

**REQUEST FOR PROPOSAL  
FOR  
SELECTION OF SYSTEM INTEGRATOR  
FOR IMPLEMENTATION OF INTEGRATED  
COMMAND AND CONTROL CENTRE, ITMS  
AND CITY SURVEILLANCE SYSTEM IN  
GUWAHATI ON  
DESIGN, SUPPLY, IMPLEMENTATION AND  
O&M  
(5-YEARS) BASIS**

**Volume 2: Scope of Work & Technical  
Specifications**



Guwahati Smart City Limited,  
Guwahati, Assam

**Tender Notice No: SPV/GSCL/DEV/55/2017/396**

## TABLE OF CONTENTS

<b>1.0</b>	<b>DISCLAIMER</b> .....	<b>5</b>
<b>2.0</b>	<b>GLOSSARY</b> .....	<b>6</b>
<b>3.0</b>	<b>INTRODUCTION</b> .....	<b>7</b>
3.1	PROJECT BACKGROUND .....	7
3.2	STANDARDS & PROTOCOLS .....	9
3.3	PROJECT BROAD SCOPE.....	10
3.4	PROJECT OBJECTIVES .....	11
<b>4.0</b>	<b>PROJECT SCOPE OF WORK</b> .....	<b>12</b>
4.1	GEOGRAPHICAL SCOPE OF SERVICES .....	12
4.2	OVERVIEW OF SCOPE OF SERVICES.....	13
4.3	ASSESSMENT, SITE SURVEY AND PROJECT PLAN .....	15
4.4	DOCUMENTS/ DRAWINGS SUBMISSION AFTER AWARD OF CONTRACT .....	16
4.5	FINALIZATION OF DETAILED TECHNICAL ARCHITECTURE.....	17
4.6	SITE CLEARANCE OBLIGATIONS AND OTHER RELEVANT PERMISSIONS .....	23
4.6.1	<i>Survey And Commencement of Works</i> .....	23
4.6.2	<i>Existing Traffic Signal system</i> .....	23
4.6.3	<i>Electrical Works and Power Supply</i> .....	23
4.6.4	<i>Miscellaneous:</i> .....	24
4.7	OTHER EXPECTATIONS FROM SYSTEM INTEGRATOR (SI).....	25
4.8	DESIGN AND IMPLEMENTATION OF INTEGRATED COMMAND & CONTROL CENTER SYSTEM.....	28
4.9	DESIGN, SUPPLY, INSTALLATION & COMMISSIONING OF THE FIELD EQUIPMENT .....	28
4.10	CITY SURVEILLANCE SYSTEM – (CCTV CAMERA) .....	29
4.11	INTEGRATED TRAFFIC MANAGEMENT SYSTEM (ITMS) .....	31
4.11.1	<i>Traffic Violation Detection System</i> .....	32
4.11.2	<i>ANPR System</i> .....	33
4.11.3	<i>RLVD System</i> .....	33
4.11.4	<i>Speed Violation Detection (SVD) System</i> .....	34
4.11.5	<i>E-Challan Devices</i> .....	35
4.12	LIGHTNING-PROOF MEASURES .....	35
4.13	EARTHING SYSTEM .....	35
4.14	JUNCTION BOX / OUTDOOR CABINET, POLES AND CANTILEVER .....	36
4.15	POWER & UPS - FOR FIELD LOCATIONS.....	38
4.16	CIVIL AND ELECTRICAL WORKS.....	39
4.17	CABLING INFRASTRUCTURE.....	40
4.18	GEOGRAPHICAL INFORMATION SYSTEM (GIS) PLATFORM .....	40
4.19	GEO-TAGGING .....	42
4.20	EDGE ANALYTICS.....	42
4.21	NETWORK CONNECTIVITY (OFC & RF) FOR ICCC, DC AND OTHER FIELD SENSORS .....	42
4.21.1	<i>Network Design and Rollout plan</i> .....	45
4.21.2	<i>Implementation of Network connectivity</i> .....	45
4.21.3	<i>Hosting Services</i> .....	48
4.22	DESIGN, SUPPLY, INSTALLATION AND COMMISSIONING OF IT INFRASTRUCTURE AT DATA CENTRE (DC) AND ICCC .....	49
4.23	INSTALLATION & COMMISSIONING OF A SAMPLE SITE – PROOF OF CONCEPT (POC) .....	51
4.24	RESPONSIBILITY MATRIX - OVERALL .....	52
4.24.1	<i>Overall Activities – Responsibility Matrix</i> .....	52
4.24.2	<i>Network O&amp;M, Payments – Responsibility Matrix</i> .....	56
4.25	PROJECT DELIVERABLES .....	58
4.26	PROJECT TIMELINES.....	60
4.27	PROJECT DEFECT LIABILITY PERIOD (DLP) / WARRANTEE OF PRODUCT & SERVICES.....	61

<b>5.0</b>	<b>FUNCTIONAL REQUIREMENTS &amp; TECHNICAL SPECIFICATIONS.....</b>	<b>61</b>
5.1	COMPONENT 1 - CCTV CITY SURVEILLANCE SYSTEM .....	63
5.1.1	Indicative Solutions Architecture – CCTV City Surveillance .....	63
5.1.2	Functional Requirements – CCTV City Surveillance .....	64
5.1.3	Technical Specifications – CCTV Surveillance System.....	71
5.1.4	Video Management System (VMS) .....	89
5.2	COMPONENT 2 – INTEGRATED COMMAND CONTROL CENTRE (ICCC) .....	108
5.2.1	Functional Requirement – ICCC.....	109
5.2.2	Technical Specification – ICCC.....	111
5.2.3	Workstation with Joystick Controller .....	131
5.2.4	Desktop PC for ICCC .....	133
5.2.5	Structured Cabling .....	134
5.2.6	Electrical Cabling Components.....	135
5.2.7	Unified Threat Management System (UTM).....	135
5.2.8	Internet Switch (L-3).....	136
5.2.9	Internet Lease Line (ILL) .....	137
5.2.10	Helpdesk .....	137
5.2.11	Technical Specification of ICT Components & Accessories at ICCC .....	140
5.2.12	UPS 50 KVA at ICCC.....	148
5.2.13	KVM Switches .....	149
5.2.14	Structured Cabling .....	149
5.2.15	Electrical Cabling Components .....	150
5.2.16	Diesel Generator Set (DG) 75 KVA - ICCC.....	150
5.2.17	Electrical work for Data Center & ICCC.....	154
5.2.18	General: Post implementation requirements: .....	155
5.2.19	Handholding and Training .....	157
5.3	COMPONENT 3 – DATA CENTER .....	159
5.3.1	Data Centre (DC) .....	159
5.3.2	Data Center Spine & Leaf Switching Solution .....	165
5.3.3	Data Center Out of Band Switches.....	169
5.3.4	Network Management System / Enterprises Management System (NMS/EMS) .....	171
5.3.5	Intranet Firewall with IPS.....	180
5.3.6	Next Generation Firewall .....	183
5.3.7	End Host Anti – Virus .....	187
5.3.8	Load Balancer with Web Application Firewall .....	188
5.3.9	SIEM solution .....	190
5.3.10	Authentication, Authorization and Accounting – Network Access Control (AAA – NAC) .....	193
5.3.11	Storage Specifications .....	198
5.3.12	Hyper Converged Infrastructure (HCI) .....	201
5.3.13	GIS Map for Guwahati City.....	204
5.4	COMPONENT 4 – INTEGRATED TRAFFIC MANAGEMENT SYSTEM (ITMS) .....	206
5.4.1	Adaptive Traffic Signal Control (ATSC) System.....	207
5.4.2	Traffic Violation Detection System (TVDS) with ANPR & RLVD Camera .....	229
5.4.3	Speed Violation Detection System (SVD).....	248
5.4.4	Traffic Enforcement & E-Challan System .....	257
5.5	COMPONENT 5 – BACKBONE NETWORK & RF CONNECTIVITY .....	262
5.5.1	Network Backbone Connectivity .....	262
5.5.2	OFC Deployment Guidelines & Specification.....	269
5.5.3	Transmission Equipment Specifications (POP Sites).....	295
5.5.4	Wireless RF Connectivity.....	304
5.5.5	Wireless RF for redundant Connectivity – Short Distance.....	305
5.5.6	Wireless RF for Redundant Connectivity – Long Distance.....	307
5.5.7	Point-to-Point (P2P) Connectivity – Long Distance .....	310

5.5.8	Customer Premises Equipment's (CPE) / Client Radio – Subscriber Module .....	312
5.6	COMPONENT 6 – ENABLING WORK AT TEMPORARY ICCC LOCATIONS .....	314
5.6.1	Functional Requirements – ICCC (Temp. Location) .....	314
5.6.2	Functional Requirements – Non-IT Work at Temp. ICCC Location .....	315
5.6.3	Technical Specifications – Non-IT Requirements.....	316
5.6.4	Shifting of ICCC to Permanent Building.....	319
<b>6.0</b>	<b>ANNEXURE I: DETAILED WORK PHASES AND CONSIDERATIONS.....</b>	<b>319</b>
6.1.1	Requirement Survey Phase .....	319
6.1.2	Design Phase.....	320
6.1.3	Project Development Phase .....	320
6.1.4	Integration Phase.....	322
6.1.5	Go-Live Preparedness and Go-Live.....	324
6.1.6	Operations and Maintenance .....	324
6.1.7	Exit Management .....	328
6.1.8	Compliance to Standards & Certifications .....	330
6.1.9	Project Management and Governance .....	332
6.1.10	Change Management & Control.....	335
6.1.11	Testing and Acceptance Criteria.....	337
<b>7.0</b>	<b>ANNEXURE II: PAYMENT SCHEDULE AND MILESTONES .....</b>	<b>341</b>
7.1	PAYMENT SCHEDULES FOR IMPLEMENTATION PHASE .....	342
7.2	MILESTONES AND PAYMENT SCHEDULES FOR OPERATIONS AND MAINTENANCE PHASE.....	346
<b>8.0</b>	<b>ANNEXURE III - COMMON GUIDELINES REGARDING COMPLIANCE OF SYSTEMS/EQUIPMENT .....</b>	<b>346</b>
<b>9.0</b>	<b>ANNEXURE IV - STATUS OF THE SYSTEMS TO BE INTEGRATED IN ICCC IN GUWAHATI CITY.....</b>	<b>349</b>
<b>10.0</b>	<b>ANNEXURE V – SMART CITY GUIDELINES FOR ENSURING UNIVERSAL ACCESSIT SYSTEMS TO EMPOWER CITIZENS WITH DISABILITY TO ACCESS ICT SYSTEMS WITH EASE.....</b>	<b>349</b>
<b>11.0</b>	<b>ANNEXURE VII – CYBER SECURITY REQUIREMENTS FOR GUWAHATI SMART CITY PROJECT .....</b>	<b>354</b>
11.1	CYBER SECURITY FRAMEWORK.....	354
11.2	CYBER SECURITY POLICY .....	355
11.3	CYBER SECURITY GOVERNANCE.....	355
11.4	CYBER SECURITY ORGANIZATION STRUCTURE .....	355
11.5	SMART CITY IT ASSET MANAGEMENT .....	355
11.6	PHYSICAL & ENVIRONMENTAL SECURITY.....	355
11.7	ACCESS CONTROL.....	356
11.8	COMMUNICATIONS AND OPERATIONS MANAGEMENT.....	356
11.9	INFORMATION SYSTEMS ACQUISITION, DEVELOPMENT AND MAINTENANCE .....	359
11.10	BUSINESS CONTINUITY PLANNING AND DISASTER RECOVERY .....	359
11.11	INFORMATION SECURITY AUDITS.....	359
11.12	SECURITY OPERATIONS CENTER .....	360
11.13	AWARENESS TRAINING.....	360
11.14	SECURITY CONTROLS FOR CLOUD SERVICES .....	360
<b>12.0</b>	<b>ANNEXURE VIII- LIST OF LOCATIONS.....</b>	<b>362</b>
12.1	LOCATIONS FOR CITY SURVEILLANCE SYSTEM .....	362
12.2	LOCATIONS FOR TRAFFIC JUNCTIONS & ITMS.....	390
12.3	LOCATIONS FOR SVD .....	392
12.4	LOCATIONS FOR POLICE STATIONS – UNDER THE POLICE COMMISSIONERATE GUWAHATI .....	392
12.5	LOCATIONS FOR INTEGRATED COMMAND & CONTROL CENTER (ICCC).....	392
12.6	TENTATIVE POP SITE LOCATIONS .....	393
12.7	BILL OF MATERIAL (BOM) SUMMARY .....	394

## 1.0 DISCLAIMER

The information contained in this Request for Proposal document (“**RFP**”) whether subsequently provided to the bidders, (“**Bidder/s**”) verbally or in documentary form by Guwahati Smart City Limited (henceforth referred to as “**GSCL**” in this document) or any of its employees or advisors, is provided to Bidders on the terms and conditions set out in this Tender document and any other terms and conditions subject to which such information is provided.

This RFP is not an agreement and is not an offer or invitation to any party. The purpose of this RFP is to provide the Bidders or any other person with information to assist the formulation of their financial offers (“**Bid**”). This RFP includes statements, which reflect various assumptions and assessments arrived at by GSCL in relation to this scope. This Tender document does not purport to contain all the information each Bidder may require. This Tender document may not be appropriate for all persons, and it is not possible for the Managing Director, GSCL and their employees or advisors to consider the objectives, technical expertise and particular needs of each Bidder. The assumptions, assessments, statements and information contained in the Bid documents, may not be complete, accurate, adequate or correct. Each Bidder must therefore conduct its own analysis of the information contained in this RFP and to seek its own professional advice from appropriate sources.

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

GSCL and their employees and advisors make no representation or warranty and shall incur no liability to any person, including the Bidder under law, statute, rules or regulations or tort, the principles of restitution or unjust enrichment or otherwise for any loss, cost, expense or damage which may arise from or be incurred or suffered on account of anything contained in this RFP or otherwise, including the accuracy, reliability or completeness of the RFP, and any assessment, assumption, statement or information contained therein or deemed to form part of this RFP or arising in any way in this Selection Process.

GSCL also accepts no liability of any nature whether resulting from negligence or otherwise howsoever caused arising from reliance of any Bidder upon the statements contained in this RFP. GSCL may in its absolute discretion, but without being under any obligation to do so, can amend or supplement the information in this RFP.

The issue of this Tender document does not imply that GSCL is bound to select a Bidder or to appoint the Selected Bidder (as defined hereinafter), for implementation and GSCL reserves the right to reject all or any of the Bidders or Bids without assigning any reason whatsoever.

The Bidder shall bear all its costs associated with or relating to the preparation and submission of its Bid including but not limited to preparation, copying, postage, delivery fees, expenses associated with any demonstrations or presentations which may be required by GSCL or any

other costs incurred in connection with or relating to its Bid. All such costs and expenses will remain with the Bidder and

GSCL shall not be liable in any manner whatsoever for the same or for any other costs or other expenses incurred by a Bidder in preparation for submission of the Bid, regardless of the conduct or outcome of the Selection process.

## 2.0 GLOSSARY

<b>Terms</b>	<b>Meaning</b>
ANPR	Automatic Number Plate Recognition
AP	Access Points
APDCL	Assam Power Distribution Company Ltd.
BOM	Bill of Material
CCTV	Closed Circuit Television
COP	Common Operating Picture
DC	Data Centre
FMS	Facility Management Services
GIS	Geographical Information Systems
GOA	Govt of Assam
GPS	Global Positioning System
GSCL	Guwahati Smart City Limited
GSM	Global System for Mobile Communication
ICCC	Integrated Command and Control Center
ICOC	Integrated Command and Operation Center
ICT	Information and Communication Technology
IOE	(Internet of Everything
IOP	Integrated Operation Platform
IP	Internet Protocol
IT	Information Technology
ITMS	Integrated Traffic Management System
KPI	Key Performance Indicator
MSI	Master System Integrator
O&M	Operations and Maintenance
OEM	Original Equipment Manufacture
OFC	Optical Fiber Cable
PoP	Point of Presence
PTZ	Pan Tilt Zoom
PWD	Public Work Department
RFP	Request for Proposal
RLVD	Red Light Violation Detection
SDC	State Data Centre

<b>Terms</b>	<b>Meaning</b>
SI	System Integrator
SI	System Integrator
SLA	Service Level Agreement
SOP	Standard Operating Procedures
SVD	Speed Violation Detection
TPA	Third Party Auditor
UAT	User Acceptance Testing
UPS	Uninterrupted Power Supply
VA	Video Analytics
VM	Virtual Machine
VMS	Video Management System

### **3.0 INTRODUCTION**

#### **3.1 Project Background**

Guwahati has incorporated a special purpose vehicle (SPV) – Guwahati Smart City Limited (GSCL) (the 'Authority') to plan, design, implement, coordinate and monitor the smart city projects in Guwahati. GSCL is a company incorporated under Indian Companies Act 2013 with equal shareholding from Govt. of Assam.

One of the primary objectives of GSCL under its smart city mission is to enhance the safety and security, improve traffic management, improve efficiency of municipal services and promote a better quality of life for residents. In order to achieve these objectives, GSCL desires to foster the development of a robust ICT infrastructure that supports digital applications and ensures seamless steady state operations, city transport services, traffic management, surveillance, emergency response mechanisms, real time tracking of services and vital city metrics throughout the city and in government departments.

Following city-wide domains will be covered under the scope of this project through the Information's & Communication Technology (ICT) initiatives.



It may be noted that, the permanent Integrated Command Control Centre (ICCC) is yet to be created at a suitable location in the city, hence this project is envisaged to be implemented in two phases in the following manner.

1. **Temporary Phase**
2. **Permanent Phase**

### **Temporary Phase**

In this phase, GSCL will provide a space approximately 5000 SQF for temporary ICCC at BSNL Bhawan (Administrative Building) at Cotton Road, Pan Bazar, Guwahati. Space for Data Centre will be provided in State Data Centre through the Department of Information & Technology, Govt of Assam. Data Centre & Disaster Recovery Centre shall be remains with State Data Center irrespective of ICCC locations. SI must provide the following arrangement at temporary location.

- a) A fully furnished 15-Seater ICCC with minimum furniture, fixtures, workstations etc.
- b) Power Supply arrangement for ICCC
- c) A Video-Wall & other accessories.
- d) Conference/ Meeting Room of about 15-Seater
- e) Managers Cabin – 2 Nos
- f) Rack & Server Space for ICCC, NOC and City Operation Centre
- g) DG & UPS Power Backups for the all the equipment's in the temporary ICCC.
- h) HVAC System.

SI has to note and load the above components including all other necessary costs in his price bid for complete solution of the system as per the detailed scope of works mentioned in section 4.0 and include the all cost under the work enablement at Temporary ICCC & Shifting of ICCC.

### **Permanent Phase**



Once the permanent ICCC Building is ready, SI must make all the shifting arrangement from the temporary ICCC building to the permanent ICCC building and quote a lump sum price for the same in the price bid. The shifting must happen in a time bound manner & shall be completed within **30 days** so that the all the services can be restored on priority.

System Integrator to note that irrespective of the ICCC location, all the data under this Project shall be hosted at State Data Centre. All the above equipment's except civil work will be shifted to new permanent ICCC building.

### 3.2 Standards & Protocols

The System Integrator project under this RFP shall comply with the following standards and protocols as well as others as may be applicable:

S. No.	Standard/Protocol	Remarks
1	Localisation and Language Technology Standards	Unicode Standards 5.1.0 and future upgrades, ISO/IEC 14496-OFF
2	Copy Right	Proper copyright policy
3	Use of National Emblem	Directives as per the 'State Emblem of India (Prohibition of improper use) Act, 2005'.
4	Domain name convention	Government's Domain Name Policy
5	Link with National Portal	As per guidelines provided in at <a href="http://india.gov.in/linktous.php">http://india.gov.in/linktous.php</a>
6	Content Hyper linking	Hyperlinking Policy
7	Open APIs/Open Standards like One M2M	<a href="http://egovstandards.gov.in/frameworkinstitutional-mechanism-and-policies">http://egovstandards.gov.in/frameworkinstitutional-mechanism-and-policies</a>
8	Internet of Things	Sensors & Actuators (IEEE 1451), Identification technology (ISO/IEC JTC 1/SC 31), Domain Specific Compliance-respective domain specific standards like HL 7 for healthcare devices etc.
9	Communication Technology	Thread, AllJoyn, IEEE 802.15.4, IETF 6 LoWPAN, IETFROLL, IETF CoAP
10	Use Case/Application Specific	Domain specific standards like IEEE 11073 for e-health etc.
11	Consortia	Open Interconnect consortium, Industrial Internet Consortium
12	Architecture Technology	IEEE P2413
13	Disaster Management	Please refer Annexure B

S. No.	Standard/Protocol	Remarks
14	Cyber Security	Cyber Security Model Framework for Smart Cities vide Ministry of Housing and Urban Affairs (erstwhile Ministry of Urban Development), Government of India OM No. K-15016/61/2016 SC-1 dated 20th May 2016.
15	Information Security	ISO 27001
16	IT Infrastructure Management	ITIL specifications
17	Service Management	ISO 2000 specifications
18	Project Documentation	IEEE/ISO/CMMi
19	Differently abled people	Should be compliant with The Rights of Persons with Disabilities Act, 2016 and related guidelines.

### 3.3 Project Broad Scope

The bidders shall be responsible to carry out the detailed survey prior to start of implementation of scope of work for the complete solution component requirement in order to finalize infrastructure requirement, network bandwidth requirement, operational & administrative challenges etc.

The subsequent sections detail out the solution and scope with respect to each of the solution component. The SI shall note that the activities defined within scope of work mentioned are indicative and may not be exhaustive. SI is expected to perform independent analysis of any additional work that may be required to be carried out to fulfil the requirements as mentioned in this RFP and factor the same in its response. The subsequent sections detail out the solution and scope with respect to each of the solution component.

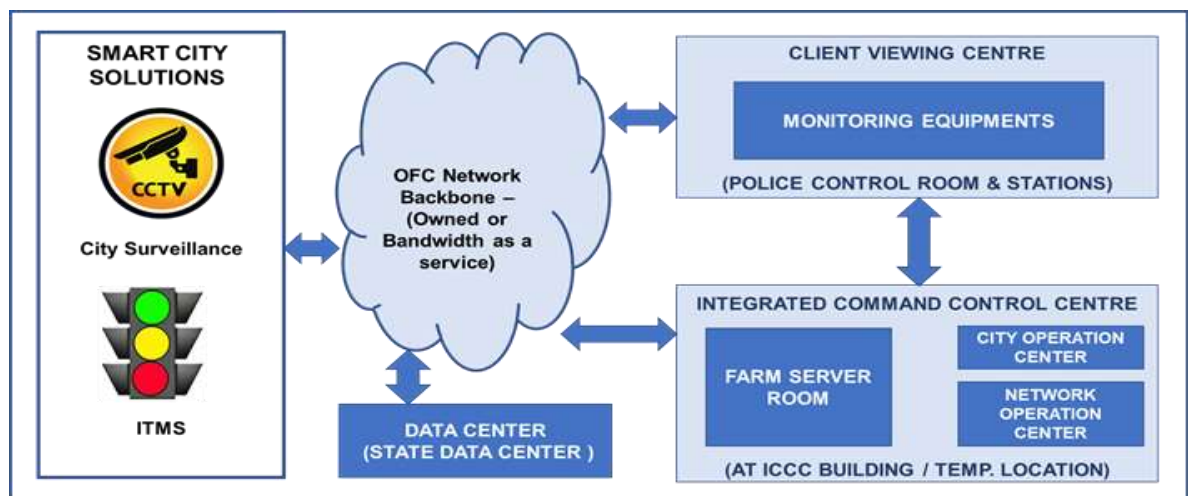


Figure 1: Diagrammatic Representation of Scope of Work for System Integrator

### 3.4 Project Objectives

The core objective is to create a supporting mechanism for the city law enforcement agencies through 24x7 surveillance and monitoring throughout the city as well as enable proactive identification of security issues leveraging intelligent analytics from the surveillance system. Along with city surveillance a dedicated ITMS system with Traffic violation detection system is also planned. This ITMS with traffic violation detection system would be used to monitor and control traffic signals, including signalized pedestrian crossings, using a traffic responsive strategy based on real time traffic flows obtained using vehicle presence sensors.

