The parties may amend Service Level by mutual agreement in accordance. Changes can be proposed by either party. Unresolved issues shall also be addressed. SI's representative shall maintain and distribute current copies of the Service Level document as directed by Authority. Additional copies of the current Service Levels shall be available at all times to authorized parties.

**43.3 Version Control/Release Management:** All negotiated changes shall require changing the version control number. As appropriate, minor changes may be accumulated for periodic release or for release when a critical threshold of change has occurred.

## D. ANNEXURES

### Annex I: Change Control Note

<b>Change Control Note</b>		<b>CCN Number:</b>
<b>Part A: Initiation</b>		
Title		
Originator		
Sponsor		
Date of Initiation		
<b>Details of Proposed Change</b>		
(To include reason for change and appropriate details/specifications. Identify any attachments as A1, A2, and A3 etc.)		
Authorized by Authority	Date	
Name		
Signature		
Received by the Bidder	Date	
Name		
Signature		
Change		
<b>Change Control Note</b>		<b>CCN Number:</b>
<b>Part B: Evaluation</b>		
(Identify any attachments as B1, B2, and B3 etc.) Changes to Services, payment terms, payment profile, documentation, training, service levels and component working arrangements and any other contractual issue.		
<b>Brief Description of Solution:</b>		
<b>Deliverables:</b>		
<b>Timetable:</b>		
<b>Charges for Implementation:</b>		
<b>Other Relevant Information:</b> (including value-added and acceptance criteria)		
Authorized by Authority	Date	
Name		
Signature		
<b>Change Control Note</b>		<b>CCN Number:</b>
<b>Part C: Authority to Proceed</b>		
Implementation of this CCN as submitted in Part A, in accordance with Part B is: (tick as appropriate)		
<b>Approved</b>		
<b>Rejected</b>		
<b>Requires Further Information</b> (as follows, or as Attachment 1 etc.)		
<b>For Authority and its nominated</b>	<b>For SI</b>	

<b>agencies</b>	
Signature	Signature
Name	Name
Title	Title
Date	Date



**Annex II: Form of Agreement**

THIS Agreement made the .....date of.....2016, between..... (hereinafter.....referred to as the "SI") of the one part and ..... (hereinafter called the "Authority") of the other part.

WHEREAS SI has the required professional skills, personnel and technical resources, has agreed to provide the Services on the terms and conditions set forth in this Contract and is about to perform services as specified in this RfP .....(hereinafter called "works" ) mentioned, enumerated or referred to in certain Contract conditions, specification, scope of work, other sections of the RfP, covering letter and schedule of prices which, for the purpose of identification, have been signed by ..... on behalf of the .....

SI and .....( the Authority) on behalf of the Authority and all of which are deemed to form part of the Contract as though separately set out herein and are included in the expression "Contract" whenever herein used.

**NOW, THEREFORE, IT IS HEREBY AGREED** between the parties as follows:

- a. The Authority has accepted the tender of SI for the provision and execution of the said works for the sum of .....upon the terms laid out in this RfP.
- b. SI hereby agrees to provide Services to Authority, conforming to the specified Service Levels and conditions mentioned
- c. The following documents attached hereto shall be deemed to form an integral part of this Agreement:

<b>Complete Request for Proposal (RfP) Document</b>	<i>Volumes I, II and III of the RfP and corrigendum and addendum, if any</i>
<b>Break-up of cost components</b>	<i>Bidder's Commercial bid</i>
<b>The Authority's Letter of Intent dated &lt;&lt;&gt;&gt;</b>	<i>To be issued later by the Authority</i>
<b>SI's Letter of acceptance dated &lt;&lt;&gt;&gt;</b>	<i>To be issued later by the SI</i>
<b>Bid submitted by SI</b>	<i>Bidder's Technical bid</i>

- d. The mutual rights and obligations of the "Authority" and SI shall be as set forth in the Agreement, in particular:
  - SI shall carry out and complete the Services in accordance with the provisions of the Agreement; and
  - The "Authority" shall make payments to SI in accordance with the provisions of the Agreement.

**NOW THESE PRESENTS WITNESS** and the parties hereto hereby agree and declare as follows, that is to say, in consideration of the payments to be made to SI by the Authority as hereinafter mentioned, SI shall deliver the services for the said works and shall do and perform all other works and things in the Contract mentioned or described or which are implied there from or there in respectively or may be reasonably necessary for the completion of the said works within and at the times and in the manner and subject to the terms, conditions and stipulations mentioned in the said Contract.

**AND** in consideration of services and milestones, the Authority shall pay to SI the said sum of .....or such other sums as may become payable to SI under the provisions of this Contract, such payments to be made at such time and in such manner as is provided by the Contract.

IN WITNESS WHEREOF the parties hereto have signed this deed hereunder on the dates respectively mentioned against the signature of each.

Signed  
Name : \_\_\_\_\_  
Designation : \_\_\_\_\_  
Date : \_\_\_\_\_  
Place : \_\_\_\_\_

Signed  
Name : \_\_\_\_\_  
Designation : \_\_\_\_\_  
Date : \_\_\_\_\_  
Place : \_\_\_\_\_

**in the presence of :**

**in the presence of :**

Signed  
Name : \_\_\_\_\_  
Designation : \_\_\_\_\_  
Date : \_\_\_\_\_  
Place : \_\_\_\_\_

Signed  
Name : \_\_\_\_\_  
Designation : \_\_\_\_\_  
Date : \_\_\_\_\_  
Place : \_\_\_\_\_