- Implementation of Fixed, Dome and PTZ cameras with edge analytics capabilities in **661 locations** (Including the 145 Bus Stops and 23 Nos of AMTRON - POP sites)
- Implementation of ITMS system including the Adaptive Traffic Signal Control system along with RLVD & ANPR Camera at **64 location**
- Implementations of ANPR camera at every entry & exit point to the city on the Major Highways.
- Implementations of SVD system at **3 locations** (By-pass Road & Airport Road)
- Intelligent Video analytics at edge devices locations and centralized.
- Develop a full-fledged Integrated Command & Control Centre (ICCC) for ensuring 24X7 monitoring and enabling effective action to be taken in case of law and order/ disaster/ traffic situations
- Integration with existing safety & surveillance systems already implemented as part of the initiative taken by Police department etc.

The system is to be designed taking into consideration the future scalability and integration with upcoming systems.

The system shall help to meet the following objectives:

- Safety and Security
- Improved & Smooth Traffic Movement in the City
- Effective Policing
- Improved Responsiveness
- Improved Management

Ensuring safety and security in fragile settings remains among the department's key objectives in addition to handling crisis management during serious incidents, the list of strategic objectives include:

Safety and Security	<ul style="list-style-type: none"> <li>• Live monitoring of critical infrastructures, city entry &amp; exit points, important locations/ public places in city area like area near to railway stations, airport, bus stops and other public places through surveillance camera.</li> <li>• Live monitoring and control of Traffic Signals, Live monitoring of over speeding vehicles, live monitoring of vehicles passing through important locations of the city including entry and exit points.</li> <li>• Live alerts in case of an event/ incident.</li> <li>• Help to identify, apprehend and prosecute offenders.</li> <li>• Monitoring of suspicious people, activity, vehicles, objects etc. with respect to protecting life &amp; property and maintaining law and order in the city.</li> </ul>
Improved Responsiveness	<ul style="list-style-type: none"> <li>• Access to Police by the Citizens for quick and effective response, improved visibility and transparency.</li> <li>• Better Management of Security breaches based on alerts received from system.</li> <li>• Provide assistance to emergency services and fast turn-around time.</li> </ul>
Effective Policing	<ul style="list-style-type: none"> <li>• Address detection of hot listing vehicles.</li> <li>• Assist in management and policing of large-scale events (political, religious etc.).</li> <li>• Aid to investigation by Police Department by integration of analytic tools.</li> <li>• Providing evidence for criminal and civil action in the courts.</li> </ul>
Improved Traffic Movement in the City	<ul style="list-style-type: none"> <li>• Address the manual Traffic Signalling in the city.</li> <li>• Optimizing the traffic movement with help of Adaptive Traffic Signal Control</li> </ul>
Improved Management	<ul style="list-style-type: none"> <li>• Help in maintaining Law &amp; Order situations.</li> <li>• Help in improving traffic discipline.</li> </ul>

#### 4.0 PROJECT SCOPE OF WORK

##### 4.1 Geographical Scope of services

The following is a summary of the geographical extent of the project.

#	System Description	Locations
1	Integrated Traffic Management System (ITMS) - Adaptive Traffic Signal Control	64 Junctions
2	ANPR & RLVD Systems at Traffic Junctions	

#	System Description	Locations
3	Speed Violation Detection at selected locations (SVD)	3 Locations
4	Surveillance System (Fixed, Dome and PTZ Cameras)	638 CCTV Camera Locations + 23 POP sites
5	Data Center (DC)	DC at State Data Centre
6	Integrated Command & Control Center (ICCC)	Initially at a temporary location to be provided by GSCL and later on SI to shift the ICCC at permanent building.

The Indicative list of locations to be covered under this project are provided as Annexure VIII under section of 12.0.

#### 4.2 Overview of Scope of Services

The System Integrators scope of work shall include but will not be limited to the following broad areas. Details of each of these broad areas have also been outlined in Section -5.0.

1. **Assessment, Scoping and Survey Study:** Conduct a detailed assessment, scoping study and develop a comprehensive project plan, including:
  - a. Assess existing systems, street infrastructure and connectivity within the city for the scope items mentioned in section 4.3
  - b. Conduct site survey for finalization of detailed technical architecture, gap analysis and project plan
  - c. Conduct site surveys to identify need for site preparation activities
  - d. Obtain site Clearance obligations & other relevant permissions
  
2. **Design, Supply, Installation, Commissioning and Testing which includes the following components:** Bidder is flexible to choose best hardware & software as per their proposed solutions to meet the desired requirement and minimum specified standards in documents.
  - a. Integrated Traffic Management System (Adaptive Traffic SignalControl)
  - b. City Surveillance System
  - c. ANPR, RLVD & SVD System
  - d. Integrated Command and Control Centre
  - e. Data Centre

#### 3. Operation and Maintenance Phase:

The SI will also be responsible for supply of IT solution for the management of hardware and application software, networking, installation, Training, Maintenance and operations of the solution for the period of 5 years from the Go Live date. The O&M period will commence after Go- Live and will be for a period of 5 years. Warranty period of the product supplied under this project i.e. hardware, software, IT/Non-IT etc., will be considered after Go-Live. Any cost for extension of warranty if required, shall be borne by the System Integrator and GSCL shall make no extra payment for this.

**4. Integration with provisions available for Network Connectivity within the city which includes:**

- a. Integration of all CCTV Surveillance Components and ITMS (ATSC) including the ANPR, RLVD, SVD system with central Monitoring station (ICCC) and State Data Centre (SDC) with suitable optical network.
- b. Bidder shall utilize the State-owned OFC Network infrastructure and strengthening of the network to meet the connectivity requirements for all proposed components.
- c. Internet connectivity procured as part of this tender.

**5. Provisioning Hardware and Software Infrastructure:** Which includes design, supply, installation, and commissioning of IT Infrastructure at Data Center (DC), Integrated Command & Control Center (ICCC). This consist of:

- a. Basic Site preparation services
- b. IT Infrastructure including server, storage, other required hardware, application portfolio, licenses
- c. Command Center infrastructure including operator workstations, IP phones, joystick controller etc.
- d. Establishment of LAN and WAN connectivity between ICCC and DC limited to scope of infrastructure procured for the project.
- e. RF connectivity to 100% of ITMS Signal Crossing for network redundancy.

**6. Phase wise Integration of the ICT systems with Integrated Command & Control Center (ICCC):**

- a. Integrated Traffic Management System (ITMS)
- b. City Surveillance System - CCTV
- c. ANPR & RLVD System
- d. SVD Camera System
- e. Geographical Information System (GIS)
- f. Any other sensors/systems
- g. Grievance Management

- 7. Capacity Building:** Capacity building for GSCL and other end user department which includes preparation of operational manuals, training documents and capacity building support, including:
  - a. Training of the city authorities, police personnel and operators on operationalization of the system
  - b. Support during execution of acceptance testing
  - c. Preparation and implementation of the information security policy, including policies on backup and redundancy plan
  - d. Developing standard operating procedures for operations management and other services to be rendered by ICCC
- 8. Documentation:** Preparation of all system documents, user manuals, performance manuals, Operation manual including the OFC infrastructure, Circuit diagrams, Electrical Diagrams, Diagrams for Cables, Ducts routing and Path, OH & UG OFC Route, Wireless NW Diagram, Route Markers, latitude and longitude of field equipment etc.
- 9. Operations and Maintenance:** O&M services for the software, hardware and other IT and Non-IT infrastructure installed as part of the project after Go-Live and for a period of 5 years from the date of Go-Live. Five years of warranty period of the product supplied under project i.e. hardware, software, IT/Non-IT etc., will be initiated/considered after Go-Live only.

#### **4.3 Assessment, Site Survey and Project Plan**

After signing of contract, the SI needs to deploy local team (based out of Guwahati) proposed for the project and ensure that a Project Inception Report is submitted to GSCL which should cover following aspects:

1. Names of the Project Team members, their roles and responsibilities
2. Approach and methodology to be adopted to implement the Project (which should be in line with what has been proposed during bidding stage but may have value additions / learning in the interest of the project).
3. Responsibility matrix for all stakeholders
4. Risks the SI anticipates and the plans they have towards their mitigation
5. Detailed project plan specifying dependencies between various project activities / sub- activities and their timelines
6. The SI shall conduct a comprehensive As-Is study of the existing infrastructure of Traffic Junctions, CCTV camera locations to establish the key performance indicators (KPIs) for the project. The KPIs of the study shall be included in the survey.

7. The SI shall study the existing business processes, functionalities, existing management systems and applications including MIS reporting requirements.

Additionally, the SI should provide detailed designs specifying the following:

1. High Level Design (including but not limited to) Application architecture, Logical and physical database design, Data dictionary and data definitions, ER diagrams (Entity Relationship Diagram) and other data modelling documents and Physical infrastructure design for devices on the field
2. Concept of Operations for the TO-BE state that covers – Layout of the ICCC, Staffing Requirements, Standard Operating Procedures, Operations Model for 24/7 coverage, Roles and Responsibilities
3. Application component design including component deployment views, control flows, etc.
4. Low Level Design (including but not limited to) Application flows and logic including pseudo code, GUI design (screen design, navigation, etc.), Database architecture, including defining data structure, data dictionary as per standards laid-down by Government of India/ Government of Assam
5. Location of all field systems and components proposed at the junctions, (KML /KMZ file plotted on GIS platform like google earth etc.)
6. Location of Network Provider's Point of Presence (PoP)
7. Design of Cables, Ducts routing, digging and trenching
8. Details survey with link budgeting of RF redundancy network for all ITMS Signal Crossing.
9. Electrical power provisioning.

#### **4.4 Documents/ Drawings Submission after Award of Contract**

SI shall submit documents and drawings as mentioned below within **Three (3) Months** after award of contract for review and approval from Client/ Consultant. Following are the minimum list of documents and drawings to be submitted, however, SI shall not restrict himself to the same and it is in the obligation of the SI to submit all supporting documents, detailed drawings as requested by Client/ Consultant during engineering and execution stage.

##### **Stage 1: Design engineering**

- a) Design basis report and individual system block diagram.
- b) Overall system architecture and flow diagrams
- c) Design calculation sheets for all systems
- d) System and location wise Equipment list along with GIS coordinates
- e) System and location wise Load list/ power requirement
- f) System and location wise UPS load list



- g) System and location wise Heat load calculation list
- h) Technical specifications and datasheets for all systems.
- i) Standard Operating Procedures (SOPs) for Integrated Command & Control Center (ICCC).
- j) Key Performance Indicators (KPIs) for each system.
- k) Electronics Services Delivery (ESD) Rules and services need to be notified as per the Rules.

### **Stage 2: Project execution**

- a) General arrangement drawings.
- b) Job execution schedule
- c) Equipment general arrangement, internal wiring and third-party integration provision
- d) QAP and FAT/ SAT procedures
- e) System/ equipment Installation/ erection drawings.
- f) Installation manuals

### **Stage 3: Post commissioning**

- a) As-built drawings
- b) Training manuals and schedules.
- c) Operation and maintenance manuals.
- d) Spares list (recommended spares, commissioning spares and operation spares)

## **4.5 Finalization of Detailed Technical Architecture**

The SI shall also identify the customizations/ workaround that would be required for successful implementation and operation of the ICCC, DC, Surveillance & ITMS project and finalize the detailed technical architecture for the overall system, incorporating findings of site survey exercise. The network so envisaged should be able to provide real time video stream to the Integrated Command Control Centers and viewing centers (Police Control Room & Police Stations shall be decided by city administrations and GSCL). The System Integrator (SI) shall submit the detailed Technical Architecture, which should take into consideration following guiding principles:

- 1. Scalability** - Important technical components of the architecture must support scalability to provide continuous growth to meet the growing demand of the city. The system should also support vertical and horizontal scalability so that depending on changing requirements from time to time, the system may be scaled upwards. There must not be any system-imposed restrictions on the upward scalability in number of cameras, data center equipment's or other smart city components. Main technology components requiring scalability are storage, bandwidth, computing performance (IT

Infrastructure). The architecture should be scalable (cater to increasing load of internal and external users and their transactions) and capable of delivering high performance till the system is operational. In this context, it is required that the application and deployment architecture should provide for Scale-Up and Scale out on the Application and Web Servers, Database Servers and all other solution components. The data centre infrastructure shall be capable of serving at least 1000 concurrent users.

2. **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 SI shall make the provision for high availability for all the services of the system. Redundancy must be considered at the Core / Data Center components level.
3. **Security** - The architecture must adopt an end-to-end security model that protects data and the infrastructure from malicious attacks, theft, natural disasters etc. SI 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 endeavour 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. The SI shall carry out the security audit for vulnerability Assessment and access control assessment of the entire system upon handover and at regular intervals during O&M period also.

Field equipment installed through this project would become an important public asset. During the contract period of the project the SI shall be required to repair / replace any equipment if stolen/damaged/faulty. Appropriate insurance cover must be provided to all the equipment's supplied under this project.

The systems implemented for project should be highly secure, considering that it is intended to handle sensitive data relating to the city and residents of the city. The overarching security considerations are described below.

- a) The security services used to protect the solution shall include: Identification, Authentication, Access Control, Administration and Audit and support for industry standard protocols.
- b) The solution shall support advanced user authentication mechanisms including digital certificates and biometric authentication.

- c) 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.
  - d) 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.
  - e) The overarching requirement is the need to comply with ISO-27001 standards of security.
  - f) The application design and development should comply with OWASP top 10 principles
- 4. 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. Network should be auto/manual configurable for various future requirements for the ease of maintenance / debugging.
- 5. 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.
- 6. Open Standards** - Systems should use open standards and protocols to the extent possible. Keeping in view the evolving needs of interoperability, especially the possibility that the solution shall become the focal point of delivery of services and may also involve cross-functionality with the e-Government projects of other departments / businesses in future, the solution should be built on Open Standards. The SI shall ensure that the application developed is easily integrated with the existing applications. The code does not build a dependency on any proprietary software, particularly, through the use of proprietary 'stored procedures' belonging to a specific database product. The standards should at least comply with the published e-Governance standards, frameworks, policies and guidelines available on <http://egovstandards.gov.in> (updated from time-to-time)
- 7. Single-Sign ON-** The application should enable single-sign-on so that any user once authenticated and authorized by system is not required to be re-authorized for completing any of the services in the same session. For employees of the department concerned, the browser-based application accessed on the intranet, through single-sign-on mechanism, will provide access to all the services of the departments concerned (based on their roles and responsibilities), Help module, basic and advanced reporting etc. Similarly, for external users (citizens, etc.), based on their profile and registration, the system shall enable single-sign on facility to

apply for various services, make payments, submit queries /complaints and check status of their applications.

- 8. Support for PKI based Authentication and Authorization-** The solution shall support public key infrastructure (PKI) based Authentication and Authorization, in accordance with IT Act 2000, using the Digital Certificates issued by the Certifying Authorities (CA). In particular, 3 factor authentications (login id & password, biometric and digital signature) shall be implemented by the SI for officials/employees involved in processing citizen services.
- 9. Convergence** - GSCL has already initiated many projects which have state of the art infrastructure at field locations deployed under them. The ICCC Infrastructure should be made scalable for future convergence needs. Under the smart city program, GSCL has envisaged to create a state of the art infrastructure and services for the citizens of Guwahati, hence it is imperative that all infrastructure created under the project shall be leveraged for maximum utilization. Hence the SI is required to ensure that such infrastructure will allow for accommodation of equipment's being procured under other smart city projects. Equipment like Junction Boxes and poles deployed under the ICCC project at the field locations will be utilized.
- 10.** The Platform shall have tightly integrated Asset Management System to have all relevant information of all assets in Smart City Area to give real time status of assets & update automatically in case of failure.
- 11. ICCC** - Applications should have mobility devices & applications for field staff to ensure fast restoration of services in case of alarms & issues. In case of non-attending of alarm, decision escalations will be done automatically. After closure of issue the workflow must be closed with feedback from those devices.
- 12. Historian** – ICCC Application should have an inbuilt Historian. All the personnel working on the Project and having access to the Servers / Data Center should be on direct payroll of the SI/OEM/Consortium partner. The SI would not be allowed to sub-contract work, except for following:
  - a) Passive networking & civil work during implementation and O&M period,
  - b) Viewing manpower at ICCC during post-implementation
  - c) FMS staff for non- IT support during post-implementation
  - d) Services of professional architect for design of ICCC

However, even if the work is sub-contracted , the sole responsibility of the work shall lie with the SI. The SI shall be held responsible for any delay/error/non-compliance/penalties 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 GSCL and approved by the GSCL before resource mobilisation.

**13. GIS Integration-** SI shall undertake detail assessment for integration of the Surveillance System and all other components with the Geographical Information System (GIS). SI is required to carry out the seamless integration to ensure ease of use of GIS in the Dashboards in Command Control Centre. If this requires field survey, it needs to be done by SI. If such a data is already available with city, it shall facilitate to provide the same. SI is to check the availability of such data and it's suitability for the project. SI is required to update GIS maps from time to time.

**14. SMS Gateway Integration-** SI shall carry out SMS Gateway Integration with the Smart City System and develop necessary applications to send mass SMS to groups/individuals. Any external/third party SMS gateway can be used, but this needs to be specified in the Technical Bid, and approved during Bid evaluation.

### **15. Application Architecture**

- a) The applications designed and developed for the departments concerned must follow best practice and industry standards. In order to achieve the high level of stability and robustness of the application, the system development life cycle must be carried out using the industry standard best practices and adopting the security constraints for access and control rights. The various modules / application should have a common Exception Manager to handle any kind of exception arising due to internal/ external factors.
- b) The modules of the application are to be supported by the Session and Transaction Manager for the completeness of the request and response of the client request. The system should have a module exclusively to record the activities/ create the log of activities happening within the system / application to avoid any kind of irregularities within the system by any User / Application.
- c) SI shall design and develop the ICCC System as per the Functional and System requirement specifications finalized.
  - I. The Modules specified will be developed afresh based on approved requirement.
  - II. Apart from this, if some services are already developed/under development phase by the specific department, such services will be integrated with the ICCC System. These service will be processed through department specific Application in backend.
  - III. The user of citizen services should be given a choice to interact with the system in local language in addition to English. The application should provision for uniform user experience across the multi lingual functionality covering following aspects:
    - Front end web portal in English and local language
    - E-forms (Labels & Data entry in local languages). Data entry should be provided preferably using the Enhanced In script standard (based

- on Unicode version 6.0 or later) keyboard layout with option for floating keyboard.
  - Storage of entered data in local language using UNICODE (version 6.0 or later) encoding standard.
  - Retrieval & display in local language across all user interfaces, forms and reports with all browsers compliant with Unicode version 6.0 and above.
  - Facility for bilingual printing (English and the local language)
- IV. Application should have a generic workflow engine for citizen centric services. This generic workflow engine will allow easy creation of workflow for new services. At the minimum, the workflow engine should have the following features:
- Feature to use the master data for the auto-populating the forms and dropdowns
  - Creation of application form, by “drag & drop” feature using meta data standards
    - i. Defining the workflow for the approval of the form
    - ii. First in First out
    - iii. Defining a citizen charter/delivery of service in a time bound manner
  - Creation of the “output” of the service, i.e. Certificate, Order etc.
  - Automatic reports
    - i. of compliance to citizen charter on delivery of services
    - ii. delay reports
- d) The application should have a module for management of digital signature including issuance, renewal and suspension of digital signatures based on the administrative decisions taken by the State. SI shall ensure using Digital signatures/e-Authentication(Aadhar Based) to authenticate approvals of service requests etc.

#### 1. e-Transaction & SLA Monitoring Tools

- The SI should be able to measure and monitor the performance of the deployed infrastructure and all SLAs set out in this RFP. More importantly, it should be possible to monitor in REALTIME, the number of citizens touched through e- Services each day, month and year, through appropriate tools and MIS reports.
- The Infrastructure management and Monitoring System shall be used by SI to monitor the infrastructure (Both IT and Non-IT) hosted at the Data center and DR site.

- For monitoring of uptime and performance of IT and non-IT infrastructure deployed, the SI shall have to provision for monitoring and measurement tools, licenses, etc. required for this purpose.
2. The ICCC Application should have roadmap to integrate with key initiatives of State namely Portal Services, Citizen Contact Centre, Certifying Authority etc.
  3. Complete mobile enablement of the ICCC System

The functional requirements and technical specifications provided in this RFP are indicative and carry guiding rule. The SI is free to offer products and solutions which meet requirements of the RFP focusing on the outcome, future scalability, security, reliability and adherence to specified SLA under this RFP, in line with applicable standards & best practices adopted in the industry. The SI is encouraged to design an Optimized solution which is technically superior, innovative, proven, better in terms of functionality and is cost effective. Any specified parameters mentioned in the scope/technical requirement in the RFP may be considered if it is required for meeting current & future requirements during the contract period. The SI is fully responsible for the specified outcome to be achieved.

#### **4.6 Site Clearance Obligations and Other Relevant Permissions**

##### **4.6.1 Survey And Commencement of Works**

Prior to starting the site clearance, the SI shall carry out survey of field locations as specified in Annexure VIII under section of 12.0, for buildings, structures, fences, UG utilities' – Power Cables & Water Pipelines, OFC NW of other Operators, Trees, existing installations, etc. The GSCL shall be fully informed of the results of the survey and the amount and extent of the demolition and site clearance shall then be agreed with the GSCL.

##### **4.6.2 Existing Traffic Signal system**

The infrastructure of existing traffic signal systems including the aspects, controllers etc. will be dismantled and replaced with the new systems which are proposed and required under the scope of this project. The dismantled infrastructure shall be delivered at the GSCL designated location without damage at no extra cost.

##### **4.6.3 Electrical Works and Power Supply**

The SI shall directly interact with APDCL for provision of mains power supply at all locations for ICCC field systems. The SI shall be responsible to pay the electricity bills including connection charge, meter charge, recurring charges etc. to the APDCL directly. SI shall have to submit the challan of bill submission to GSCL. GSCL will reimburse the amount deposited by the SI after verification in next billing cycle.

#### **4.6.4 Miscellaneous:**

1. Authority shall assist in obtaining all necessary go ahead, legal permissions, NOC (No Objection Certificate) from various departments to execute the project. SI shall have to identify and obtain necessary legal / statutory clearances for erecting the poles and installing cameras, for provisioning of the required power, etc. SI shall provide & manage all necessary paper work to pursue permission from respective authorities. No commercial/legal fees (except the RoW charges) shall be applicable to Authority for obtaining the necessary permissions. These shall be provisioned for by the SI in their financial bid.
2. The SI shall provide all material required for mounting of components such as cameras and other field equipment. All mounting devices for installation of CCTV cameras such as mounting bracket, Lens, Weather proof housing, Pole, Junction Box, Power Supply, Cables, accessories, etc. shall be included in the costs of the respective component. The same is also applicable to crossheads and cross arms, mounting brackets, stainless steel bands, screws and other accessories.
3. All the equipment, software and workmanship that form a part of the service are to be under O&M from the SI throughout the contract period.
4. SI shall also get comprehensive insurance from reputed insurance company for the project duration for all the equipment's / components installed under this project.
5. SI shall ensure all the equipment's installed in the outdoor locations are vandal proof and in case the equipment's get damaged /stolen for reasons whatsoever, it shall repair/replace the same in the specified time as per SLAs at no extra cost to the Authority. All such costs shall be factored in the comprehensive insurance of field equipment for the duration of the contract.
6. Preventive maintenance shall be carried out once in a quarter along with corrective maintenance and also when calls are placed by Authority or its designated agency.
7. In addition to above, the SI shall be fully responsible for all maintenance activities for the period between installation of equipment and roll-out of the system.
8. During implementation, if observed that any camera / field equipment requires change in the field of view / orientation, it shall be done by SI without any extra cost.
9. In case of request for change in location of field equipment post installation, the same shall be borne by Authority at either a unit rate as per commercials or a mutually agreed cost.



#### **4.7 Other Expectations from System Integrator (SI)**

1. SI shall engage early in active consultations with the Authority, City Police and other key stakeholders to establish a clear and comprehensive project plan in line with the priorities of all project stakeholders and the project objectives.
2. Study the existing fiber duct (if any) layout in the city and existing network to understand the existing technology adopted in each of the following areas (not limited to):
  - i. City wide OFC network provided by State Owned Network Provider / GSCL own Network.
  - ii. Surveillance Infrastructure – CCTV Cameras, Data Communication, Data Centre, Monitoring, Control Room and Infrastructure provided by State Owned Network / GSCL own Network..
  - iii. ITMS – Locations of Traffic Signals, Data Communication, Data Centre, Monitoring, Control Room and Infrastructure provided by State Owned Network / GSCL own Network.
3. SI shall assess existing infrastructure's current ability to support the entire solution and integrate the same with the proposed solution wherever applicable and possible.
4. SI shall judiciously evaluate the resources and time planned for undertaking the current state assessment, given the overall timelines and milestones of the project.
5. SI shall be responsible for supply of all the Active-Components (Products/Equipment) such, Hardware, Software, Devices, etc. as indicated (but not limited to) in the tentative Bill of Materials included in the RFP and their appropriate quantity & capacity.
6. SI shall be responsible for supply of Passive-Components as indicated (but not limited to) in the Bill of Materials section of the RFP along with other essential items which required to fulfill the scope of this RFP, viz. Housings, Fiber Patch Cords, Racks etc. All civil work required for the site shall also be undertaken by the SI.
7. Validate / Assess the re-use of the existing infrastructure if any with Authority.
8. Supply, Installation, and Commissioning of entire solution at all the locations.
9. SI shall establish high availability, reliability and redundancy of the network elements to meet the Service Level requirements.
10. SI shall be responsible for planning and design of the access network architecture (access controllers, backhaul connectivity, routers, switches, etc.) to meet the technical, capacity and service requirements for all smart city initiatives.

11. SI shall be responsible for upgradation, enhancement and provisioning additional supplies of network (including active / passive components), hardware, software, etc. as requisitioned by Authority.
12. SI shall ensure that the end of support is not reached during the concurrency of the contract and 5 years thereafter.
13. SI shall be responsible for maintaining the SLA for the complete NW infrastructure (either maintained by self or other agency), including all City Optical fiber network (Which shall be maintained by Network Service Provider) for the period of five (5) years after final acceptance testing and handover the complete systems to the Authority after project defeat liability period. Authority has full right to use the city network for his other requirements of connecting the existing and or upcoming systems and solutions for entire contract period and thereafter.
14. SI shall ensure compliance to all mandatory government regulations as amended from time to time.
15. The SI shall ensure that all the peripherals, accessories, sub-components required for the functionality and completeness of the solution, including but not limited to devices, equipment, accessories, patch cords (fiber), cables, software, licenses, tools, etc. are provided according to the requirements of the solution.
16. SI is required to maintain the spares for all the components minimum 5% or 2 no's whichever is more during the O&M period and handover the same on completion of the contract.
17. Authority shall not be responsible if the SI has not provisioned some components, sub-components, assemblies, sub-assemblies as part of Bill of Materials in the RFP. The SI shall have to provision these & other similar things to meet the solution requirements at no additional cost and time implications to Authority.
18. All the software licenses that the SI proposes shall be perpetual software licenses along with maintenance, upgrades and updates for the concurrency of the entire contract period. The software licenses shall not be restricted based on location and Authority shall have the flexibility to use the software licenses for other requirements if required.
19. The SI shall ensure there is a 24x7 comprehensive onsite support for duration of the contract for respective components to meet SLA requirement. The SI shall ensure that all the OEMs understand the service levels required by Authority. SI is required to provide the necessary MAF (Manufacturer Authorization Form) as per the format provided in the RFP in support of OEMs active support in the project.

20. The SI is required to keep the preventive maintenance / corrective maintenance van for the complete O&M Period.
21. The SI must provide the System Architecture drawings, System Integration drawings, Location layout, Component Specifications, etc. for the Authorities / the engineer's review.
22. All the necessary components required for systems to function completely are required to be supplied without any extra cost. The SI has to consider the cost of these components and load in their price bid.
23. Considering the criticality of the infrastructure, SI is expected to design the solution considering the RFP requirement of no single point of failure with high level of redundancy and resilience to meet the network uptime requirements.
24. SI shall be responsible for periodic updates & upgrades of all equipment, cabling and connectivity provided at all locations during the contract period.
25. SI shall be responsible for setting up / building / renovating the necessary physical infrastructure including provisioning for network, power, rack, etc. at all the locations.
26. SI is expected to provide following services, including but not limited to:
  - a) Provisioning hardware and network components of the solution, in line with the proposed authority's requirements
  - b) Size and propose for network devices (like Router, switches, security equipment including firewalls, IPS / IDS, routers, etc.) as per the location requirements with the required components/modules, considering redundancy and load balancing in line with RFP.
  - c) Size and provision the WAN bandwidth requirements across all locations considering the application performance, data transfer and other requirements for smart city initiatives.
  - d) Size and provision the internet connectivity for Service Provider network and Network Backbone.
  - e) Liasoning with NW service providers for commissioning and maintenance of the links in case of any service degradation.
  - f) Furnish a schedule of delivery of all IT/Non-IT Infrastructure items
  - g) All equipment proposed as part of this RFP shall be rack mountable.
  - h) Authority may at its sole discretion evaluate the hardware sizing document proposed by the SI. The SI needs to provide necessary explanation for sizing to the Authority
  - i) Complete hardware sizing for the complete scope with provision for upgrade
  - j) Specifying the number and configuration of the racks (size, power, etc.) that shall be required at all the locations.

- k) The SI shall provide for all required features like support for multiple routing protocols, congestion management mechanisms and Quality of Service support.
- l) The SI shall ensure that all active equipment (components) are Simple Network Management Protocol (SNMP) V3 compliant and are available for maintenance/management through SNMP from the date of installation by a Network Monitoring System.

#### **4.8 Design and Implementation of Integrated Command & Control Center System**

The SI should ensure the successful implementation of the proposed ICCC Project as per the scope of services described below. SI shall implement and deliver the following systems and capabilities linked ICCC.

1. Integrated Traffic Management System (ITMS)
  - a) Adaptive Traffic Signal Control
  - b) Traffic Violation Detection System
  - c) ANPR, RLVD, SVD System
2. City Surveillance System – CCTV (Fixed, PTZ, Dome)
3. Network Connectivity – OFC Backbone & Access Network
4. Data Center (DC) & Disaster Recovery Center.

#### **4.9 Design, Supply, Installation & Commissioning of the Field Equipment**

The Scope includes Supply, Installation, commissioning and Customization (as required) of various field systems which include Integrated Traffic Management System (ITMS) at Traffic Junctions, City Surveillance System, DC & DR and other IT infrastructure required for successful operations of the ICCC project.

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

1. The implementation methodology and approach must be based on the global best practices in-order to meet the defined Service Levels during the operation.
2. Best efforts have been made to define major functionalities for each sub- system of ICCC system. However, SI should not limit its offerings to the functionalities proposed in this RFP and is suggested to propose any functionality over and above what has already been given in this tender.
3. The SI shall design the field level equipment architecture to ensure maximum optimization of network equipment, poles, cantilever, mounting infrastructures, power supply equipment including, electric meters and junction box.

4. Finally approved/accepted solution for each component of ICCC project shall be accompanied with "System Configuration" document and the same should be referenced for installation of ICCC systems at Junctions/Locations that are identified within the scope of this project.
5. The SI shall be required to submit a detailed installation report post installation of all the equipment at approved locations. The report shall be utilized during the acceptance testing period of the project to verify the actual quantity of the equipment supplied and commissioned under the project.
6. The SI shall be responsible for obtaining all permissions/ NOC and approvals necessary to install the ICCC systems components as per the approved design.

The sub-systems included as part of the ICCC project which are required to be implemented and integrated are given in the subsequent sections.

#### **4.10 City Surveillance System – (CCTV Camera)**

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

1. This Component covers planning & implementation of the Surveillance system comprising cameras and other field equipment at identified locations. Actual placement of pole & number of cameras at each location, type of cameras, fixation of height & angle for the cameras to ensure maximum coverage shall be done in consultation with the Guwahati Smart City authority.
2. A detailed survey shall be conducted, by the SI along with a team of Authority and the Guwahati police, at each of the strategic locations. This survey shall finalize the position of all field equipment's and the orientation/ field of view of the cameras. Appropriate field of view snapshot shall be taken by a handheld camera for future reference at the time of survey. The surveyors shall also finalize the approximate location of foundation for junction box and camera poles. The route for all the underground cable laying shall be finalized during this survey (wherever required). Every detail, finalized during the survey, shall be demarcated on an AutoCAD drawing by the SI and submitted to Authority in the form of a detailed site survey report along with other details for its approval.
3. The SI shall install Surveillance System Cameras for CCTV monitoring and management at all locations across Guwahati city mentioned in the respective annexure.
4. The SI shall undertake due diligence for selection and placement of surveillance cameras to ensure the optimized coverage of the traffic junction and other locations along with all associated junction arms, accuracy of the information captured on the field and for rugged operations.

5. The SI shall design, supply, and install the surveillance cameras as defined in the RFP; all wiring connections for the system shall be installed by the SI. The SI shall supply all of the necessary equipment for the camera operations including camera housings and mountings, camera poles, switches, cabling, and shall make the final connections to the junction box.
6. The SI shall be responsible for providing the entire necessary IT infrastructure for monitoring, recording, storage & retrieval of the video streams at ICCC or any other location as specified in the RFP.
7. System shall provide inter-operability of hardware, operating system, software, networking, printing, database connectivity, reporting, and communication protocols. SI shall prepare the detailed report for field level requirements e.g. Cameras (types & numbers), Camera Mounting requirements, Power Requirements, Connectivity Requirements etc. for perusal of Authority. Indicative list of the field level hardware to be provided by SI is as follows:
  - a. Cameras (Fixed Box Cameras, PTZ Cameras etc.)
  - b. Dome camera for the indoor applications – POP sites monitoring
  - c. Industrial Grade Switches
  - d. Outdoor Cabinets
  - e. Pole for cameras / Mast
  - f. Outdoor Junction box
  - g. UPS
  - h. Networking and power cables and other related infrastructure
  - i. Redundancy RF network equipment at all ITMS signal crossing.
8. SI shall use industry leading practices during the implementation phase w.r.t positioning and mounting the cameras, poles and junction boxes. Some of the check-points that need to be adhered to by the SI while installing / commissioning cameras are as follows:
  - a. Ensure surveillance objective is met while positioning the camera such that the required field of view is being captured as finalized in field survey.
  - b. Ensure camera is protected from the on-field challenges of weather, physical damage and theft.
  - c. Make proper adjustments to have the best possible image / video captured.
  - d. Ensure that the pole is well placed for vibration resistance adhering to the road safety norms.
  - e. Collusion preventive barriers around the junction box & pole foundation in case it's installed in collision prone place.
  - f. Appropriate branding or color coding (Police/Authority Branding) of poles and junction boxes, to warn mischief mongers against tampering with the equipment at the junction.
9. The functional requirements and technical specifications provided in this RFP are indicative and carry guiding rule. The SI is free to offer products and solutions which

meet requirements of the RFP focusing on the outcome, future scalability, security, reliability and adherence to specified SLA under this RFP, in line with applicable standards & best practices adopted in the industry. The SI is encouraged to design an Optimized solution which is technically superior, innovative, proven, better in terms of functionality and is cost effective. Any specified parameters mentioned in the scope/technical requirement in the RFP may be considered if it is required for meeting current & future requirements during the contract period. The SI is fully responsible for the specified outcome to be achieved.

10. For more details on technical and functional specifications of Surveillance Cameras, SI should refer to **Section: 5.0** for Functional and Technical specifications.

#### **4.11 Integrated Traffic Management System (ITMS)**

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

1. Preparation of Solution Architecture for Adaptive Traffic Signal Control System (ATSCS) as per project blueprint to develop a final BOQ for installation of traffic signaling systems.
2. Installation of Vehicle Detectors, Controllers, Traffic Light Aspects, Poles, Cantilevers, Junction Box and other required accessories at 64 Traffic Junctions for successful operation of the ITMS project for Guwahati Smart City.
3. Integration of ITMS field infrastructures with the proposed ITMS software application.
4. Configuration of traffic signal at each of the junction along with development of signal control plan for individual operations, coordinated signal plan for the junction in sync with the area wide signal plan for different operating conditions. The operating conditions may include different peak and off-peak conditions, special events, contingency plans etc.
5. The SI should design and propose energy saving signaling system by using solar powered signals or other advanced technologies.
6. The functional requirements and technical specifications provided in this RFP are indicative and carry guiding rule. The SI is free to offer products and solutions which meet requirements of the RFP focusing on the outcome, future scalability, security, reliability and adherence to specified SLA under this RFP, in line with applicable standards & best practices adopted in the industry. The SI is encouraged to design an Optimized solution which is technically superior, innovative, proven, better in terms of functionality and is cost effective. Any specified parameters mentioned in the scope/technical requirement in the RFP may be considered if it is required for

meeting current & future requirements during the contract period. The SI is fully responsible for the specified outcome to be achieved.

7. For more details on technical and functional specifications of ITMS, SI should refer to Section # 5.3 for Functional and Technical specifications.

#### **4.11.1 Traffic Violation Detection System**

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

1. The SI shall install the Traffic Violation Detection System at 64 traffic junctions across the city. This system shall capture the infractions of Red light and stop line violations at these junctions.
2. The SI shall design, supply, and install the Traffic Violation Detection System as defined in the RFPs, all wiring connections to the traffic signal controllers and to the camera platforms shall be installed by the SI. The SI shall supply all of the necessary equipment for the camera and detection system, including but not limited to: computers, ancillary camera equipment, camera housings, camera poles, warning signs and shall make the final connections to the camera.
3. The solution proposed by the SI shall seamlessly integrate with the E-Challan system proposed under the scope of this project. GSCL shall facilitate to get access to the Vaahan and Sarathi database. Bidder shall be required to access the same through use of appropriate APIs.
4. The SI shall be responsible for providing all the necessary IT infrastructure for analysis, storage & retrieval of the infraction information at ICCC or any other location as specified in the RFP.
5. The functional requirements and technical specifications provided in this RFP are indicative and carry guiding rule. The SI is free to offer products and solutions which meet requirements of the RFP focusing on the outcome, future scalability, security, reliability and adherence to specified SLA under this RFP, in line with applicable standards & best practices adopted in the industry. The SI is encouraged to design an Optimized solution which is technically superior, innovative, proven, better in terms of functionality and is cost effective. Any specified parameters mentioned in the scope/technical requirement in the RFP may be considered if it is required for meeting current & future requirements during the contract period. The SI is fully responsible for the specified outcome to be achieved.
6. For more details on technical and functional specifications of Traffic Violation Detection system, SI should refer to Section: 5.0 for Functional and Technical specifications.



#### **4.11.2 ANPR System**

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

1. The SI shall install the ANPR Cameras at every entry & exit points of the city on major highway and 64 ITMS junctions/locations across the city. This system shall automatically capture the license number plate of the vehicle at these junctions.
2. The SI shall design, supply, and install the ANPR camera system as defined in the RFPs, all camera accessories such as IR Illuminators, camera housing and mounting shall be installed by the SI. The SI shall supply all of the necessary equipment for the camera and local processing system, including but not limited to: computers, local storage, and ancillary camera equipment, camera poles, warning signs and shall make the final connections to the camera.
3. The SI shall be responsible for providing all the necessary IT infrastructure for detection, analysis, storage & retrieval of the number plate information at ICCC or any other location as specified in the RFP.
4. The functional requirements and technical specifications provided in this RFP are indicative and carry guiding rule. The SI is free to offer products and solutions which meet requirements of the RFP focusing on the outcome, future scalability, security, reliability and adherence to specified SLA under this RFP, in line with applicable standards & best practices adopted in the industry. The SI is encouraged to design an Optimized solution which is technically superior, innovative, proven, better in terms of functionality and is cost effective. Any specified parameters mentioned in the scope/technical requirement in the RFP may be considered if it is required for meeting current & future requirements during the contract period. The SI is fully responsible for the specified outcome to be achieved.
5. For more details on technical and functional specifications of ANPR Cameras, SI should refer to Section: 5.0 for Functional and Technical specifications.

#### **4.11.3 RLVD System**

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

1. The SI shall install the RLVD Systems at 64 traffic junctions across the city. This system shall capture the infractions of Red light and stop line violations at these junctions.
2. The SI shall design, supply, and install the RLVD system as defined in the RFPs, all wiring connections to the traffic signal controllers and to the camera platforms shall be installed by the SI. The SI shall supply all the necessary equipment for the

camera and detection system, including but not limited to: computers, ancillary camera equipment, camera housings, camera poles, warning signs and shall make the final connections to the camera.

3. The SI shall be responsible for providing all the necessary IT infrastructure for detection, analysis, storage & retrieval of the number plate information at ICCC or any other location as specified in the RFP.
4. The solution proposed by the SI shall seamlessly integrate with the E-Challan system proposed under the scope of this project. GSCL shall facilitate to get access to the Vaahan and Sarathi database. Bidder shall be required to access the same through use of appropriate APIs.
5. The functional requirements and technical specifications provided in this RFP are indicative and carry guiding rule. The SI is free to offer products and solutions which meet requirements of the RFP focusing on the outcome, future scalability, security, reliability and adherence to specified SLA under this RFP, in line with applicable standards & best practices adopted in the industry. The SI is encouraged to design an Optimized solution which is technically superior, innovative, proven, better in terms of functionality and is cost effective. Any specified parameters mentioned in the scope/technical requirement in the RFP may be considered if it is required for meeting current & future requirements during the contract period. The SI is fully responsible for the specified outcome to be achieved.
6. For more details on technical and functional specifications of RLVD Cameras, SI should refer to Section: 5.0 for Functional and Technical specifications.

#### **4.11.4 Speed Violation Detection (SVD) System**

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

1. SVD camera will be installed on major highways of the city.
2. Primarily, SVD will be at 3 major locations along with real time visual indications of speed violation on LED display board.
3. System will be able to record the vehicle speed with proof of video/photograph and event time and date.

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

#### **4.11.5 E-Challan Devices**

The SI is required to supply 64 devices for 64 junctions along with e-Challan application for spot challan issuance. The SI is required to seamlessly integrate the handheld e-Challan application with the E-Challan system proposed under the scope of this project.

The functional requirements and technical specifications provided in this RFP are indicative and carry guiding rule. The SI is free to offer products and solutions which meet requirements of the RFP focusing on the outcome, future scalability, security, reliability and adherence to specified SLA under this RFP, in line with applicable standards & best practices adopted in the industry. The SI is encouraged to design an Optimized solution which is technically superior, innovative, proven, better in terms of functionality and is cost effective. Any specified parameters mentioned in the scope/technical requirement in the RFP may be considered if it is required for meeting current & future requirements during the contract period. The SI is fully responsible for the specified outcome to be achieved.

#### **4.12 Lightning-Proof Measures**

The SI shall comply with lightning-protection and anti-interference measures for system structure, equipment type selection, equipment earthing, power, signal cables laying. The SI shall describe the planned lightning-protection and anti-interference measures in the As-Is report. Lightning arrester for all pole shall be erected for the entrance cables of power line, video line, data transmission cables. All crates shall have firm, durable shell. Shell shall have dustproof, antifouling, waterproof function & should be capable to bear certain mechanical external force. Signal separation of low and high frequency; equipment's protective field shall be connected with its own public equal power bodies; small size/equipment signal lightning arrester shall be erected before the earthing. The Internal Surge Protection Device for Data Line Protection shall be selected as per zone of protection described in IEC 62305, 61643-11/12/21, 60364-4/5. Data line protection shall be used for security system, server data path and other communication equipment. Data line protection shall be installed as per zone defined in IEC 62305. Type 1 device shall be installed between zone 0B and zone 1. Type 2 devices shall be installed before the equipment in zone 2 and 3.

#### **4.13 Earthing System**

All electrical components are to be earthen by connecting two earth tapes from the frame of the component ring and will be connected via several earth electrodes. The cable arm will be earthen through the cable glands. The entire applicable IT infrastructure i.e. field locations/traffic junctions or command centre shall have adequate earthing. Further, earthing should be done as per Local state national standard in relevance with IS standard.

1. SI shall comply with the technical specifications considering lightning-proof and anti-interference measures for system structure, equipment type selection, equipment

earthing, power and signal cable laying. SI shall describe the planned lightning-proof and anti-interference measures in their technical bid.

2. Corresponding lightning arrester shall be erected for the entrance cables of power line, video line, data transmission cables.
3. All interface board and function board, interfaces of equipment shall adopt high speed photoelectric isolation to reduce the damage to integrated circuit CMOS chip due to the surge suppression.
4. Install the earthing devices for the equipment, including lightning earthing, protection earthing and shielded earthing. All earthing shall meet the related industry standards.
5. The earthing cable shall be installed in a secure manner to prevent theft and shall be rust proof. Earthing down lead and the earthing electrode shall be galvanized.
6. 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. GSCL shall provide the necessary space required to prepare the earthing pits.
7. All metallic objects on the premises that are likely to be energized by electric currents should be effectively grounded.
8. 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.
9. The earth connections shall be properly made.
10. A complete copper mesh earthing grid needs to be installed for the server farm area, every rack needs to be connected to this earthing grid. A separate earthing pit needs to be in place for this copper mesh.
11. Provide separate Earthing pits for Servers, & UPS as per the standards.

#### **4.14 Junction Box / Outdoor Cabinet, Poles and Cantilever**

1. The SI shall provide the Junction Boxes, poles and cantilever to mount the field sensors like the cameras, traffic sensors, traffic light aspects, active network components, controller and UPS at all field locations, as per the specifications given in the RFP.
2. Each intersection shall be fitted with outdoor cabinets dimensioned to host all equipment necessary to operate enforcement systems and traffic surveillance systems as defined in this RFP.

3. SIs shall reserve additional room in the intersection controller cabinet to accommodate the future system requirements
4. The size of outdoor cabinet / Junction Boxes shall be sufficient to house all the system components, which may be installed at the intersection or nearby. Boxes shall be dustproof and impermeable to splash-water. They shall be suitable for the Guwahati's environmental conditions. They shall have separate lockable doors for:
  - i. Power cabinet: This cabinet shall house the electricity meter, online UPS system and the redundant power supply system
  - ii. Control cabinet: This cabinet shall house the controllers for all the field components at that location e.g. PTZ, Fixed cameras etc.
5. Internal cabinet cabling shall be designed for an easy connection and disconnection of the equipment and power
6. The cabinets shall be of robust construction and shall include 3-point security-locking mechanisms to prevent unauthorized access to the field equipment
7. The Junction Box for UPS with Battery bank needs to be considered separately.
8. It should be noted that the SI should design the Junction box keeping in mind the scalability requirements of the project.
9. Temperature and Humidity Control: All enclosure compartments shall be equipped with a natural convection air circulation system via provision of air circulation filters that shall not require maintenance and shall allow free circulation of air inside the enclosures to prevent overheating as well as the build-up and effects of humidity and heat, without permitting the entry of elements that might endanger system operation.
10. SI shall ensure that all the hardware is placed inside the junction boxes that could withstand temperatures prevalent in Guwahati throughout the year.
11. The junction box should be designed in a way that, separate compartment will be available for separate system (i.e. ITMS Controller, Mini server, Active component, etc.). Each compartment shall have lock & key facility. There should be provision made to integrate the systems if required.
12. At selected traffic junctions, if the existing infrastructure of poles and cantilevers can be used for mounting/installing the traffic light aspects then GSCL shall facilitate to obtain NOC from respective department for installation by the SI. However, SI will be responsible for obtaining all the necessary permissions etc. The details of traffic junctions/locations are provided in **Annexure VIII under Section of 12.0**
13. The SI shall ensure that all installations are done as per satisfaction of Authority.
14. For installation of CCTV Cameras, PTZ Cameras etc. SI shall provide appropriate poles & cantilevers and any supporting equipment.

15. SI shall be required to supply, install, configure and integrate surveillance cameras at the identified locations and thereafter undertake necessary work towards their commissioning.
16. SI shall ensure that the poles erected to mount cameras are good, both qualitatively and aesthetically
17. SI shall use the industry leading practices while positioning and mounting the cameras and ensure that the pole / mast implementation is vibration resistant. Arrangements for bird scare spikes on top of camera shall be made to prevent birds from sitting on top of camera box.
18. The poles shall be installed with base plate, pole door, pole distributor block and cover.
19. Base frames and screws shall be delivered along with poles and installed by the SI.
20. In case the cameras need to be installed beside or above the signal heads, suitable stainless-steel extensions for poles need to be provided and installed by the SI so that there is clear line of sight.
21. SI shall be responsible to undertake required structural analysis regarding the regulated load conditions and considering the respective wind load while installing the poles / cantilevers for cameras and Variable Messaging Sign boards
22. SI shall provide structural calculations and drawings for the approval of Authority. The design shall match with common design standards/ IS Codes as applicable under the jurisdiction of Authority/authorized entity.
23. SI shall coordinate with concerned authorities / municipalities for installation.
24. Poles and cabinet shall be so designed that all elements of the field equipment could be easily installed and removed.
25. SI shall ensure that physical look of the installation area returns to neat & tidy conditions after installation of poles, cantilevers etc. The placement shall be designed keeping in mind the normal flow of vehicular traffic and pedestrian movement is not disturbed.

#### **4.15 Power & UPS - for Field Locations**

1. SI Shall coordinate with Energy distribution Company for provision of power for field installations. Desired energy meters shall be installed in the junction box at appropriate locations. Energy consumption costs shall be borne by SI during implementation and O&M Period which will be reimbursed by GSCL at actual.

2. UPS shall serve as a backup for commercially available utility power at the intersections and shall ensure no-break functioning of all field components at each intersection in event of failure of utility power supply.
3. SI shall carry out a study and identify locations to provide UPS backup, depending upon power situation across city, to meet the camera and other field equipment's uptime requirements.
4. SI shall install UPS at the identified intersections in secure, tamper-proof housing in corrosion resistant cabinets.
5. SI shall ensure that the UPS is suitably protected against storms, power surges and lightning.
6. SI shall provide UPS for efficient heat dissipation without air conditioning. It shall be able to withstand temperatures prevalent in the Guwahati throughout the year.

#### **4.16 Civil and Electrical Works**

1. SI shall be responsible for carrying out all the civil work required for setting up all the field components of the system including:
  - a) Preparation of concrete foundation for MS-Poles & cantilevers
  - b) Laying of GI Pipes (B Class) complete with GI fitting
  - c) Hard soil deep digging and backfilling after cabling
  - d) Soft soil deep digging and backfilling after cabling
  - e) Chambers with metal cover at every junction box, pole and at road crossings
  - f) Concrete foundation from the Ground for outdoor racks
2. SI shall provide electricity to the cameras through the aggregation point. Since this component has dependency on approval from local authorities, it is recommended that SI plans this requirement well in advance & submits the application to the concerned electricity distribution agency with requisite fees, as applicable.
3. SI shall carry out all the electrical work required for powering all the components of the system
4. Electrical installation and wiring shall conform to the electrical codes of India.
5. SI shall make provisions for providing electricity to the cameras (PTZ and Fixed) via SJB (Surveillance Junction Box), housing the UPS/SMPS power supply, with minimum backup as defined in this RFP,
6. For the wired Box cameras, SI shall provision for drawing power through PoE (Power over Ethernet), while PTZ cameras shall be powered through PoE+ / dedicated FRLS power cable laid separately along with STP cable.

7. Registration of electrical connections at all field sites shall be done in the name of Authority.
8. SI shall house the electricity meters inside the power cabinet as mentioned in the controller Cabinet section as above.
9. Electricity Charges for implementation and O&M period for all the systems has to be borne by the SI and cost of electricity will be reimbursed on monthly basis to SI by GSCL.

#### **4.17 Cabling Infrastructure**

1. The SI shall provide standardized cabling for all devices and subsystems in the field.
2. SI shall ensure the installation of all necessary cables and connectors between the field sensors /devices assembly, outstation junction box, for pole mounted field sensors /devices the cables shall be routed down the inside of the pole and through underground duct to the outstation cabinet.
3. All cables shall be clearly labeled with indelible indications that can clearly be identified by maintenance personnel. The proposed cables shall meet the valid directives and standards.
4. Cabling must be carried out per relevant BIS standards. All cabling shall be documented in a cable plan by the SI.

#### **4.18 Geographical Information System (GIS) platform**

SI shall provide GIS system and integrate it with ICCC or other systems. The SI will have to consult with GSCL and confirm what all GIS map/layer/dataset is available with the city. If the map/layer/dataset is not already available or in the process of being created by the city, the SI will have to prepare the GIS base maps, layers and dataset for all the components, assets, properties, critical infrastructure etc. as the part of this project. It will also be the scope of SI to develop component specific GIS layers/utilities as & when requested by GSCL. The SI will also be responsible to ensure that the GIS datasets are updated at regular frequency based on nature of datasets to ensure accuracy during the course of the entire project.

The SI is required to carry out implementation of City GIS Platform and seamless integration to ensure ease of use of GIS in the Dashboards at ICCC. If this requires field survey, it needs to be done by SI. If such a data is already available with city, it shall facilitate to provide the same. The SI is required to update GIS maps from time to time.

The SI will be required to undertake a detailed assessment for integration of all the Field level ICT interventions proposed with the Geographical Information System (GIS).



The scope of work for the SI while implementing GIS are:

1. Creation of City Base Map
2. Creation of layers for roads, properties, forest zones etc.
3. Mapping of city assets, utilities, smart components in the Map/ Layers
4. Mapping of potentially affected infrastructure in high-hazard zone in one municipality that will include critical infrastructure (life-line infrastructure, schools, police stations etc.), housing, commercial and industrial facilities, transport infrastructure etc.

An indicative list of the GIS datasets that are relevant to ICCC operations and would be required to be collected from stakeholder/end users' departments, field surveys and other ongoing projects is given below in the table:

S.No.	Systems/Departments	GIS Database
1	CITY Surveillance	CCTV Camera Locations on GIS Map
		Locations of Data Centre
		Locations of ICCC
		Backbone Network Connectivity Details including POP sites
2	Public Transport	Bus Routes on GIS Map
		Location of Bus Stations, Bus Depots, Bus Stops
		Location of traffic lights
		Location of Public Toilets
3	Traffic and Police	Locations of existing surveillance cameras from Traffic and Police
		Locations of Smart Traffic Signals
		ANPR, RLVS, SVD Camera Locations
		Location of Police Stations
4	Parking	Locations of Parking
5	E-Governance	Location of important Government buildings
		Location of Tourist Attractions
		Location of Public Advertisement Boards
6	Disaster Management	Location of highest Disaster Impact Areas in the city (Geofence)
		Location of fire stations
		Amenities at each Fire Station
7	Emergency Management	Location of Health centers/Hospital
		Amenities at each Health Centre/Hospital
		Type of fleet vehicle
		Location of Water Assets
8	Sewerage	Location of Sewerage Assets (STPs, ETPs etc.)
9	Storm Water	Location of Storm Water drains

The functional requirements and technical specifications provided in this section are indicative and carry guiding rule. The SI is free to offer products and solutions which meet requirements of the RFP focusing on the outcome, future scalability, security, reliability and adherence to specified SLA under this RFP, in line with applicable standards & best practices adopted in the industry. The SI is encouraged to design an Optimized solution which is technically superior, innovative, proven, better in terms of functionality and is cost effective. Any specified parameters mentioned in the scope/technical requirement in the RFP may be considered if it is required for meeting current & future requirements during the contract period. The SI is fully responsible for the specified outcome to be achieved.

For more details on technical and functional specifications of GIS Platform, the SI should refer to Section: 5.0 for functional requirements and technical specifications.

#### **4.19 Geo-Tagging**

System Integrator shall implement Geo-tagging for the all field equipment's, sensor, network touch points, connectivity and other IT/not-IT equipment's of the entire project.

#### **4.20 Edge Analytics**

The SI will be responsible for designing and implementing edge analytics at camera level. Following listed use cases should be part of implementation and should be not be limited to:

1. Safety: Detection and classification based on:
  - a) Parking violation
  - b) Loitering detection
  - c) Crowd Detection
  - d) Gesture recognition: Identification through gesture change
2. Wrong way or illegal turn detection at ITMS Signal Crossing.

#### **4.21 Network Connectivity (OFC & RF) for ICCC, DC and other Field Sensors**

To expedite the project deployment, GSCL intended to use the State-Owned Network's OFC Connectivity along with their existing POP sites' Space, Backbone OFC (Between POP Sites to SDC & ICCC) and Power Infrastructure. SI will design the OFC network in coordination with State Owned NW service Provider and deploy the Active Components (Transmission Equipment & other Devices) at provided POP sites space.

1. SI shall Design, Supply and Implement all Transmission Equipment's related to OFC Network. Deployment of OFC Network and O&M of all passive components will be taken care by State-owned Network Provider/NW Service Provider.
2. State-owned Network Provider/NW Service Provider shall provide the 20-30 Nos of POP sites across the Guwahati city and bidder shall decide the final locations and count of POS sites and also design the OFC network with coordination with State-owned Network Provider/NW Service Provider.
3. SI will also deploy the Access Network OFC (POP Sites to Field Devices) as per OFC Deployment Specification.
4. The intranet bandwidth required will be based on the connecting end point device capability for data feeds in to the ICCC & Data Centre etc. May vary depending on the nature of the connecting devices and the objectivity of the system.
5. Network & Backbone Connectivity is an important component of the project and needs very careful attention in assessment, planning and implementation. It is important not only to ensure that the required connectivity is provisioned within the required timelines but also ensure that it is reliable, secure and supports the required SLA parameters of Latency, Jitter, Packet Loss and Performance.
6. Network between SDC and ICCC will be on dual protection scheme with high level of availability.
7. The provisioning of the POPs for the City Network Backbone at the Junction and other field locations will be mutually agreed upon by the GSCL and the SI for the city surveillance and ITMS project.
8. The SI should provide a detailed network architecture of the overall system, incorporating findings of site survey exercise. The network so envisaged should be able to provide real time data streams to the Data Centre, and ICCC. All the components of the technical network architecture should be of industry best standard and assist SI in ensuring that all the connectivity SLAs are adhered to during the operational phase.
9. The SI shall prepare the overall network connectivity plan for this project. The plan shall comprise of deployment of network equipment at the junctions/locations to be connected over network, any clearances required from other government departments for setting up of the entire network. The network architecture proposed should be scalable and in adherence to network security standards. It is necessary that the proposed last mile connectivity should be wired. Last Mile to be defined as "the access link from the service provider's POP – (as per Telco Standards) to the field device".
10. The actual bandwidth requirement to cater the above-mentioned bandwidth parameters and to meet SLAs shall be calculated by the SI and the same shall be clearly proposed in the technical proposal with detail calculations. SI also to meet the parameters of video

feed quality, security & performance and thus SIs should factor the same while designing the solution. GSCL reserves its right to ask the Systems Integrator Systems Integrator to increase the bandwidth if the provided bandwidth is not enough to give the functionality of the system mentioned in the RFP and adhere to the SLAs.

11. In case the Telecommunication guidelines of Government of India require the purchaser to place Purchase Order to the Service Provider for bandwidth, GSCL shall do so. However, Systems Integrator shall sign a contract with Telecom Service Provider(s) or State-owned NW Service Providers and ensure the performance.
12. Service Charges and Related Payment will be paid to respective authority by GSCL directly.
13. The SI shall be required to submit a detailed installation report post installation of all the equipment at approved locations. The report shall be utilized during the acceptance testing period of the project to verify the actual quantity of the equipment supplied and commissioned under the project.
14. SI will propose and implement RF redundancy network to connect all ITMS signal Crossing.
15. ROW Permission will be taken by the SI and GSCL will assist the SI for any paperwork related to ROW permission. Cost related to this will be directly paid to ROW issuing authority by GSCL.
16. The System Integrator (SI) will require Right of Way (ROW) and permissions from following departments/ agencies for smooth implementation of CCTV City Surveillance, ITMS, ANPR System and Speed Violation Detection System in Assam
  - a) Police Department, Assam Police
  - b) APDCL
  - c) Highway Authorities (NH/NHAI)
  - d) Road & Building Department
  - e) PWD
  - f) Other Government agencies as required for system implementation
17. ROW permission required for implementation the following of the project.
  - a) Pole Erection
  - b) Main / Field Junction box installation
  - c) OFC related work
  - d) Wireless (RF) connectivity related work
  - e) Laying of Data cable and electrical cable
  - f) Electrical Connection with electricity meter installation at junction
  - g) Permission for changes in Building
  - h) Permission for State Level Control Centre and City Level Control Center

SI is required to cover following aspects while designing the network architecture, roll-out plan and implementation of network backbone across all the locations.

#### **4.21.1 Network Design and Rollout plan**

1. The SI shall be required to prepare detailed network architecture of the overall system, incorporating findings of site survey exercise. Network so designed shall be able to provide real time video stream to the City Operation Centre along with RF redundancy to all ITMS signal crossing.
2. The design shall also cover LAN connectivity requirements at locations such as Command and Control center, Data center that shall include setting up of structured cabling, commissioning of active and passive components for operationalization of the Integrated Security and Surveillance system.
3. SI is expected to provision for necessary bandwidth and connectivity during the contract period. Provisioning for bandwidth shall be done on bandwidth as a service model. City Network backbone shall provision for all the Safe & Smart initiatives for the Guwahati including City Surveillance and Integrated Traffic Management System.

#### **4.21.2 Implementation of Network connectivity**

1. SI shall ensure that redundant, high quality, seamless connectivity is provided to all cameras across the city.
2. Connectivity to Data center and Command Control Center shall be provided with scalable capacities to allow for expansion in the future.
3. SI shall provide adequate bandwidth for each camera to maintain high quality FHD/1080p/4K video transmission to the Data Center and City Operation Centre. The actual bandwidth requirement to cater to above mentioned bandwidth & storage parameters and to meet SLAs shall be estimated by the SI and proposed in the technical bid with detailed calculations. It is expected that SI shall design the networking solution in such a manner that there is no single point of failures at every pole and solution meets all the uptime & and quality related SLAs.
4. SI shall ensure the redundancy to the critical locations over captive RF at all ITMS Signal Crossing.
5. SI needs to undertake the following activities (including but not limited to) provisioning of the network backbone for Authority:

##### **I. Provisioning Network Links**

- a) All field locations shall be connected to Data Center (DC) & Integrated Command & Control Center (ICCC) through optical fiber backbone network.
- b) SI shall ensure that the bandwidth estimated and proposed meets the locations' requirement and expected performance level.
- c) All the required network and security equipment like routers, switches, firewall, etc. shall be provided by the SI.

## **II. Infrastructure Management Services**

- a) SI shall ensure that the network is available 24x7x365 as per the prescribed SLAs.
- b) SI shall provide services for management of complete infrastructure to maintain performance at optimum levels.
- c) SI shall be responsible for attending to and resolving network failures and snags
- d) SI shall support and maintain the overall network infrastructure including but not limited to LAN passive components, routers, switches, Firewalls', etc.
- e) SI shall provide information on performance of Ethernet segments, including capacity utilization and error statistics for the segment and the top-contributing hosts and routers
- f) SI shall create required facilities for providing network administration services including administrative support for user registration, creating and maintaining user profiles, granting user access and authorization, providing ongoing user password support, announcing and providing networking services for users and providing administrative support for print, file, directory and e-mail servers for the Authority.
- g) SI shall provide a single-point-of-contact for requesting LAN and Server administration services and answering administrative questions. Network Administrator shall respond to the initial request from the users within the agreed service level objectives and service coverage hours.
- h) SI shall provide support as required to assist with hardware and software problem isolation and resolution in the LAN environment.
- i) SI shall undertake LAN and Server problem determination.
- j) SI shall communicate server changes affecting the LAN environment.
- k) SI shall maintain LAN and server configuration data.
- l) SI to monitor the non-IT components such as UPS, DG set, LT Panel, Air conditioning system, as well through a common dashboard.
- m) SI shall be responsible for polling / collecting of server, devices and desktops security logs from all the systems. All these logs shall be made available to the Infrastructure Management System (IMS) solution.

## **III. Network Security**

SI shall be responsible for management of Integrated Security and ITMS and City Surveillance system's network security. As part of network security, the SI shall ensure the following:

- a) Network shall be used for valid purposes only. Protection of information available on the networks is the responsibility of SI. The activity and content of user information on the computer networks is within the scope of review by management.
- b) SI shall develop and implement network security systems and procedures and provide network security resources (Firewall etc.) to protect all Authority's data, related application systems and operating systems software from unauthorized or illegal access at a level that is appropriate for the information /computing resources.
- c) SI shall be responsible for the following activities:

#### **IV. Network Access**

- a) SI shall ensure that Access to network and network resources shall be on need to know basis and authorizations shall be obtained from appropriate authorities before providing access.
- b) Network and network services required for every job function and role shall be identified and verified by the SI.
- c) Policies detailed in Access Controls Policy – User Account Management shall be followed by the SI for providing access to network and network services
- d) SI shall ensure that the networks are logically or physically divided based on the criticality of the information stored in the networks.

#### **V. Internet Service Management**

- a) SI shall be responsible for granting, monitoring, and revoking access to the internet.
- b) SI shall ensure that users utilize the internet only for operational use.
- c) All the internet activity shall be logged and monitored, and appropriate network devices shall be deployed so that access controls and related security mechanisms could be applied.

#### **VI. Infrastructure Management**

- a) All network equipment and communication lines shall be identified, documented, and shall be regularly updated by the SI.
- b) Network diagrams at all levels shall be maintained and updated regularly by the SI.
- c) Minimum Baseline Security Standards (MBSS) shall be developed and maintained by the SI.
- d) All network equipment shall be configured as per MBSS.

- e) All network services that are not required on the servers shall be disabled.
- f) Any problems with the network equipment leading to delay or stopping of any business processes shall be escalated as an Incident.

## **VII. Data Transmission**

- a) Care shall be taken by the SI while transmitting confidential information over public networks to other government agencies with a prior permission from the concerned authority.
- b) Confidential information not being actively used, when stored or transported in computer-readable storage media (such as magnetic tapes or CDs), shall be stored securely under lock and key
- c) SI shall ensure and prevent unauthorized disclosure of data when computers are sent out for repair or used by others within or outside COC and the data could be deleted. All data stored on hard disks shall be backed up and erased via user-transparent processes.

## **VIII. Network Assessment**

- a) Network vulnerability assessments shall be performed on an ongoing basis by the SI.
- b) Assessment report shall be submitted to the Authority on a quarterly basis.
- c) The SI shall coordinate for Third-party independent network assessment that shall be carried annually in order to provide assurance to the Authority.

### **4.21.3 Hosting Services**

1. The infrastructure of Data Center for ICCC, ITMS and City Surveillance system shall be hosted at State Data Center (SDC) of Govt. of Assam. The following services shall be provisioned by State Data Center.
  - Internet Bandwidth
  - Hosting Space
  - Power & Cooling
  - Secured Data Center Environment
2. The SI shall responsible for any payments or charges (if required) for hosting data center services at State Data Centre, (which will be reimbursed to SI or will be directly paid to SDC)



3. The SI needs to do the sizing of rack space required at facilities based on its capacity planning and sizing for the entire duration of the contract with adequate space for future expansion.
4. All the requisite consumables like tapes, hard disks, etc. for backup shall be provided by the SI as per the project requirements. All the tapes, hard disks, etc. once deployed for the project will become property of GSCL including corrupted/damaged devices.

#### **4.22 Design, Supply, Installation and Commissioning of IT Infrastructure at Data Centre (DC) and ICCC**

1. SI shall provide the IT hardware infrastructure at the DC for successful operations of the systems. DC will be hosted preferably in State Data Centre. MoU may be signed between GSCL and IT Department, Govt of Assam for finalization of hosting location of Data Centre at SDC. The permanent ICCC building has been envisaged to be established at Panjabari, Near Bipanan Khetra, Guwahati. Till the time ICCC is operational, SI is expected to establish Interim ICCC in an approximate area of 3000 to 5000 Square Feet at suitable location to be provided GSCL. Once the permanent ICCC in Guwahati is operational, then the SI shall migrate the Interim ICCC to the permanent ICCC.
2. Temporary location of ICCC is identified and address is as mentioned below;

**BSNL Bhawan  
5<sup>th</sup> Floor, Administrative Building  
Cotton Road, Pan Bazar,  
Guwahati - 781001**

3. SI has to ensure that redundancy is provided for all the key components to ensure that no single point of failure affects the performance of the overall system. It will be SI's responsibility to:
  - a) Supply, Install and Commission of IT Infrastructure including site preparation in DC (State Data Center) and ICCC (First temporary locations & then after shifting the all HW & SW to new permanent building)
  - b) To provide system integration services at ICCC to monitor:
    - I. Video feeds from field CCTV cameras
    - II. Live MIS Reports of ICCC operations
  - c) Establish LAN and WAN connectivity at DC and ICCC

- d) To give area wise video feed to monitor only at Twenty (20) Nos. Police Stations (Central, East & West District),
4. Network and server racks for hosting Data Centre Infrastructure.
  5. Data Centre developed by SI should be as per Telecommunications Infrastructure Standard for Data Centers.
  6. The SI shall provide system integration services to customize and integrate the applications procured through the project. The ITMS and Surveillance System applications proposed by the SI should have open APIs and should be able to integrate and share the data with other third-party systems already available or coming up in the coming future.
  7. As part of preparing the final bill of material for the data centre, the successful SI will be required to list all passive & active components required in the data centre.
  8. The bill of material proposed by the successful SI will be approved by GSCL for its supply and installation. Indicative IT Infrastructure to be commissioned as part of the ITMS and City Surveillance System project at Data Centre are as under:
    - a) Servers (inclusive of OS) - Application Servers, Database Server, Video Recording Server, Video Management Server, Enterprise Backup Server, Domain Controller, Failover Servers for application and Recording Servers
    - b) Application & System Software (with necessary customization) – Integrated Traffic Management System including the Adaptive Traffic Signal Control and Traffic Violation Detection System application, Video Management System application, ANPR application, Red Light Violation Detection application, Speed Violation Detection System and E-Challan application.
    - c) RDBMS (if required)
    - d) Anti-virus Software
    - e) NMS/EMS software
    - f) Primary Storage Solution
    - g) Storage Management Solution
    - h) Switches
    - i) KVM Switches
    - j) Firewall
    - k) IP Phones
    - l) Racks
    - m) All required Passive Components
    - n) Any other Server required to cater to the scope of work mentioned in this

9. The above are only indicative requirements of IT & Non-IT Infrastructure requirements at DC. The exact quantity and requirement shall be proposed as part of the technical proposal of the SI.
10. The SI shall prepare the overall data centre hosting & their operational plan for this project. The plan shall comprise of deployment of all the equipment required under the project. The implementation roll-out plan for hosting of the data centre shall be approved by GSCL. The detailed plan shall also be comprised of the scalability, expandability and security that such data centre will implement under this project.
11. The bidder is expected to calculate and design the IT Infrastructure requirements including compute, storage and video management software licenses etc. required for real-time monitoring, recording and integration of Surveillance (PTZ and Fixed Box) and Traffic Violation detection (RLVD, ANPR, SVD) Cameras and Dome for the POP sites. The supply, installation and connectivity till ICCC of the provided cameras will be in their scope. SI is expected to capture and propose the IT Infrastructure for successful operations and integrations of the same.
12. The SI shall establish a state of the art ICCC, the key components for the same will be as follows:
  - a) Video Wall system
  - b) Operator workstations
  - c) IP Phones
  - d) Active Networking Components (Switches, Routers)
  - e) Passive Networking Components
  - f) Electrical Cabling and Necessary LED Illumination Devices
  - g) Office Workstations
  - h) UPS (as per the requirement mentioned in the Technical Specification)
13. The SI shall be required to submit a detailed installation report post installation of all the equipment at approved locations. The report shall be utilized during the acceptance testing period of the project to verify the actual quantity of the equipment supplied and commissioned under the project.

#### **4.23 Installation & Commissioning of a Sample Site – Proof of Concept (POC)**

The SI shall complete the installation work at the identified sample sites from all the aspects and then request the Authority to conduct a detailed assessment of all the quality

parameters that it expects at the sample site. Following aspects shall be assessed thoroughly:

- a) Functionality test of all CCTV Cameras & Field Sensors, ITMS (ATSC & Traffic Volition Detection) Equipment's and allied applications.
- b) Quality of Poles and Junction Box erected at site.
- c) Functional test of storage system, switches, routers & other networking gears.
- d) Quality of resurfacing of the cut roads and pavements.
- e) Placement of relevant equipment like network switch, local processing unit, UPS, Telecom Service Providers MUX inside the rack.
- f) Electrical earthing of the Junction Box and Poles.
- g) Structured cabling standards inside the Junction box.
- h) Cabling from the junction box to the poles to be completely covered
- i) Labelling of the entire infrastructure inside the rack and all the poles and cameras at the junction site for ease of maintenance.

A Site visit report shall be prepared and presented to the Authority covering all the observations. The same shall be dually vetted by Authority and changes if any suggested shall be highlighted.

The SI shall ensure the observations/ changes suggested by Authority shall be incorporated for the first site and incorporated for all locations. Due verification of the same shall be done at the time of User Acceptance of the project.

#### 4.24 Responsibility Matrix - Overall

##### 4.24.1 Overall Activities – Responsibility Matrix

#	Key Activities	System Integrator (SI)	Designated Technical Agency	PMC	GSCL	State-Owned NW Service Provider	Electricity Providers	ROW Issuing Authority	Others ICT Vendors/OEM at GSCL
<b>Project Inception Phase</b>									
1	Project Kick Off	R/A	C	C	C	I	I	I	I
2	Deployment of Manpower	R/A	C	C	C	I	I	I	I
<b>Requirement Phase</b>									

#	Key Activities	System Integrator (SI)	Designated Technical Agency	PMC	GSCL	State-Owned NW Service Provider	Electricity Providers	ROW Issuing Authority	Others ICT Vendors/OEM at GSCL
3	Assess the requirement of IT Infrastructure and Non-IT Infrastructure	R/A	C	C	C	C	C	C	C
4	Assessment of Business Processes	R/A	C	C	C	I	I	I	I
5	Assessment of Software Requirements	R/A	C	C	C	I	I	I	I
6	Assess the Integration Requirement	R/A	C	C	C	C	C	I	C
7	Assess the connectivity requirement all locations (including Building)	R/A	C	C	C	C	I	I	I
8	Assess the Network Laying Requirement	C	C	C	C	R/A	I	I	I
9	POP Site - Space & Power & Power Backup	C	C	C	C	R/A	I	I	I
10	Assessment of training Requirement	R/A	C	C	C	I	I	I	I
<b>Design Phase</b>									
11	Develop the Concept of Operations (CONOPS)	R/A	C	C	C	C	I	I	I
12	Formulation of Solution Architecture	R/A	C	C	C	C	I	I	I
13	Creation of Detail Drawing	R/A	C	C	C	C	I	I	I
14	Detailed Design of Smart City Solutions	R/A	C	C	C	C	I	I	I

#	Key Activities	System Integrator (SI)	Designated Technical Agency	PMC	GSCL	State-Owned NW Service Provider	Electricity Providers	ROW Issuing Authority	Others ICT Vendors/OEM at GSCL
15	Development of test cases (Unit, System Integration and User Acceptance)	R/A	C	C	C	C	I	I	I
16	Preparation of final bill of quantity and material	R/A	C	C	C	C	C	I	I
17	SoP & KPIs preparation	R/A	C	C	C	C	C	C	I
<b>Development Phase</b>									
18	Helpdesk setup	R/A	C	C	C	I	I	I	I
19	Physical Infrastructure setup	R/A	C	C	C	I	I	I	I
20	Procurement of Equipment, edge devices, COTS software (if any), Licenses	R/A	C	C	C	I	I	I	I
21	IT and Non-IT Infrastructure Installation	R/A	C	C	C	I	I	I	I
22	Development, Testing and Production environment setup	R/A	C	C	C	I	I	I	I
23	Software Application customization (if any)	R/A	C	C	C	I	I	I	I
24	Development of Bespoke Solution (if any)	R/A	C	C	C	I	I	I	I
25	Integration with Third party services/ application (if any)	R/A	C	C	C	I	I	I	I
26	Unit Testing	R/A	C	C	C	I	I	I	I
27	Implementation of Solutions	R/A	C	C	C	I	I	I	I

#	Key Activities	System Integrator (SI)	Designated Technical Agency	PMC	GSCL	State-Owned NW Service Provider	Electricity Providers	ROW Issuing Authority	Others ICT Vendors/OEM at GSCL
28	Preparation of User Manuals, training curriculum and training materials	R/A	C	C	C	I	I	I	I
29	Role based training(s) on the Smart City Solutions	R/A	C	C	C	I	I	I	I
<b>Integration Phase</b>									
30	SoP & KPI Implementation	R/A	C	C	C	C	C	C	I
31	Integration with GIS	R/A	C	C	C	C	C	C	I
32	Integration of solutions with Command and Control Centre	R/A	C	C	C	C	C	C	I
33	Integration Testing	R/A	I	C	I	C	C	C	C
34	User Acceptance Testing	A	R	C	R	C	C	C	I
<b>Go –Live</b>									
35	Go Live	R/A	C	C	C	I	I	I	I
<b>Operation and Maintenance</b>									
36	Operation and Maintenance of IT, Non-IT infrastructure and Applications	R/A	C	C	C	I	I	I	I
37	SLA and Performance Monitoring	R/A	C	C	C	I	I	I	I
38	Logging, tracking and resolution of issues.	R/A	C	C	C	I	I	I	I
39	Application enhancement	R/A	C	C	C	I	I	I	I
40	Patch & Version Updates	R/A	C	C	C	I	I	I	I

#	Key Activities	System Integrator (SI)	Designated Technical Agency	PMC	GSCL	State-Owned NW Service Provider	Electricity Providers	ROW Issuing Authority	Others ICT Vendors/OEM at GSCL
41	Helpdesk services	R/A	C	C	C	I	I	I	I

**INDEX**

**R/A = Responsible/Accountable**

**C = Consulted,**

**I = Informed**

**Note:** All decisions will be taken by GSCL which will be abided by all the stakeholders in the above matrix.

**4.24.2 Network O&M, Payments – Responsibility Matrix**

S. No.	Activities Details	System Integrator (SI)	State Owned NW Service Provider	GSCL	Remarks
1	POP to POP backbone connectivity through Dark Fibre including O&M	C	R/A	I	
2	Connectivity from POP to Data Centre through Dark Fibre including O&M	C	R/A	I	
3	Connectivity from POP to ICCC through Dark Fibre including O&M	C	R/A	I	
4	O&M of Backbone OFC as per SLA	C	R/A	I	



S. No.	Activities Details	System Integrator (SI)	State Owned NW Service Provider	GSCL	Remarks
5	O&M for following components at POP Site: * AC/DC Backup Power Source * Genset for Backup * Civil & Electrical Work * Earthing * Electricity Bill * Diesel/ Fuel Cost for Genset * 24X7 Security	C	R/A	I	
6	Connectivity from POP to POE switches at Camera location through OFC including O&M	R/A	C	I	
7	POE switch to Camera Connectivity including O&M	R/A	C	I	
8	Installation and O&M of all active components at POP (including LIU, Rack etc.)	R/A	C	I	
9	O&M of all Active Components at POP sites and Field level	R/A	C	I	
10	O&M of Passive Components at Field Level (Except Backbone OFC)	R/A	C	I	
11	One time payment for electric meter installation required at Camera Points & Traffic Junctions	R/A	C	I	Reimbursable by GSCL at actual
12	Payment for periodic electricity bill to be generated at Camera Points & Traffic Junctions	R/A	C	I	Reimbursable by GSCL at actual
13	Payment towards Co-location charge of State Data Centre (SDC)	I	C	R/A	All payments shall be made to State Owned Network Provider directly by GSCL
14	Payment towards use of State Owned Network Infrastructure	I	C	R/A	
15	Payment towards rental charge of temporary ICCS space	I	C	R/A	

S. No.	Activities Details	System Integrator (SI)	State Owned NW Service Provider	GSCL	Remarks
16	Permission for all ROW & RI (related to Pole erection, OFC laying etc.)	R/A	C	I	GSCL will facilitate to SI related to paper work
17	Payment towards ROW & RI Charges	R/A	C	I	Reimbursable by GSCL at actual

### **INDEX**

**R/A = Responsible/Accountable**

**C = Consulted,**

**I = Informed**

#### **4.25 Project Deliverables**

#	Key Activities	Deliverables
1	Project Kick Off	1. Project Plan
2	Deployment of manpower	2. Risk Management and Mitigation Plan
3	Assess the requirement of IT Infrastructure and Non-IT Infrastructure	3. Functional Requirement Specification document
4	Assessment of Business processes	4. System Requirement Specification document
5	Assessment of requirement of Software requirements	5. Requirements Traceability Matrix
6	Assess the Integration requirement	6. Site Survey Report
7	Assess the connectivity requirement of all locations (including Building)	
8	Assessment of network laying requirement	
9	Assessment of training requirement	
10	Formulation of Solution Architecture	1. Final Bill of Quantity
		2. HLD documents
		3. LLD documents

#	Key Activities	Deliverables
		4. Application architecture documents
		5. Technical Architecture documents.
		6. Network Architecture documents.
		7. ER diagrams and other data modeling documents.
		8. Logical and physical database design.
		9. Logical and physical infra architecture
11	Creation of Detail Drawing	10. Data dictionary and data definitions.
12	Detailed Design of Smart City Solutions	11. GUI design (screen design, navigation, etc.).
13	Development of test cases (Unit, System Integration and User Acceptance)	12. Test Plans
14	Preparation of final bill of quantity and material	13. SoPs & KPIs
15	SoPs & KPIs preparation	14. Change management Plan
16	Helpdesk setup	1. IT and Non-IT Infrastructure Installation Report
17	Physical Infrastructure setup	2. Training Completion report
18	Procurement of Equipment, edge devices, COTS software (if any), Licenses	3. Application deployment and configuration report
19	IT and Non-IT Infrastructure Installation	4. Unit Testing Report
20	Development, Testing and Production environment setup	5. Functional Testing Report
21	Software Application customization (if any)	
22	Development of Bespoke Solution (if any)	
23	Integration with Third party services/application (if any)	
24	Unit Testing	
25	Implementation of Solutions	
26	Preparation of User Manuals, training curriculum and training materials	

#	Key Activities	Deliverables
27	Role based training(s) on the Smart City Solutions	
28	SoP & KPIs implementation	1. Integration Testing Report
29	Integration with Smart Components	2. Completion of UAT and closure of observations report
30	Integration of solutions with Integrated Command and Control Centre	
31	Integration Testing	
32	User Acceptance Testing	
33	Go Live	1. Go-Live Report
34	Operation and Maintenance of IT, Non-IT infrastructure and Applications	2. Detailed plan for monitoring of SLAs and performance of the overall system
35	SLA and Performance Monitoring	3. Fortnightly Progress Report
36	Logging, tracking and resolution of issues.	4. Monthly SLA Monitoring Report and Exception Report
37	Application enhancement	5. Quarterly security Report
38	Patch & Version Updates	6. Issues logging and resolution report
39	Helpdesk services	

#### 4.26 Project Timelines

Services	Approximate Time for Issuance of Request Order	Tentative Scope/ Approximate Sizing	Tentative Lead Time
Request Order	One-week post issue of LOI/ completion of site survey activity	1 Command and Control Center (ICCC) IT hardware	12 months post issuance of request order
		2 Command and Control Center (ICCC) non-IT equipment	
		3 Command and Control Center (ICCC) – software	
		4 Command and Control Center Viewing for (ICCC) IT hardware	
		5 DC – Hardware	
		6 DC – Software	
		7 DC – non-IT equipment	

Services	Approximate Time for Issuance of Request Order	Tentative Scope/ Approximate Sizing	Tentative Lead Time
		8 Implementation and Integration of City Surveillance System - CCTV & other accessories items	
		9 Implementation and Integration of Adaptive Traffic Control System / Integrated Traffic Management System including traffic violation system (Traffic Signal System, ANPR, RLVD, SVD)	
		10 Network Backbone connectivity between Field Sensors and ICCS, DC & DR and other Viewing Locations	

#### 4.27 Project Defect Liability Period (DLP) / Warrantee of Product & Services

Bidder shall be responsible for Operation and Maintenance of each components (HW, SW, SW Patches, Upgrades and Service) related to this RFP for period of Five (5)-Years after final acceptance testing and handover to client.

- All hardware items should to be quoted with 5 years replacement warranty from OEM and onsite support and services.
- All software/subscription/licenses should be quoted with 5 years warranty, updates, upgrades (wherever applicable), support and services from OEM"

#### 5.0 FUNCTIONAL REQUIREMENTS & TECHNICAL SPECIFICATIONS

The functional requirements and technical specifications provided in the below sections and at other sections in this RFP are indicative and carry guiding rule. The SI is free to offer products and solutions which meet requirements of the RFP focusing on the outcome, future scalability, security, reliability and adherence to specified SLA under this RFP, in line with applicable standards & best practices adopted in the industry. The SI is encouraged to design an Optimized solution which is technically superior, innovative, proven, better in terms of functionality and is cost effective. Any specified parameters mentioned in the scope/technical requirement in the RFP may be considered if it is required for meeting current & future requirements during the contract period. The SI is fully responsible for the

specified outcome to be achieved. Some of the basic prerequisites that bidder shall fulfill the under this RFP are mentioned below;

- 1) All hardware items shall be quoted with 5 years advance replacement warranty from OEM/Supplier/Manufacturer and onsite support and services.
- 2) All software/subscription/licenses should be quoted with 5 years warranty, updates, upgrades (wherever applicable), support and services from OEM.
- 3) Manufacturer Authorization Form should be submitted for each item clearly mentioning the items for which the bidder is authorized to quote.
- 4) OEM undertaking that the quoted product will not become end of sale within next 12 months.
- 5) OEM undertaking that the quoted product will not become end of support/end of life for next 5 years.
- 6) OEM undertaking that they have not been blacklisted by any Govt./PSU in India.
- 7) Temporarily Telecom connectivity (MPLS/etc.) may be considered either within the scope or out of the scope of this RFP for immediate deployment of ITMS/etc. nodes.
- 8) Bidder should submit complete Bill of Materials for each item with part-codes for -
  - a) Sub-components
  - b) Warranty for 5 years
  - c) Subscription for 5 years (if any)
  - d) License for 5 years (if any)
- 9) Incorrect/Incomplete Bill of Material may lead to rejection of bid.
- 10) OEM of all active IT components should have online portal to raise tickets for support and services.
- 11) Product serial numbers of all IT active components should be available in the OEM online portal for ease of maintenance and support.
- 12) OEM should have end user web interface to log case with product serial number.
- 13) Malicious Code Certificate:
- 14) Both Bidder and OEM should submit following certificate along with the bid document:

- A. This is to certify that the Hardware and the Software being offered, as part of the contract, does not contain Embedded Malicious code that would activate procedures to:
  - I. Inhibit the desires and designed function of the equipment.
  - II. Cause physical damage to the user or equipment during the exploitation.
  - III. Tap information resident or transient in the equipment/network.
  
- B. The firm will be considered to be in breach of the procurement contract, in case physical damage, loss of information or infringements related to copyright and Intellectual Property Right (IPRs) are caused due to activation of any such malicious code in embedded software.

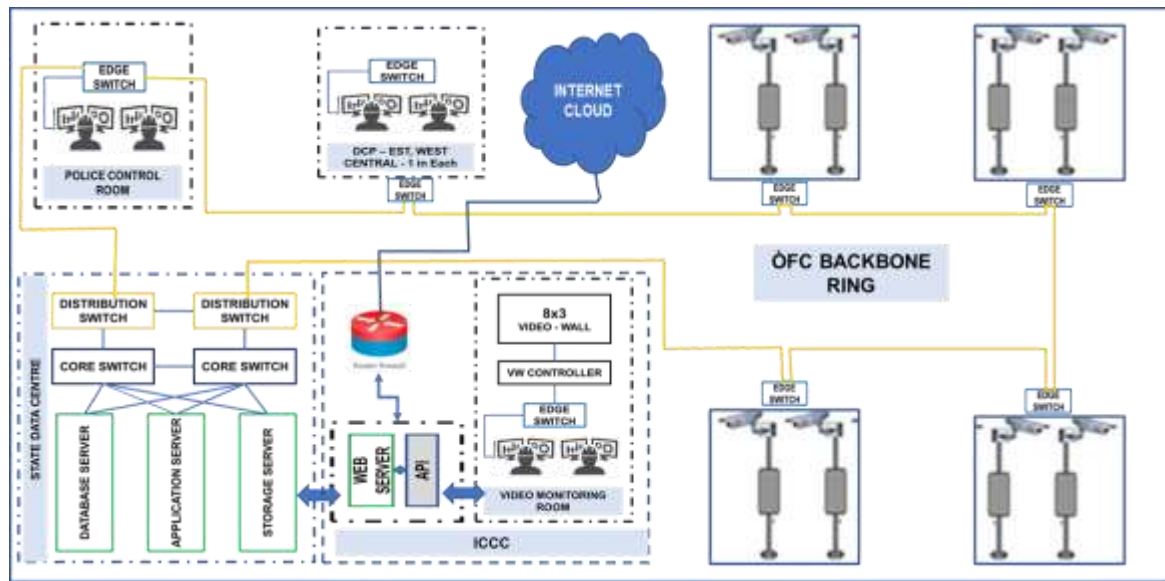
## **5.1 COMPONENT 1 - CCTV CITY SURVEILLANCE SYSTEM**

Surveillance Cameras are most important component of Traffic & Safety solution for any city. The camera at various location and junctions will have the capability to provide a potential live video to be shared with ICCC for monitoring functions of other departments too (Black spot monitoring, Event Management, etc.). In its endeavor to provide the citizens of Guwahati a safe and secure society, Guwahati Smart City has made provision to install CCTV/Surveillance cameras across different locations and junctions in the city. All these cameras must be integrated with the ICCC and feed will be provided to the Police Control Room or Specified Police Stations. The feed from all these cameras will be monitored closely to identify incidents (pre-incident and post-incident).

The functional requirements and technical specifications provided in the below sections are indicative and carry guiding rule. The SI is free to offer products and solutions which meet requirements of the RFP focusing on the outcome, future scalability, security, reliability and adherence to specified SLA under this RFP, in line with applicable standards & best practices adopted in the industry. The SI is encouraged to design an Optimized solution which is technically superior, innovative, proven, better in terms of functionality and is cost effective. Any specified parameters mentioned in the scope/technical requirement in the RFP may be considered if it is required for meeting current & future requirements during the contract period. The SI is fully responsible for the specified outcome to be achieved.

### **5.1.1 Indicative Solutions Architecture – CCTV City Surveillance**

An indicative solution architecture proposed for the installation of city surveillance system to enhance monitoring and management of incidents in the city is presented in the figure below:



**Figure 2 : Indicative Solutions Architecture - CCTV Surveillance**

As highlighted in the figure above the network comprises of a network of CCTV cameras, which are connected to scalable network video recorder (NVR) / network attached storage (NAS) / storage area network (SAN). which stores and converts the video input as per the output requirement. The converted video feed is relayed to the ICC, which is monitored by operators. On the event of detection of an incidence or possible cause of event, an alert is generated. Based upon the nature of alert the operator informs the concerned department for their timely response and resolve of the incident.

### 5.1.2 Functional Requirements – CCTV City Surveillance

Functional Requirement of the overall Surveillance System can be categorized into following components:

1. **Information to be Captured by Edge Devices**
2. **Information to be analyzed at ICC**
3. **Network connectivity – CCTV to ICC, DC, Other Viewing Centers.**
4. **Role Based Access to the Entire System**
5. **Storage / Recording Requirements**
6. **Other General Requirements**

#### 5.1.2.1 Information to be captured by Edge Devices

Surveillance Cameras being one of the core sub modules of ICC project, it is important that their selection and placement is carefully done to ensure the full coverage of the traffic junction along with all associated junction arms, accuracy of the information captured on the field and they are rugged, durable & compact. These cameras need to work on 24 X 7 basis and transmit quality video feeds to the ICC and would capture the video feeds at



25~30 FPS during entire duration of day for 30 days duration. However, Assam Police 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 5% of the cameras would be required to be viewed at higher FPS at a given point of time).

#### **5.1.2.2 Information to be analysed at ICCC**

The proposed Video Management System should provide a complete end-to-end solution for security surveillance application. The control centre shall allow an operator to view live / recorded video from any surveillance camera on the IP network. The combination of control centre and the IP network would create a virtual matrix, which would allow switching of video streams around the system.

It has been envisaged that all surveillance cameras would not be simultaneously viewed at Integrated Command & Control Center. The viewing shall vary from time to time and on-demand basis which will help to manage traffic at the junctions and coordinate with the field police officers.

#### **5.1.2.3 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 of implementation) 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:

- a) 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 interfaced to change these details, after proper authentication.
- b) Rights to different modules / sub-modules / functionalities should be role based and proper log report should be maintained by the system for such access.
- c) The system should be with login name & password enabled to ensure that only the concerned personnel are able to login into the system
- d) There should be provision to specify hierarchy of operators / officers for control of the cameras from various locations.
- e) The number of users shall increase as per phase wise implementation. SI is expected to make list of items required in BOQ for future expansion. Bidder are expected to provide the estimations cost of per Camera (CCTV)/Traffic Junction (ITMS) expansion.
- f) Windows Active Directory/LDAP or any such system can be used to design role-based access.

#### 5.1.2.4 Storage/Recording Requirements

It is proposed that the storage solution shall be modular enough to ensure compliance to the changes in storage / recording policy, to be evolved upon initial deployment of the system. The following storage requirements shall be fulfilled by the SI as scope for the project:

- a) The Data Centre (DC) will be hosted at state data center
- b) 30 days storage of all the surveillance CCTV camera feeds to be stored at Data Centre and Flagged data (critical incidents) will be stored for approximately 90 days, permanent storage envisaged on secondary/backup storage
- c) Redundancy of first 30 days storage will be provided by SI either in State Data Centre or Near Disaster Recovery Centre. (Near DR)
- d) 90 days storage for all traffic enforcement systems including RLVD, speed violation detection, Traffic violation cameras, and ANPR camera at Data Centre.
- e) 365 days storage of traffic junction data for ATSC at Data Centre and Flagged data will be stored for approximately 5 years.
- f) Above all systems except ITMS are required to be stored online thirty (30) days of video for all cameras on primary storage, balance 60 days will be on low cost secondary storage /tape library.
- g) For ATSC system, Primary storage will be for 90 days and Secondary Storage for 365 days. Back up storage for 5 Years approximately.
- h) Data on storage would be over-written automatically by newer data after the stipulated time period. If some data is flagged by police personnel (or by designated personnel) as important data / evidence data due to some reporting of crime or accident in the area or due to court order or due to suspicious activity, it would need to be stored for longer duration, as per requirements. Guwahati Police would analyze such flagged data every 3-months to take such decisions for preservation of the flagged data beyond 90 days.
- i) Full audit trail of reports to be maintained for 90 days.
- j) SI is expected to carry out the storage requirement estimation and supply as per the solution proposed.
- k) Archival/Backup to be done on NAS / Scale-out NAS / SAN / Unified or equivalent storage solution
- l) Retrieval time for any data stored on secondary storage should be max. 4 hours for critical data & 8 hours for other data.
- m) 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.
- n) 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.

- o) The system shall support H.264, H.265 or better, MPEG-4 and MJPEG compression formats for all analog cameras connected to encoders and all IP cameras connected to the system.
- p) 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.
- q) The system should not limit amount of storage to be allocated for each connected device.
- r) The on-line archiving capability shall be transparent and allow Guwahati Police to browse and archive recordings without the need to restore the archive video to a local hard drive for access.
- s) 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.
- t) 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 and sound alerts to necessary personnel.
- u) Bandwidth optimization
  - The Recording Server / System shall offer different codec (H.264, H.265, MJPEG, MPEG-4, etc.) and frame rate (CIF, HD, FHD, 4CIF, QCIF) options for managing the bandwidth utilization for live viewing on the Client systems. (through use of multiple systems such as transcoding server)
  - From the Guwahati Police, 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.
- v) The Recording Server / System shall support camera (analogue and IP cameras) devices from various manufacturers.
- w) The Recording Server / System shall support the PTZ protocols of the supported devices listed by the camera OEMs or ONVIF.
- x) The system shall support full two-way audio between Client systems and remote devices. (Audio from certain set of cameras can be recorded in future).

#### **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 if one of a group of designated recording servers fails. Recordings shall be synchronized back to the original recording server once it is back online.

- The system shall support multiple failover servers for a group of recording servers.

#### **SNMP / Object Model Support**

- The system shall support Simple Network Management Protocol (SNMP)/ Object Model for third-party software systems to monitor and configure the system.
- The system shall act as an SNMP / Object Model agent which can generate an SNMP trap /Integration as a result of rule activation in addition to other existing rule actions.

### **5.1.2.5 Other General Requirements**

#### **A. Management/Integration functionality**

- a) The Surveillance System shall offer centralized management of all devices, servers and users.
- b) 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.
- c) The Surveillance System shall support distributed viewing of any camera in the system using Video walls or big screen displays.
- d) 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.
- e) It should be possible to integrate the Surveillance System with 3rd-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.
- f) It should be possible to integrate social media platforms to Surveillance System / ICCC to enable Guwahati Police to track and monitor certain trending incident or crime.
- g) System should be able to be integrated with Event Management / Incident Management System, if implemented by Guwahati Police in future.

#### **B. System Administration functionality**

- a) The System Administration Server shall provide a feature-rich administration client for system configuration and day-to-day administration of the system
- b) 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

### **C. 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

### **D. Client Viewing System**

The Client viewing 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).

### **E. Remote Web Client**

The web-based remote client shall offer live view of up to 16 cameras, 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

#### **F. Matrix Monitor**

- a) Matrix Monitor – The Matrix Monitor feature shall allow distributed viewing of multiple camera on the system on any monitor
- b) The Matrix Monitor feature shall access the H.264/H.265/MJPEG/MPEG4 stream from the connected camera directly or sourced through the recording server

#### **G. 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;
  - Graphical overview of the operational status and alarms from servers, network cameras and external devices including motion detectors and access control systems.
  - 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
- e) Based on alarms/alerts, customized/standard alert messages should be published on VMB/PA, after authorization by a supervisor/operator.

#### **H. Other Miscellaneous Requirements**

- a) 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 tampering 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 & the same can be listed in miscellaneous section of the commercial bid. 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.
- b) All the systems proposed and operationalization of Video Management System should comply with requirements of IT Acts.
  - c) Any hardware or software required to achieve the functional requirement and technical solution of the overall Project (may not be not specified in the schedule) is to be proposed in the Bid and borne by the SI.
  - d) SI shall be required to provide a standardized Mobile Application to integrate smart phones and tablets for 2-way communication with the Surveillance System in a secure manner. Guwahati Police may provide such tablets / smart phones to the designated Police Personnel. It will be responsibility of SI to configure such tablets / Smartphone, for the Surveillance System being implemented a part of this project and ensure that all the necessary access is given to these mobile users. Functionalities to be provided through mobile application: Viewing of any video steam from Central VMS, uploading of video / pictures central VMS, Location based GIS Map access, tagging of mobile device/location information for all relevant functionalities.
  - e) There would be the provision for Third party audit periodically, paid by GSCL separately. GSCL reserves the right to appoint any Independent Evaluation Agency at any time during the phases of the project.

### 5.1.3 Technical Specifications – CCTV Surveillance System

#### 5.1.3.1 Dome CCTV Cameras

#	Parameters	Minimum Specifications	Bidder Compliance (Yes/No)	Product Documentation Reference
1	Make	<to be provided by the bidder>		
2	Model	<to be provided by the bidder>		
3	Video Compression	H.265, H.264, M-Jpeg or better		
4	Shutter Time	1/5 sec. to 1/25,000 sec. or better		
5	Iris	Automatic with manual override or P-Iris		
6	IP delay	(typical) 30 fps: 200 ms		
7	FOV (Field of	Wide: 104° x 54° (H x V) Tele: 33° x 19° (H x V) & “+/-		

#	Parameters	Minimum Specifications	Bidder Compliance (Yes/No)	Product Documentation Reference
	View)/Angel	30° allowed"		
8	Video Resolution	2MP- 1920x 1080p		
9	Frame rate	Min. 30 FPS or better		
10	Image Sensor	1/2.8" Progressive Scan CMOS or better		
11	Lens Type	Motorized zoom/Auto focus		
12	Lens#	Lens can be 3.0 to 10 mm / 2.8 to 12 mm or better		
13	IR	IR with minimum 30 meters range, IR from same Camera OEM		
14	Multiple Streams	Triple streaming fully configurable / Multi-streaming		
15	Minimum Illumination	Colour: 0.1, Mono 0.05 lux, IR: 0 lux		
16	Auto adjustment + Remote Control of Image settings I	Saturation, contrast, brightness, sharpness, white balance, orientation: auto, 0°, 90°, 180°, 270°, mirroring of images, 4 Privacy masks, noise reduction, SNR >50 dB		
17	Defog	Automatically adjusts parameters for best picture in foggy or misty scenes (Auto/Off)		
18	Wide Dynamic Range	> 90 dB or Better		
19	Audio Streaming	Full-duplex / half duplex, 1 IN & 1 Out		
20	Protocol	IPv4, IPv6, UDP, TCP, HTTP, HTTPS, RTP/ RTCP, IGMP, ICMP, RTSP, FTP, DHCP, NTP (SNTP), SNMP, 802.1x, DNS, DDNS, SMTP		



#	Parameters	Minimum Specifications	Bidder Compliance (Yes/No)	Product Documentation Reference
21	Security	1. Three-level password protection, IP Address filtering, User Access Log, HTTPS encryption 2. 802.1x network authentication with EAP/TLS 3. Signed Firmware 4. FTP disabled and Telnet closed,		
22	Alarm I/O	Minimum 1 Input & 1 Output contact for 3rd part interface		
23	SD Card	Built in SD card slot with support up to 128 GB with Class 10 speed. Camera should have pre-installed SD card of 128 GB. The camera should have the facility to store the data on local SD card inside the camera in case of network connection loss and the stored data on SD card should be automatically sent to the storage when network reconnects.		
24	Operating conditions	-20 °C to +60 °C		
25	Casing	IP- 54 rated or better		
26	Certification	UL, EN, CE, FCC, RoHS, ONVIF profile S, G & T		
27	Power	PoE/12VDC. PoE to follow 802.3 AF/AT		
28	OEM Criteria	<ul style="list-style-type: none"> <li>• OEM without any JV/ Distributor Should have their own registered office in India since Last 7 years.</li> <li>• OEM without any JV/ Distributor Should have their own service center in India</li> </ul>		

#	Parameters	Minimum Specifications	Bidder Compliance (Yes/No)	Product Documentation Reference
		since Last 7 years. • OEM Shall have RMA Center in India. • Camera should have MTBF of minimum 7 years duly certified by NABL Accredited LAB or international reputed LAB.		

### 5.1.3.2 Fixed Bullet CCTV Cameras

#	Parameters	Minimum Specifications	Bidder Compliance (Yes/No)	Product Documentation Reference
1	Make	<to be provided by the bidder>		
2	Model	<to be provided by the bidder>		
3	Video Compression	H.265, H.264, M-Jpeg or better		
4	Video Resolution	2MP- 1920x 1080p		
5	Shutter Time	1/1 sec. to 1/10,000 sec. or better		
6	Iris	Automatic with manual override or P-Iris		
7	IP delay	(typical) 30 FPS: 200 ms		
8	FOV (Field of View)/Angel	Wide: 107° x 54° (H x V) Tele: 40° x 19° (H x V) & (+/- 30° allowed)"		
9	Frame rate	30 FPS at all resolutions or better		
10	Image Sensor	1/2.8" Progressive Scan CMOS or better		
11	Lens Type	Motorized zoom/focus		
12	Lens#	Lens can be 3.0 to 13 mm / 2.8 to 12 mm or better		
13	IR	IR with minimum 50 meters range, IR from same Camera OEM		

#	Parameters	Minimum Specifications	Bidder Compliance (Yes/No)	Product Documentation Reference
14	Multiple Streams	Quad stream		
15	Minimum Illumination	Colour: 0.1, Mono 0.05 lux, IR: 0 lux		
16	Auto adjustment + Remote Control of Image settings I	Saturation, contrast, brightness, sharpness, white balance, orientation: auto, 0°, 90°, 180°, 270°, mirroring of images, 5 Privacy masks, noise reduction, SNR >50 dB		
17	Defog	Available		
18	Wide Dynamic Range	> 120 dB or Better		
19	Audio Streaming	Full-duplex / half duplex, 1 IN & 1 Out		
20	Protocol	IPv4, IPv6, UDP, TCP, HTTP, HTTPS, RTP/ RTCP, IGMP, ICMP, RTSP, FTP, DHCP, NTP (SNTP), SNMP, 802.1x, DNS, DDNS, SMTP		
21	Security	<ol style="list-style-type: none"> <li>1. Three-level password protection, IP Address filtering, User Access Log, HTTPS encryption</li> <li>2. 802.1x network authentication with EAP/TLS</li> <li>3. Signed Firmware</li> <li>4. FTP disabled and Telnet closed,</li> <li>5. OEM need to confirm on their letter head that any component/ hardware/ parts/ assembly/ software including firmware used in the offered solutions</li> <li>6. Any of the security certifications of IEC/EN/UL -</li> </ol>		

#	Parameters	Minimum Specifications	Bidder Compliance (Yes/No)	Product Documentation Reference
		60950-1 /60950-22, IEC-62471		
22	Analytics	Edge-based analytics Line crossing, Enter / leave field, Idle / removed object, Crowd density estimation.		
23	Alarm I/O	Minimum 1 Input & 1 Output contact for 3rd part interface		
24	SD Card	Built in SD card slot with support up to 128 GB with Class 10 speed. Camera should have pre-installed SD card of 128 GB. The camera should have the facility to store the data on local SD card inside the camera in case of network connection loss and the stored data on SD card should be automatically sent to the storage when network reconnects.		
25	Operating conditions	-20 °C to +60 °C		
26	Casing	IP- 67 rated & IK 10 (casing)		
27	Certification	UL, EN, CE, FCC, ONVIF profile S, G & T		

#	Parameters	Minimum Specifications	Bidder Compliance (Yes/No)	Product Documentation Reference
28	Power	PoE/12VDC. PoE to follow 802.3 AF/AT		
29	OEM Criteria	<ul style="list-style-type: none"> <li>• OEM without any JV/ Distributor Should have their own registered office in India since Last 7 years.</li> <li>• OEM without any JV/ Distributor Should have their own service center in India since Last 7 years.</li> <li>• OEM Shall have RMA Center in India.</li> <li>• Camera should have MTBF of minimum 7 years duly certified by NABL Accredited LAB or international reputed LAB.</li> </ul>		

### 5.1.3.3 PTZ CCTV Cameras

#	Parameters	Minimum Specifications	Bidder Compliance (Yes/No)	Product Documentation Reference
1	Make	<to be provided by the bidder>		
2	Model	<to be provided by the bidder>		
3	Video Compression	H.265, H.264, M-Jpeg or better		
4	Video Resolution	2MP- 1920x1080p		
5	Shutter Time	1/1 sec. to 1/10,000 sec. or better		
6	Iris	Automatic with manual override or P-Iris		
7	IP delay	(typical) 60 fps: 200 ms		
8	Frame rate	50/60 FPS at full resolutions		
9	Image Sensor	1/2.8" Progressive Scan CMOS or better		

#	Parameters	Minimum Specifications	Bidder Compliance (Yes/No)	Product Documentation Reference
10	Lens	Auto-focus, 4.3 – 129 mm (-/+ 1mm) (corresponding to 30 X)		
11	Multiple Streams	Quad Stream		
12	Minimum Illumination	Colour: 0.04 lux @ F 1.6, B/W: 0.00 lux (at 30 IRE, F 1.6) or better		
13	Day/Night Mode	Colour, Mono, Auto		
14	Wide Dynamic Range	> 120 dB or Better		
15	Calibration	Automatic self-calibrating when height is set		
16	Pan	Pan: 360° endless/continuous, up to 120°/s		
17	Tilt	Tilt: 3° ~ 90°, up to 300°/s		
18	Zoom	30x optical zoom and 12x digital zoom		
19	Privacy Masks	24 individually configurable privacy masks		
20	Pre-set / Tour	256 pre-set positions, Minimum 8 Tour		
21	Image settings	Saturation, contrast, brightness, sharpness, white balance, BLC, Noise reduction, SNR >55 dB		
22	Defog	Automatically adjusts parameters for best picture in foggy or misty scenes (Auto/Off)		
23	Protocol	TCP, HTTP, HTTPS, RTP, FTP, RTSP, NTP, SMTP, 802.1x, IP v4 & v6 Remote Administration: Remote configuration and status using web-based tool		

#	Parameters	Minimum Specifications	Bidder Compliance (Yes/No)	Product Documentation Reference
24	Security	<p>1. Three-level password protection, IP Address filtering, User Access Log, HTTPS encryption</p> <p>2. 802.1x network authentication with EAP/TLS</p> <p>3. Signed Firmware</p> <p>4. FTP disabled and Telnet closed,</p> <p>5. OEM need to confirm on their letter head that any component/ hardware/ parts/ assembly/ software including firmware used in the offered solutions</p> <p>6. Any of the security certifications of IEC/EN/UL - 60950-1 /60950-22, IEC-62471</p>		
25	Local Storage	<p>Built in SD card slot with support up to 128 GB with Class 10 speed. Camera should have pre-installed SD card of 128 GB.</p> <p>The camera should have the facility to store the data on local SD card inside the camera in case of network connection loss and the stored data on SD card should be automatically sent to the storage when network reconnects.</p>		
26	Camera Analytics	<p>Camera must have edge base analytics Viz; Enter / leave field, Loitering, Line Crossing, follow route, Idle / removed object, Counting, Occupancy, Crowd density estimation. Bidder to ensure minimum 8 Different types of analytics shall run simultaneously in each Camera.</p>		

#	Parameters	Minimum Specifications	Bidder Compliance (Yes/No)	Product Documentation Reference
27	Alarm I/O	Minimum 4 Input & 2 Output contact integrated/ external for 3rd part interface		
28	Operating conditions with IR	-20 °C to +60 °C		
29	Audio	Audio Port -IN/OUT -Should be there in Camera.		
30	Casing	IP66 Rated		
31	Power	802.3at PoE+ (Class 4) or 24VDC/24AC		
32	Certification	UL, CE, FCC, RoHS, ONVIF Profile S, G & T		
33	IR Illuminator	Inbuilt 850nm intensity adjustable IR with minimum 180 meters range, with object identification		
34	OEM Criteria	<ul style="list-style-type: none"> <li>• OEM without any JV/ Distributor Should have their own registered office in India since Last 7 years.</li> <li>• OEM without any JV/ Distributor Should have their own service center in India since Last 7 years.</li> <li>• OEM Shall have RMA Center in India.</li> <li>• Camera should have MTBF of minimum 7 years duly certified by NABL Accredited LAB or international reputed LAB.</li> </ul>		

#### 5.1.3.4 Field Junction Box

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



#	Parameters	Minimum Specifications	Bidder Compliance (Yes/No)	Product Documentation Reference
3	Size	Suitable size as per site requirements to house the field equipment		
4	Cabinet Material	GI with powder coated		
5	Material Thickness	Min 1.2 mm		
6	Number of Locks	Preferably Two		
7	Protection	IP 55, Junction Box design should ensure to keep the temperature within suitable operating range for equipment's and should also avoid intentional water splash and dust intake		
8	Mounting	On Camera Pole / Ground mounted on concrete base		
9	Form Factor	Rack Mount/DIN Rail		
10	Other Features	Rain Canopy, Cable entry with glands, proper earthing and Fans/any other accessories as required for operation of equipment's within junction box.		

#### 5.1.3.5 Poles for Camera

#	Parameters	Minimum Specifications	Bidder Compliance (Yes/No)	Product Documentation Reference
1	Make	<to be provided by the bidder>		
2	Model	<to be provided by the bidder>		
3	Pole type	Hot Dip Galvanized after Fabrication with Silver coating of 86 micron as per IS:2629; Fabrication in accordance with IS-2713 (1980)		

#	Parameters	Minimum Specifications	Bidder Compliance (Yes/No)	Product Documentation Reference
4	Height	10 Meters (or higher), as-per-requirements for different types of cameras & Site conditions		
5	Pole Diameter	Min. 10 cm diameter pole (bidder to choose larger diameter for higher height)		
6	Cantilevers	Based on the location requirement suitable size cantilevers to be considered with the pole		
7	Bottom base plate	Minimum base plate of size 30x30x1.5 cm		
8	Mounting facilities	To mount RLVD Cameras, ANPR, CCTV cameras, Traffic Signals, Pedestrian Signals, Switch, etc.		
9	Pipes, Tubes	All wiring must be hidden, through tubes/pipes. No wires shall be visible from outside.		
10	Foundation	Casting of Civil Foundation with foundation bolts, to ensure vibration free erection (basic aim is to ensure that video feed quality is not impacted due to winds in different climatic conditions). Expected foundation depth of min. 100cms. Please refer to earthing standards mentioned elsewhere in the document.		
11	Protection	Lightning arrester shall be provided, to protect all field equipment mounted on pole.		

#### 5.1.3.6 PoE+ Switches (Industrial Rugged) – 4 Port

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

S. No.	Parameter	Minimum Specifications	Bidder Compliance (Yes / No)	Product Doc. Reference
3	Enclosure Type	Rack Mount / DIN Rail mount		
4	Subtype	Gigabit Ethernet		
5	Ports	4 x 10/100/1000 (PoE+) + 2 x combo Gigabit SFP, Switch should support MSA Compliant Rugged SFPs		
6	Power Over Ethernet (PoE)	PoE+		
7	PoE Budget	120 W or Better		
8	Performance	Forwarding performance (64-byte packet size): 09 Mbps or better Switching capacity: 12 Gbps or better		
9	Remote Management Protocol	SNMP 1,2,3, RMON 1,2,3,9 Telnet, HTTP.		
10	Protocols	a) Ring Protocol - Ethernet Ring Protection- G.8032 ready b) Static Routing Protocols		
11	Authentication Method	RADIUS/TACACS+		
12	Features	Flow control, layer 2 switching, BOOTP support, VLAN support, IGMP snooping, Syslog support, port mirroring, DiffServ support, MAC address filtering, Broadcast Storm Control, IPv6 support, Multicast Storm Control, firmware upgradable, Unicast Storm Control, firmware upgradable, STNP support, Spanning Tree Protocol (STP) support, Rapid Spanning Tree Protocol (RSTP) support, Multiple Spanning Tree Protocol (MSTP) support, Trivial File Transfer Protocol (TFTP) support, Access Control List (ACL) support, Quality of Service (QoS), LLDP support, DHCP relay, DHCP client, Energy Efficient Ethernet, Quality of Service (QoS), Media Access Control security (MACsec) on all ports or IP Security (IPsec)/Secure Sockets Layer (SSL).		
13	Compliant Standards	IEEE 802.3, IEEE 802.3u, IEEE 802.3z, IEEE 802.1D, IEEE 802.1Q, IEEE 802.3ab, IEEE 802.1p, IEEE 802.3af, IEEE 802.3x, IEEE 802.3ad (LACP),		

S. No.	Parameter	Minimum Specifications	Bidder Compliance (Yes / No)	Product Doc. Reference
		IEEE 802.1w, IEEE 802.1x, IEEE 802.1s, IEEE 802.3at, IEEE 802.3bt.		
14	RAM	128 MB		
15	Flash Memory	1 GB or Better		
16	Status Indicators	Port transmission speed, system, PoE, link/activity		
17	Power Requirement	Internal power supply		
18	Voltage Required	48V to 57V (Able to run on both AC or DC supply)		
19	Persistent PoE	Persistent PoE Switch should have option of redundant power solution to ensure there is no break in connectivity and power to POE devices wherever required.		
20	Per Port PoE Configuration	Switch shall support per Port PoE Configuration		
21	Surge Protection	Switch should support power surge protection on all ports.		
22	OEM Criteria	<p>1. OEM should be committed to India and should have a registered office, for at least the last 5 years with a charter to manufacture/design/sales/support of Carrier Grade Products.</p> <p>2. The OEM must have well documented Quality Manual and certification of that Quality Processes as per TL9000 and ISO 14001.</p> <p>3. OEM should not be blacklisted in India or Internationally.</p>		
<b>Environmental Parameters</b>				
23	Min Operating Temperature	0 Degree C or better		
24	Max Operating Temperature	+70 Degree C or better		
25	Humidity Range Operating	10 - 95% (non-condensing) or better & As per Guwahati weather conditions		
26	Compliance	FCC or CE compliance Ingress Protection-IP30		
27	MAC Address	Port Security for binding MAC address of IP Cameras to an interface.		

### 5.1.3.7 PoE+ Switches (Industrial -Rugged) – 8 Port

S. No.	Parameter	Minimum Specifications	Bidder Compliance (Yes / No)	Product Doc. Reference
1	Make	<to be provided by the bidder>		
2	Model	<to be provided by the bidder>		
3	Enclosure Type	Rack Mount / DIN Rail mount		
4	Subtype	Gigabit Ethernet		
5	Ports	8 x 10/100/1000 (PoE+) + 4 x combo Gigabit SFP, Switch should support MSA Compliant Rugged SFPs		
6	Power Over Ethernet (PoE)	PoE+		
7	PoE Budget	150 W for better		
8	Performance	Forwarding performance (64-byte packet size): 14 Mbps or better Switching capacity: 24 Gbps or better		
9	Remote Management Protocol	SNMP 1,2,3, RMON 1,2,3,9 Telnet, HTTP or better		
10	Protocols	a) Ring Protocol - Ethernet Ring Protection, G.8032 ready. b) Static Routing Protocols c) Dynamic Routing Protocol – OSPFv2 & OSPF v3 from day 1. d) Layer 3 multicast routing from day 1		
11	Authentication Method	RADIUS/TACACS+		

S. No.	Parameter	Minimum Specifications	Bidder Compliance (Yes / No)	Product Doc. Reference
12	Features	Flow control, layer 2 switching, BOOTP support, VLAN support, IGMP snooping, Syslog support, port mirroring, DiffServ support, MAC address filtering, Broadcast Storm Control, IPv6 support, Multicast Storm Control, firmware upgradable, Unicast Storm Control, firmware upgradable, SNTP support, Spanning Tree Protocol (STP) support, Rapid Spanning Tree Protocol (RSTP) support, Multiple Spanning Tree Protocol (MSTP) support, Trivial File Transfer Protocol (TFTP) support, Access Control List (ACL) support, Quality of Service (QoS), LLDP support, DHCP relay, DHCP client, , Energy Efficient Ethernet, Quality of Service (QoS), Media Access Control security (MACsec) on all ports or IP Security (IPsec)/Secure Sockets Layer (SSL).		
13	Compliant Standards	IEEE 802.3, IEEE 802.3u, IEEE 802.3z, IEEE 802.1D, IEEE 802.1Q, IEEE 802.3ab, IEEE 802.1p, IEEE 802.3af, IEEE 802.3x, IEEE 802.3ad (LACP), IEEE 802.1w, IEEE 802.1x, IEEE 802.1s, IEEE 802.3at, IEEE 802.3bt.		
14	RAM	128 MB		
15	Flash Memory	1 Gb		
16	Status Indicators	Port transmission speed, system, PoE, link/activity		
17	Power Requirement	Internal power supply		
18	Voltage Required	48V to 57V (Able to run on both AC or DC supply)		
19	Persistent PoE	Switch should have option of redundant power solution to ensure there is no break in connectivity and power to POE devices wherever required.		
20	Per Port PoE Configuration	Switch shall support per Port PoE Configuration		
21	Surge Protection	Switch should support power surge protection on all ports.		

S. No.	Parameter	Minimum Specifications	Bidder Compliance (Yes / No)	Product Doc. Reference
22	OEM Criteria	1. OEM should be committed to India and should have a registered office, for at least the last 5 years with a charter to manufacture/design/sales/support of Carrier Grade Products. 2. The OEM must have well documented Quality Manual and certification of that Quality Processes as per TL9000 and ISO 14001. 3. OEM should not be blacklisted in India or Internationally.		
<b>Environmental Parameters</b>				
23	Min Operating Temperature	- 0 Degree C or better		
24	Max Operating Temperature	+70 Degree C or better		
25	Humidity Range Operating	10 – 95 % (non-condensing) or better & As per Guwahati weather conditions		
26	Compliance	FCC or CE compliance Ingress Protection-IP30		
27	MAC Address	Port Security for binding MAC address of IP Cameras to an interface.		
28	Power Surge Protection			

#### 5.1.3.8 Online UPS for Field Locations

#	Parameters	Minimum Specifications	Bidder Compliance (Yes/No)	Product Documentation Reference
1	<b>Make</b>	<to be provided by the bidder>		
2	<b>Model</b>	<to be provided by the bidder>		
3	Capacity	1 KVA		
4	Technology	IGBT based PWM Technology, True Online UPS		
5	Input Frequency Range	Preferably 45 to 55 Hz		

#	Parameters	Minimum Specifications	Bidder Compliance (Yes/No)	Product Documentation Reference
6	Output Frequency Range	Preferably 45 to 55 Hz		
7	Output Voltage	Preferably 220VAC - 230VAC		
8	Voltage Regulation	Preferably +/- 2% (or better) and with built- in Over Voltage Cut off facility in the Device		
9	Frequency	Preferably 50 Hz +/- 0.1% (free Run Mode)		
10	Harmonic Distortion (THD)	Preferably < 3% (linear load)		
11	Output Waveform	Pure Sine wave		
12	Output Power Factor	0.8 or more		
13	Battery Backup	30 Mins Power backup Required. Adequate and required battery backup to achieve required uptime of field device as well as SLA of the overall solution.		
14	Battery Type	Preferably Lead acid, Sealed Maintenance Free (SMF)		
15	General Operating Temperature & Humidity	Temp.: (-)10 Degree C to (+)70 Degree C or better Humidity: 10 - 90% (non-condensing) As per Guwahati weather conditions		
16	Alarms & Indications	All necessary alarms & indications essential for performance monitoring of UPS like mains fail, low battery & fault detection		
17	Bypass	Automatic, Manual Bypass Switch		
18	Certifications	For Safety & EMC as per international standard • BIS Certification for the specific model offered • CE Certification • ISO 9001, ISO 14001, OHSAS 18001 certified. • RoHS Compliance		



#	Parameters	Minimum Specifications	Bidder Compliance (Yes/No)	Product Documentation Reference
19	Service Support	UPS OEM should have their own established service center and Service Engineers in Guwahati to attend any issues on 24x7 basis. Service Center should be fully operational for last 5 years		
20	Remote Monitoring & Maintenance Ports & LED Indication	a) SNMP port for remote monitoring. b) RS232/Management Port for onsite servicing. c) LED indicators to be mentioned for Load/Backup/Overload/etc.		
21	Overall Protection	IP 55, Junction Box design should ensure to keep the temperature within suitable operating range for equipment's and should also avoid intentional watersplash and dust intake		

#### 5.1.4 Video Management System (VMS)

Video Management System (VMS) shall bring together physical security infrastructure and operations and shall use the IP network as the platform for managing the entire surveillance system. End users shall have rapid access to relevant information for analysis. Bidder should include the hardware and software required to complete the proposed VMS solution without any additional cost.

This shall allow operations managers and system integrator to build customized video surveillance networks that meet their exact requirements. Software suite shall be a scalable and flexible video management system that could be easily managed and monitored. Scalable system shall permit retrieval of live or recorded video anywhere, anytime on a variety of clients via a web browser interface.

Video management server, on which the VMS is hosted upon, shall run seamlessly in the background to manage connections, access and storage. Video management server shall accept the feed from IP Camera installed at field locations. Server shall stream incoming video to a connected storage. VMS shall support video IP fixed color / B&W cameras, PTZ / Dome cameras, infrared cameras, low light/IR cameras and any other camera that provides a composite PAL video signal.

VMS shall facilitate situational awareness of the on-ground condition at Command Control Center or any other view center. This shall be achieved by transmission of real time

imagery (alarm based or on-demand). This imagery can be viewed live by operators and/or recorded for retrieval and investigation at a later time. Major functionalities are described here:

1. The VMS shall support a flexible rule-based system driven by schedules and events.
2. The 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.
3. The VMS shall support IP cameras of different makes.
4. All the offered VMS and cameras shall have ONVIF compliance.
5. VMS solutions shall be open standards, scalable and interpretable.
6. The VMS shall be enabled for latest technology (i.e. iSCSI) and any latest standard storage technologies and video wall system integration.
7. The VMS shall be enabled for integration with any external Video Analytics Systems.
8. The VMS shall be capable of being deployed in a virtualized environment without loss of any functionality.
9. The VMS server shall be deployed in a clustered server environment for high availability and failover.
10. The Video Management software shall be server Client Architecture, Server architecture in the way that camera shall stream incoming video to a connected storage directly
11. The Video Management software should be provided with Failover feature. In case of central server failure. All Clients should work independently and Recording of all Camera at ICCC (Integrated Command Control Centre) should not be impacted by the Central server failure. Bidder to consider N: N redundancy of VMS and Recording Servers.
12. VMS shall be designed in such a way the Central Server downtimes do not affect the functionality of the recording services (Video Recording Manager, Recording Station, Local Storage etc.). Normal recording and Motion recording shall continue during the Central Server downtimes
13. Video recording manager shall support the cameras to directly stream the data to the Internet Small Computer Systems Interface (iSCSI) Storage or any other compatible features.

14. Video recording manager shall provide load balancing and failover for the iSCSI storage system. Video Recording Manager (VRM) shall manage all disk arrays in the system as a single virtual common pool of storage. It shall dynamically assign portions of that pool to the encoders and IP-Cameras
15. VMS shall support security feature like Bit Encryption or any other compatible feature.
16. All CCTV cameras locations shall be overlaid in graphical map in the VMS Graphical User Interface (GUI). The cameras selection for viewing shall be possible via clicking in the camera location on the graphical map. The graphical map shall be of high-resolution enabling operator to zoom-in for specific location while selecting a camera for viewing.
17. The VMS shall have an administrator interface to set system parameters, manage codecs, manage permissions and manage storage.
18. The VMS day to day control of cameras and monitoring on client workstations shall be controlled through the administrator interface.
19. Whilst live control and monitoring is the primary activity of the Operator workstations, video replay shall also be accommodated on the GUI for general review and also for pre and post alarm recording display.
20. The solution design for the VMS shall provide flexible video signal compression, display, storage and retrieval.
21. All CCTV camera video signal inputs to the system shall be provided to command control Center, and the transmission medium used shall best suit the relative camera deployments and access to the CCTV Network.
22. The VMS shall be capable of transferring recorded images to recordable media (such as CD/DVD and/or DAT tapes) in tamper evident and auditable form. All/any standard formats shall be supported including, but not limited to:
  - a. AVI files
  - b. Motion- Joint Photographic Experts Group (M-JPEG)
  - c. Moving Picture Expert Group-4 (MPEG-4)
  - d. Windows Media Video (wmv) format (smaller files but transcoded)
  - e. Advanced Systems Format (asf)
23. All the streams shall be available in real-time (expecting the network latency) and at full resolution. Resolution and other related parameters shall be configurable by the administrator in order to provide for network constraints.

24. The VMS shall support field sensor settings. Each channel configured in the VMS shall have an individual setup for the following minimum 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
  
25. The VMS shall support the following minimum 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)
  
26. 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.
  
27. The VMS shall support bookmarking the videos. Thus, allowing the users to mark incidents on live and/or playback video streams.
  
28. The VMS shall be capable of intrusion detection: Detection of moving objects in selected areas covered by the camera (those that are specified as restricted areas like those before some major events, etc.). Avoid false alarms due to wildlife or other moving objects (e.g., tree leaves).
  
29. The VMS shall be capable of tracing of a specific person or object in multi-camera videos: Track a specific person or object across several surveillance (e.g., to trace and identify criminals and/or anti-social elements).
  
30. The VMS shall be capable of counting of people and detection of abnormal crowd behavior: Detection of people flow and counting of people in selected areas. To identify abnormal crowd behavior and raise alarms to avoid untoward incidences in public places and maintaining law & order.

31. The VMS shall be capable of summarize videos and create a content summary of the captured video depicting relevant movements or objects of interest. This would on off-line as well as online videos captured by the camera. For example, an hour-long surveillance video could be shortened by considering only the frames that depict major movements in the video.
32. The VMS shall allow the administrator to distribute camera load across multiple recorders and be able shift the cameras from one recorder to another by operating simple facility.
33. VMS shall support automatic failover for recording.
34. VMS shall support manual failover for maintenance purpose.
35. VMS shall support access and view of cameras and views on a smartphone or a tablet (a mobile device).
36. VMS/ICCC shall support integration with the ANPR application.
37. VMS shall support integration with other online and offline video analytic applications.

#### **5.1.4.1 VMS Core Components**

1. CCTV Camera Management – Shall enable management of cameras associated with the VMS.
2. Video recording, retrieval and archiving – Shall manage live camera viewing, recording of live feeds for future review, search and retrieval of recorded feeds and archiving of recorded video feeds for optimum utilization of resources.
3. Video Analytics (VA) alert management – Shall enable defining of rules for handling of alerts using the VA handling of events as per the defined rules.
4. MIS and Reporting – Shall provide users with business analytics reporting and tools to organize evaluate and efficiently perform day to day operations.
5. Security and Roles – Shall manage role definitions for internal as well as external access.

#### **5.1.4.2 VMS General**

1. Each camera shall be identified by giving it a minimum thirty-two (32) character long, alphanumeric unique id followed by text description field.

2. When viewed on the GIS map, the text description of each camera shall be capable of being positioned anywhere on the monitor screen, on a camera by camera basis, shall afford options for size variations, and display with a flexible solid, semi-transparent or transparent background – at VMS/ICCC.
3. The VMS shall support tamper detection for all cameras to warn of accidental or deliberate acts that disable the surveillance capability.
4. For alarm interfacing requirements, the VMS shall allow the selection of minimum five (5) cameras per single alarm source. The designated primary camera shall be automatically displayed as a full-screen image on the main GUI CCTV screen. The VMS shall also, on alarm, present associated pre/post event video allowing the Operator to assess the alarm cause. Other associated cameras, when called up, shall be displayed as split-screen images on the other monitor of the operator workstation.
5. Playback of any alarm related video, (including pre and post alarm video) shall start at the beginning or indexed part alarm sequence.
6. Video management software shall incorporate online video analytics on live video images. It shall include the following video analytics detection tools:
  - a. Presence detection for moving and stopped vehicles
  - b. Directional sensitive presence detection
  - c. Congestion Detection
  - d. Loitering detection
  - e. Improper Parking
  - f. Camera Tampering
  - g. Abandoned objects detection
7. Off-Line Video Analytics should allow for quick retrieval of video footage to metadata stored with each image. System should provide results within few seconds, system should support for below listed the user's query.
  - a) System should allow to specify the following search criteria:
    - i. Motion in the zone, user-defined with any polyline
    - ii. Detection of crossing a virtual line in a user-defined direction
    - iii. Loitering of an object in an area
    - iv. Simultaneous presence of a few objects in an area
    - v. Motion from one area to another.
  - b) System should support to apply below listed filters to search results:
    - i. Object size
    - ii. Object color
    - iii. Direction of object motion

- iv. Speed of the moving object
  - v. Defined area entry/appearance and zone exit/disappearance
8. Video clips of specific events via the VA or by the operator action shall be capable of being separately stored and offloaded by operator with appropriate permissions on to recordable media such as CD or Write Once Read Many (WORM) together with any associated meta-data for subsequent independent playback.
  9. The system shall provide the capability to select duration of storage by camera, time and activity event and user request. Frequency/trigger of transfer shall be configurable by user.
  10. The system shall provide the capability to digitally sign recorded video.
  11. **Live video viewing:** The system shall allow the viewing of live video from any camera on the system at the highest rate of resolution and frame rate that the camera shall support on any workstation on the network.
  12. **Recorded video viewing:** The system shall allow the viewing of recorded video from any camera on the system at whatever rate the camera was recorded.
  13. **Storage of video:** The system shall store online thirty (30) days of video for all cameras. Balance 60 days will be on low cost secondary storage (compressed form) or tape library.
  14. The system shall provide the capability to manage the video storage to allow backups and auto aging.
  15. VMS shall have an extensive reporting capability with ability for administrator to define reports in a user-friendly manner. The pre-existing reports shall include, but not limited to, the following:
    - a) Reports on alerts received by type, date and time, location
    - b) Reports on system errors and messages
    - c) Reports on master data setup including cameras, decoders, locations
    - d) Reports on cameras health check
    - e) Reports on audit trails such as user actions
    - f) Reports on system health including storage availability, server performance, recordings.

#### **5.1.4.3 VMS GUI Capabilities**

1. The user interface shall be via a GUI providing multiple video streams simultaneously on multiple monitors.

2. The GUI shall have the minimum capability of naming locations, users, and cameras events be displayed correctly on user's screen.
3. The system shall have the capability to store and record operator specific options, such as screen layout, video layout, action on alarm, and automatic video transmission settings on events.
4. The GUI shall conform to standard Windows conventions.
5. The system shall provide unified GUI camera control at an operator's workstation for all types of cameras installed whether existing or new or connected via another agency.
6. By means of this unified control the following functions shall be provided:
  - a) Selection
  - b) Display
  - c) PTZ
  - d) Setup and adjustment
  - e) Determination of pre-sets
  - f) Any other commissioning and camera setup activity
7. All user interfaces shall support English Language and shall conform to standard Windows protocols and practices and allow the control of all functions via a simple easy to use interface.

#### **5.1.4.4 VMS/ICCC Map Functionality**

1. The system shall support a mode of operation whereby a map of all or part of the map (at operator request) is displayed on a separate or same screen and that status information can be provided via an icon, and access to any cameras shall be accessible by means of an icon on that screen.
2. These Maps shall be defined so that an operator may select from the same source of mapping that is available to the other systems within the command control center, displaying whichever Map or section the operator needs, and it shall be displayed within one (1) second.

#### **5.1.4.5 VMS Configuration**

1. The VMS shall include a configuration facility to provide system administrators with a single interface utility to configure all VMS operating parameters.
2. The configuration tool shall be capable of supporting multiple concurrent users of the system, providing the ability to automatically update. It shall also allow the codec and camera configurations to be imported and exported in excel format.



3. The import/export tool shall be as sophisticated as necessary to support the following:
  - a. Log every action so an audit or report can be completed
  - b. Only update and log configurations where there is a difference between the system configuration and the new configuration file to be loaded
  - c. The import configuration file can contain any amount of data
  - d. Ability to run an update on the fly - i.e. no or minimal downtime to the system
  - e. Not require a reset or restart after any upgrades
  - f. Definable update times
  
4. The VMS configuration tool shall define:
  - a. Cameras (whether via codec units or directly connected IP cameras) and text-based names
  - b. Camera Groups
  - c. User Groups
  - d. Monitors
  - e. Codec parameters
  - f. Alarms
  - g. Workstations
  - h. storage
  
5. The configuration utility shall allow the system administrator to:
  - a. Install new devices
  - b. Configure all aspects of existing devices
  - c. Configure and set up users/user groups and their rights/permissions/priorities
  - d. To define multiple camera groups
  - e. Each group to be defined for combinations of viewing and control rights
  - f. Individual Operators to be assigned multiple groups
  - g. Each group to be allocated to multiple Operators
  - h. Each camera may be in multiple groups
  - i. Program camera/monitor selection and configuration of the video wall(s) in response to an incoming alarm
  - j. Designate workstation destination for picture presentation in response to alarm initiation
  
6. User permissions/privileges, to be allocated, shall extend from full administrator rights down to basic operation of the system, and shall include the ability to designate workstations to an operator, and to designate one or more camera groups to an operator for viewing and/or control.

7. The configuration utility shall store all changes to the system, including but not limited to:
  - a. User log-ins
  - b. User log-offs
  - c. Human interface device inputs (key strokes)
  - d. External alarm commands
  - e. Error messages
8. A copy of the system configuration shall be stored external to the system to allow system restoration in case of hardware failure. External would mean another site, to be agreed with (City) during detail design.

#### **5.1.4.6 VMS User Hierarchy**

1. The System Integrator shall request a detailed User Prioritization List (UPL) from the Authority during the project.
2. The UPL shall enable the programming of the CCTV management system with the agreed user prioritization.
3. Over and above user priority, users shall be enabled for the following in varying combinations:
  - a. Image viewing
  - b. Image recording
  - c. PTZ control
4. In addition, the control location shall be prioritized as such that the City Operation Centre has full control of all functions and priority one (1) override over all other locations.
5. Within the hierarchy, each user's log-on password shall not only allow access to varying levels of system functionality but shall also provide for a relative priority between users of equal access rights. In this manner, operators in the above groups shall be individually allocated a priority level that allows or denies access to the functions when in conflict with another operator of lower or higher priority level.
6. These priority levels and the features they contain shall be discussed and defined with the system administrator. The SI shall allow time to carry out this exercise together with the relevant configuration of groups, sub-groups, permissions and priorities.

#### 5.1.4.7 VMS Recording Requirements

All images shall be recorded centrally as a background process at configurable parameters.

1. It shall not be possible to interrupt, stop, delay or interfere with the recording streams in any way, without the appropriate user rights.
2. The CCTV recording system shall enable pre and post event (PPE) recording, presentation and storage, initiated automatically in response to system alarm sources received by the VMS.
3. The PPE recording clips shall be provided by the VMS and retrieved from the central video archive on the buffer storage system. This PPE stream shall be totally independent / same of the background recording stream provided to the central video archive such that central video archive recording, as programmed, continues under all circumstances
4. The information stored shall be full real-time and full resolution from each incoming camera channel. In the absence of a trigger from a manual input or from a programmed alarm source, the PPE video recording shall be written to buffer storage on a FIFO basis.
5. PPE periods initiated by a single alarm occurrence shall be configurable via the VMS as follows:
  - a. Pre – 0 to 30 seconds
  - b. Post – 30 to 300 seconds
6. Shall be variable for each camera according to each individual alarm and the alarm type
7. In the event of a trigger, the VMS shall ensure that the programmed sections of pre and post event video are immediately presented to the Operator to complement the alarm display and simultaneously saved as an identified indexed video clip, complete with time/date stamp, in a reserved and protected area of the storage system. Such PPE recording shall then be capable of later retrieval via search criteria.
8. Once tagged and saved, the PPE video clip shall NOT be overwritten except by an operator with the required permissions i.e. it is excluded from the normal FIFO regime of the bulk storage system. Recording shall also be initiated on-demand by manual triggers from system operators e.g. keyboard key-stroke.
9. The VMS shall support the following recording modes:

10. Total recording – the VMS shall constantly record the video input. The VMS shall allow for continuous recording of all video inputs
11. Event based recording – the VMS shall record the video input only in case an event has occurred
12. VMS shall support the following triggers to initiate a recording
13. Scheduler – the recorder will record the video inputs based on a specified schedule.
14. The VMS shall allow recording based on a time schedule for all or some of the video channels
15. The VMS shall allow for multiple recording periods per day, per channel
16. The VMS shall have the option for individual channel setup of pre/post-alarm recording for defined interval (e.g. up to 10 minutes pre-alarm and 30 min post-alarm recording)
17. The VMS shall have the ability to enable/disable triggers through a daily time schedule
18. Manual – the user shall be able to initiate a manual recording upon request.
19. The VMS shall work in conjunction to the any previous alarm operations
20. The VMS shall allow API Triggers / Object model
21. All trigger information shall be stored with the video information in the VMS data set and shall be made available for video search

#### **5.1.4.8 Manual or On-Demand Recording**

1. Recording shall also be initiated on-demand by manual triggers from system operators e.g. keyboard key-stroke (subject to user rights).
2. The system shall allow for an operator to initiate recording on any live steam being viewed.

#### **5.1.4.9 VMS Review System**

The VMS recording and replay management systems shall support the following features and operations:

1. Play back shall not interfere with recording in any way
2. Support either analogue cameras connected via Codecs or IP-cameras directly connected to the network

3. Stream live images through the network using IP Multi-cast techniques
4. Stream images from the Codec to the attached storage system
5. Store the recording stream from all cameras simultaneously with no degradation to any individual camera recorded image stream unless the system is configured by administrator to allow for change in quality
6. Deliver live video to VMS workstation within a period of one second from manual call up
7. Deliver live video to VMS workstation within a period of three seconds from automatic alarm receipt on alarm interface
8. Storage of each camera's images at a rate and resolution as defined in the Codec or IP camera configuration. The system VMS programming shall automatically vary these rates in response to time profiles, alarm inputs
9. Support multiple, configurable recording time schedules per camera. Each schedule shall support different recording parameters and automatically implement against the configured time schedule e.g. operational and non-operational hours shall be scheduled with different recording parameters on designated cameras
10. Playback multiple, synchronized recorded streams at differing speeds and frame rates
11. Record and playback a video stream simultaneously at differing speeds and frame rates
12. Time stamping of every recorded video field based upon Network Time Protocol (NTP) time
13. Selectable on-screen-display of time and camera title during playback
14. Security file lock to prevent specific recorded files from being overwritten regardless of their date and time, in addition to those records stored as PPE clips. The duration and policy for retention of such videos would be same as that of the PPE clips
15. Configurable granularity of video files
16. Generate alarm / take Report when storage medium has fallen below a user selectable threshold.
17. Stored video files can be "down-loaded" to directly CD ROM and/or DVD or WORM (Write once read many) for replay using the VMS video replay application, and shall incorporate proof of authenticity

18. Download video records in common (e.g. AVI) file format for remote, cursory review and assessment prior to generating tamper-evident auditable copies.

#### **5.1.4.10 VMS Alarm Handling**

1. The video alarm handling shall provide the following facilities for the handling and management of video images generated by alarms associated with other systems integrated with the VMS.
2. Whilst the pre and post alarm requirement has been included (up to thirty (30) seconds pre alarm, three hundred (300) seconds post alarm per camera at fifteen (30) FPS) the VMS shall display and manage the pre and post alarm information as follows for a maximum of two hundred (200) alarms per day:
3. The pre and post alarm video clip shall be displayed full screen, in real-time.
4. The pre and post alarm shall be displayed on a dedicated monitor
5. Each monitoring station shall be able to display simultaneous alarms
6. The 'video clip' associated with the alarm shall be tagged with date and time etc. and stored in a dedicated location for retrieval at a later date
7. Alarm archived video shall be readily available for one month but accessible for six months
8. The VMS shall accommodate at least 100 simultaneously alarm activating CCTV cameras
9. All alarm-based images shall be displayed
10. The VMS shall have the capability to automatically display a primary camera, plus minimum of four additional cameras associated with each alarm based on either camera locations with respect to the alarm, or a programmed set of parameters defining the associated cameras.
11. The VMS shall also accommodate operator-initiated recording of a given camera. The operator-initiated recording shall:
12. Record the selected camera/s for an administrator configured number of hours or until stopped, whichever is the sooner

#### **5.1.4.11 VMS Integration Requirements**

1. VMS shall be integrated within a consolidated GUI that would include other command control Center systems as well. All events, activations and alarms that

occur with the VMS and its sub systems will interact seamlessly between the command and control center sub systems as required

2. Either the OPC or the SDK or Object Model shall manage the interface between the VMS, GUI and the other City Management systems as required.
3. The OPC or SDK or Object Model shall allow the operator workstations to control the VMS irrespective of the vender chosen by duplicating all control functionality of the VMS used for normal day-to-day activities.
4. Alarm linking between VMS sub-systems shall be done at VMS sub-system level to, for example, call up relevant pictures to screens and move PTZ units to pre-set positions in response to alarm and activate video recordings, modifying recording parameters as necessary.
5. If an OPC interface cannot be provided, an alternative solution shall be provided for this data using a standard open protocol and confirmation as to how this shall be implemented shall be provided in the technical proposal return.
6. If an SDK solution / Object model is provided the system shall allow reconfiguration by (City) and end users without recourse to special languages. A system SDKs / Object model shall be supplied with all required supporting software to allow the integration of the system with new devices and systems.

#### **5.1.4.12 VMS System Size**

1. The VMS shall enable handling of up to at least 10,000 cameras for future scalability as may be required at additional cost of camera license.
2. The VMS OEM must have at least one project experience of minimum 2000 cameras in India. (PO copy required to be submitted).

#### **5.1.4.13 VMS System Health Monitoring And Audit Trail**

1. The VMS desktop client should show vital system parameters for components such as Database Server, Media Servers and Storage System (all available storages). The client should show the parameters such as CPU Core Usage, RAM Utilization and Storage Utilization.
2. The VMS client should have automatic or manual selection of hardware accelerator decoder or software accelerator decoder for smooth media rendering based on the available resources.
3. The VMS should have reports such as camera uptime availability, camera recording percentage, recording status, critical events, incident video, etc.
4. The VMS should allow the operator to raise support ticket from the VMS client itself.

5. The System health status like Server failure, Camera Disconnection, Storage Full Indication, etc. should always be displayed within the GUI all the time.
6. VMS should maintain a continuous log of Server Status Messages, Camera Connectivity, Storage Status, Recording ON/OFF, User Activity Logs, etc. which should be accessed from the workstations using different filters.
7. The VMS should allow for continuous monitoring of the operational status and event-triggered alarms from servers, cameras and other devices. The health monitoring module should provide a real-time overview of alarm status or technical problems while allowing for immediate visual verification and troubleshooting.
8. Health monitoring module should provide intuitive alarm management through the use tools including:
  - a) Detailed listing of all active or incoming alarms with available filters for time period, alarm source, operator and alarm state.
  - b) Ability to reassign alarms to other operators based on: change of state for one/multiple or all alarms, change of alarm priority, entering incident-specific log information and the suppression (snooze function) of alarms.
  - c) Ability to preview, view live or playback recorded images.
  - d) Automatically close an alarm based on a corresponding event.
  - e) Generate audit trail reports by incident.
9. The system should give full audit trail of the user activities in the system.
10. The system log should be searchable by Level, Source and Event Type.
11. The Audit Log should record remote user activity (searchable by User name, Audit ID, Source and Location)
12. The Alert Log should record alerts triggered by rules (searchable by Alert type, Source and Event type)
13. The Event Log should record event-related information (searchable by Service name, Source and Event type)
14. The Rule Log should record rules in which the Make new <log entry> action been specified (searchable by Service name, Source, Event type and Rule name)

The VMS should allow monitoring of the desktop screen activity of a user from the Administrator user console. This feature should replicate the entire user desktop and not just the VMS application window. This feature is required for audit of the operators. It should also be possible to monitor desktops of multiple users and record the entire activity to a file for any duration required.



#### **5.1.4.14 Video Analytics**

Surveillance system shall have the capability to deploy intelligent video analytics software on any of the selected cameras. This software shall have the capability to provide various alarms & triggers. The software shall essentially evolve to automate the Suspect activity capture and escalation; eliminate the need of human observation of video on a 24x7 basis.

Analytics software shall bring significant benefit to review the incidences and look for suspicious activity in both live video feeds and recorded footages.

Minimum video analytics that shall be offered on identified cameras are;

- a) Presence detection for moving and stopped vehicles
- b) Directional sensitive presence detection
- c) Congestion Detection
- d) Loitering detection
- e) Improper Parking
- f) Camera Tampering
- g) Abandoned objects detection
- h) Unattended object
- i) Object Classification
- j) Tripwire/Intrusion

The solution shall enable simultaneous digital video recording from network, intelligent video analysis and remote access to live and recorded images from any networked computer. It shall be able to automatically track and classify objects such as cars and people and push content to the respective security personnel as required for real time analysis. The system shall also have display of time line, customizable site map, live video, video playback, integrated site map, remote live view, multi-site capability, encryption, watermarking and event-based recording.

All cameras should support motion detection; camera tampering. All cameras must be capable to run two analytics in addition to motion detection and camera tampering as required at any given time.

Solution shall be so designed to have Automated PTZ camera control for zooming in on interesting events like motion detection etc. as picked up by camera without the need of human intervention. It shall be completely scalable, with a many-to-many client-server model allowing multiple physical systems to be used in an array of servers. The server specified in the RFP indicates only the minimum requirements. However, SI shall offer the server system to suit the video analytics requirements specified herein.

#### **a) Video Analytics Features:**

1. VA should support multiple Video Analytics servers running on different machines.
2. All the VA servers should form a cluster so that the Master server can allocate the VA processing tasks symmetrically amongst various servers to use available computational bandwidth judiciously. If the master VA server fails, the system should automatically select another master VA server without any manual intervention.
3. In case more than one VA server fails, the other servers should share the load of the failed server(s) to provide a failover support for VA applications.
4. VA should run on computer networks using industry-standard equipment.
5. The VA should be able to use free open source DBMS (e.g. PostgreSQL, MySQL) for all database related tasks.
6. VA should allow multiple instances of Client Viewer in a single workstation.
7. VA should be able to utilize multiple monitors connected to the workstation to perform various tasks simultaneously (e.g. Live viewing, Archive Search, Site map display, etc.)
8. VA should be capable of analyzing video from megapixel and high-definition enabled cameras.
9. VA should provide real-time generation of events to alert operators to irregularities.
10. The VMS should escalate the Events to recipients in the form of SMS/emails if the Events are not acknowledged by the operators within a specific period.
11. The VMS should send HTTP messages to any external server on receipt of the Events.
12. The VMS should show the Event messages on detection of Analytics events on the same Client live view panel instantly. On clicking on the message, relevant snap of the scene should appear on screen. On dragging the message to any video tile in the live view panel, the relevant portion of the video should be replayed automatically.
13. VMS should allow declaring any given video tile in the matrix layout as Event window. On detection of any Analytics event, the video Pop Up should instantly appear on the Event window.
14. VA should support simultaneous tracking of an unlimited number of targets within the detection regions and/or the cross lines.

15. The system should not store redundant Event clips on detection of events if the camera is already in recording mode.
16. VA should enable any combination of analytics rules to run on the same camera simultaneously, without limitations.
17. VA should enable the operator to define an unlimited number of detection regions per camera. The system should allow setting each region independently to be 'Active for VA' for any given period of the day.
18. It should be possible to enable different settings for the same VA application on the same camera automatically, based on hour of the day. The schedule to activate various settings at different hours of the day can be created by the user on the fly.
19. VA should have an alarm management system enabling operators to view video feeds streamed from multiple video cameras, from any PC on the network.
20. VA should enable managing multiple sensors simultaneously and will be capable of:
  21. Viewing multiple sensors meeting user-specified matching criteria (filtering)
  22. Applying common configuration settings on multiple sensors at a time
  23. Capturing a frozen image for multiple sensors.
24. VA should display a reference image with reference points for each camera, to facilitate camera identification if there's no live video stream and to align the camera back to its original position if it is moved.
25. VA should provide an events history.
26. VA should be capable of periodically purging the event database based on the event age or on a limited number of stored events. Purged events should be stored to external files for later viewing with a viewing or reporting mechanism.
27. VA should be capable of distributing event notifications to external applications – in particular: email notifications, SMS/MMS.
28. VA should allow generating reports of multiple types:
  29. For all event types, a report that contains the details for each event and also includes a captured image of the event.
  30. VA should be capable of searching over various time range options:
    - a) Over the past N minutes, hours or days (e.g., past 3 hours; past 7 days).
    - b) Given a starting and ending date and time of day

c) Over a recurring time, interval across a date interval (e.g., between 8-9 a.m., every day between Jan 1-10)

31. VA should be capable to generate Statistical analysis of various Events across different hours of the day.

32. VA should be capable to compare the occurrences of various Events across multiple days (at least 7 Days).

**b) Video Analytics Viewing Functions:**

1. VA should provide a fundamental capability to display video playback for any search result around the time that the search target / behavior was found:
2. The solution should continuously display a bounding box over the target (target tracking)
3. The solution should display the video playback in an infinite loop
4. VA should present a progress bar, including a graphic indication showing the time at which the search criteria were met.
5. VA should enable the user to Pause and Re-Play the video playback.
6. VA should enable the user to use the progress bar to navigate to any time position along the playback segment
7. The playback capability should be further incorporated with several viewing options as described below.
8. The solution should provide multiple options for viewing search results:
9. Event lists: After searching cameras for an event, the VA should be capable of displaying list of all the events in a tabular form. On clicking any entry in the table, a snap with the event detail should be displayed. It should be possible to play back the video of each event simply by a single click of mouse.

**5.2 COMPONENT 2 – INTEGRATED COMMAND CONTROL CENTRE (ICCC)**

### 5.2.1 Functional Requirement – ICCC

Snapshot of location and stakeholders operating each of the proposed Operations Centers is as follows:

Operations Center	Location	Stakeholder Operating CCC
Client Viewing Centre / Command Control Centre	As specified by the Authorities	GSCL/ Guwahati Police
Data Center	At Assam State Data Centre	GSCL/ System Integrator
Network Operations Center (NOC), Security Operation Center (SOC) and Help desk	As specified by GSCL NOC and Helpdesk is proposed to be co-located with City Operations Center / ICCC	System Integrator

1. The Command control center shall facilitate with a viewing and controlling mechanism for the selected field locations in a fully automated environment for optimized monitoring, regulation and enforcement of services. The command control Center shall be accessible by the operators and concerned authorized entities with necessary authentication credentials. The command control Center shall be used and manned by the Guwahati Police team to keep surveillance on civil issues.
2. Location for Command Control Center shall be at the designated location as decided by the Authority. The main data center infrastructure of the entire smart city components will be housed at Assam State Data Centre (SDC) for which the Authority will provide space and power to the SI.
3. The Command Control Center shall provide a comprehensive system for planning, optimizing resources and response pertaining to the standard functions of City Police and Guwahati Smart City Limited (GSCL).
4. The SI shall be required to undertake detailed assessment of the requirements at the Command Control center and commission required IT and non-IT infrastructure and also carry out the civil/ electrical work as required.
5. The data and surveillance network share the same physical infrastructure with guaranteed bandwidth for each individual segment. The software components provide comfortable monitoring experience, easy extraction of clips, and management of storage.

6. The video feed from the surveillance cameras shall be received at the command control Center where a Full HD LED Display video wall shall be installed for viewing relevant feed from the surveillance cameras. The operator on each of the workstation shall be able to work on multiple monitors at the same time, for which there is requirement of multi screens (specifically three) with one computer to be installed on work desks (appropriate furniture) with appropriate multi monitor mounts.
7. Authority shall carry out a detail assessment of the proposed design solution and review design for the Command Control Center, Data center on the parameters of overall Design, Safety & Security and reserves it right to accept, reject or suggest for modifications on the proposed solution.
8. With the increasing urbanization, the operational issues are increasing which in turn affect the quality of services offered to the citizens. Various government agencies provide multiple services to the citizens. These agencies function in silos and provide a wealth of information which can be utilized for efficient services across the city in making decisions anticipating the problems and by ensuring cross-agency responsive actions to the issues with faster turnaround time.
9. IOE (Internet of Everything) involves leveraging on the information provided by different devices/ platforms & various departments and providing a comprehensive response mechanism for the day-to-day challenges across the city. IOE shall be a fully integrated portal-based solution that provides seamless incident – response management, collaboration and geo-spatial display.
10. IOE shall provide real-time communication, collaboration and constructive decision making amongst different agencies by envisaging potential threats, challenges and facilitating effective response mechanisms. Thus, this Integrated Operation Platform (IOP) provides a Common Operating Picture (COP) of various events in real-time on a unified platform with the means to make collaborative and consultative decisions, anticipate problems to resolve them proactively, and coordinate resources to operate effectively.
11. The IOE platform should have high processing power and adequate data storage with a high-performance information highway to provide process information in real time and serving decision support system. The IOE platform should also provide portability to meet changing city scenario. The SI is required to provision data storage and processing power of the platform adequately to meet the system design and functionality to be achieved.
12. IOE solution should be capable of seamless integration to various government and emergency services such as law enforcement, disaster and emergency services, utility services etc., the proposed solution should support recording of external mobile video feeds, data communication, telephony etc., it should support scenario reconstruction and analytics capabilities with event timelines. The solution should support event logs

including operator's onscreen activities, voice & video events etc., for further analysis, training and similar activities.

13. Built in analytical tools provide real-time analysis of individual events and a measure of the incidents for each of the silos integrated on the platform. These help the decision makers with the in-situ challenges and facilitate immediate responsive actions to mitigate / control multiple complex challenges.
14. However, the platform shall support adding more layers of solutions seamlessly with minimal effort which Authority intends to develop in time to come such as:
  - Water Management
  - Smart Parking
  - Smart Pole
  - Disaster Management
15. The proposed information should be sharable on intra city and inter cities levels based on approved rights on mutual consent.
16. On the Integrated Operation Platform (IOP), the system shall provide Standard Operating Procedures (SOPs), step-by-step instructions based on the Authorities policies and tools to resolve the situation and presents the relevant situation information in a quick and easily digestible format for an operator to verify the situation. 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.
17. The city Operation center will also provision for the monitoring and control for smart city components other than City Surveillance. However, the Authority intends to provision for city surveillance monitoring cum viewing for critical field cameras and other security equipment as per the city's requirement. Moreover, all this will integrate into IOE platform.
  - The inputs/feeds from the different components of Smart City Solutions shall be received at City Operation Center video wall for monitoring, tracking and decision support purpose on real time basis supported with GIS technology. Further, operators shall be working on their respective monitors for assessing the inputs and triggering actions at ground level.

## **5.2.2 Technical Specification – ICCC**

### **5.2.2.1 Integrated Command Control Platform**

S. No.	Functional Parameters/ Description	Compliance (Yes/No)
	<b>Data Normalization capabilities</b>	
1	The Integrated Command and Control (ICCC) should have an integrated view of all the smart initiatives undertaken by GSCL with the focus to serve as a decision support engine or city administrators in day-to-day operations or as and when required.	
2	ICCC involves leveraging on the information provided by various departments/devices/sensors and providing a comprehensive response mechanism.	
3	It is envisaged that the city will implement multiple Smart City use cases like Smart Traffic Management, Smart Parking, Smart Lighting, Energy Metering, Water Metering, CCTV , Public Transport, Public Wi-Fi and other integrations as per defined scope .	
4	The platform shall also allow the manufacturers of the sensors to develop integrations themselves using SDKs/equivalent technology without affecting the northbound applications and existing integration.	
5	The platform shall 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.	
	<b>Distributed Architecture</b>	
6	The platform shall support distributed deployment of functions (workflows & policies) across city's network and compute infrastructure with centralized management and control.	
	<b>GIS Map Support &amp; Location engine</b>	
7	System shall support ESRI, Map Box, Open street etc.	
8	a) Map services and geospatial coordinates: provides the geographical coordinates of specific facilities, roads, and city infrastructure assets, as well as unmapped facilities.	
9	b) Geospatial calculation: calculates distance between two, or more, locations on the map.	
	<b>Platform Visualization</b>	
10	Platform must provide multiple options to visualize geo-spatial, operational and metrics data	
11	Platform must provide various visual widgets like Maps, Graphs, KPI, Tables, Scorecards, etc.	
12	Platform must provide end-users an ability to create dashboards and configure various widgets	
13	Platform must provide end-users an ability to share the dashboards with other users of the system	
14	Platform must provide an ability to create KPI's, Graphs and Maps from different sources of the data	



S. No.	Functional Parameters/ Description	Compliance (Yes/No)
15	Platform must provide an ability to prepare the data for visual analysis	
16	Platform must provide an ability to slice and dice based on regions, time and other criteria for detailed visual analysis	
17	Platform must provide ability to configure various geo-spatial data from different providers including but not limited to City GIS systems	
18	Platform must provide ability to support different geo spatial formats from commercial and open geospatial consortium standards like WMS, KML, SHP, City GML.	
	<b>Device engine</b>	
19	Aggregation and abstraction of sensors: provides aggregation of sensors from diverse sensor cloud.	
20	Normalization of sensor data: organizes sensor data and assigns attributes based on relations; raw data removed and passed to data engine.	
	<b>Data and Analytics engine</b>	
21	Data archive and logging: stores data feeds from the device engine and external data sources.	
22	Analytics: provides time-shifted or offline analytics on the archived data.	
23	Reporting: delivers reports based on events triggered by device engine data and external notifications.	
	<b>Developer Program tools</b>	
24	Sensor platform OEM shall provide Developer Program tools that help City to develop/integrate new applications, and/or use solution APIs to enhance or manage existing solution at no extra cost.	
	<b>Authentication, Authorization</b>	
25	System shall support standard Authentication, Authorization Performs.	
	<b>Data plan Functionalities</b>	
26	Live data and visual feed from diverse sensors connected to the platform.	
	<b>API Repository / API Guide</b>	
27	Normalized APIs shall 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.	
28	Platform OEM shall 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.	

S. No.	Functional Parameters/ Description	Compliance (Yes/No)
29	Cross APIs Integration: Enabling contextual information and correlation across domains and verticals (Multiple vendor and Multi-sensor in future).	
	<b>Platform upgrade and maintenance</b>	
30	Facility to securely access the platform remotely for platform updates / upgrades and maintenance for the given duration.	
31	Platform shall be able to be deployed on a public/private cloud for disaster recovery.	
	<b>Platform functionality</b>	
32	API management and gateway: Provides secure API lifecycle, monitoring mechanism for available APIs.	
33	User and subscription management: Provides different tier of user categorization, authentication, authorization, and services based on the subscriptions.	
34	Application management: Provides role-based access view to applications.	
35	The platform shall also be able to bring in other e-governance data in the command and control centre dashboard.	
36	All of these data shall be rendered / visualized on the command and control centre dashboard.	
	<b>Integration capabilities</b>	
37	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.	
38	Integrate devices using their APIs in to this platform. For example, if the City wants to deploy Smart Parking solution, this platform shall have the ability and provision to write adapters 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.	
39	The same logic and requirement apply 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.	
40	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.)	
41	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.	

S. No.	Functional Parameters/ Description	Compliance (Yes/No)
42	Provides urban services API(s) to develop Operations applications for each of the Urban Services domains. For example, the lighting operator of the City shall be able to develop a City Lighting management application based on the API(s) provided by the platform. This lighting application shall also have the ability to access data from other domains like environment based on the access control configured in the system.	
43	Platform must be modular and should provide an ability to host various integration adapters	
44	Platform should integrate with IT, OT, IoT, Video Analytics, VMS devices and applications	
45	Platform must provide an ability for IOT devices to upload the data in Real-time into the platform	
46	Platform must be providing a web-based application to develop, test and host adapters connecting various sources city data like sensors, applications, open-data, e-gov applications to the Smart city platform.	
47	Adapter deployment must be hot-deploying	
48	Adapter studio must have capability to consume data from multiple sources with different communications such as web services, Web Sockets, FTP, Fileserver, MQTT, real-time streams, etc.	
49	Adapter studio must support various formats like JSON, XML, CSV, TSV	
50	Adapter studio should have various standard authentication mechanisms	
51	Adapter studio must be able to impute, cleanse and transform data at attribute level	
52	Adapter studio must support development of an adapter that is capable of aggregating data from multiple sources.	
53	Integration Platform must push and pull data from various sources. The push and pull frequency should be configurable.	
54	Integration Platform must cache the data for faster performance	
55	Platform must have facility to export and import adapters	
56	Platform must be able to push or pull requests or consume data in real time	
57	Platform must be able to support multiple data types viz. hex, int, string, char, float	
58	Platform must have the following orchestration capabilities <ul style="list-style-type: none"> <li>- Hierarchical or Nested Aggregation</li> <li>- Chain based flow</li> <li>- Custom Transformation</li> </ul>	
59	Platform must have transformations snippets library for rapid transformation	

S. No.	Functional Parameters/ Description	Compliance (Yes/No)
	<b>Policies and Events</b>	
60	System shall allow policy creation to set of rules that control the behaviour of infrastructure items. Each policy shall provide a set of conditions that activate the behaviour it provides.	
61	System shall allow Default, Time-based, Event-based and Manual override polices creation. For example, an operator might enforce a "no parking zone/Lane close/ Electricity shout down" policy manually to facilitate on demand operations.	
62	System shall provision to defines a set of conditions that can be used to trigger an event-based policy	
	<b>Notifications, Alerts and Alarms</b>	
63	System shall generate Notification, Alert and Alarm messages that shall be visible within the Dashboard/GIS Platform and to the respective authority over Mobile App if required.	
64	All system messages (notifications, alerts and alarms) shall always visible from the Notifications view, which provides controls that operator can use to sort and filter the messages that it displays.	
65	Systems shall deliver message to a set of subscribers. The Notification service shall support min two types of notification methods – Email notification and Short Messaging Service (SMS) notification and any other mode available.	
	<b>Users and roles</b>	
66	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 shall be associated with one or more roles and each role is assigned a certain set of permissions for better access and responsibility.	
67	These roles and permissions define the tasks that a user can perform. Additionally, system shall assign one or more locations to each role so that the user can perform tasks at the assigned locations only.	
68	The platform shall allow different roles to be created and assign those roles to different access control policies.	
69	System shall support LDAP to be used as an additional data store for user management and authentication.	
	<b>Data Security</b>	
70	The access to data shall be highly secure and efficient.	
71	Access to the platform API(s) shall be secured using API keys.	
72	Software shall support security standards: OAuth 2.0, HTTPS over SSL or equivalent security standards help protect the data across all domains.	
	<b>Global Market Presence &amp; Support System</b>	

S. No.	Functional Parameters/ Description	Compliance (Yes/No)
73	Smart city suppliers shall be adaptable to the emerging needs of cities. Suppliers shall 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.	
74	Smart City Platform/Software provider shall be reputed company and Member of Smart Cities Council or Navigant Research Report for Smart Cities Suppliers.	
75	ICCC OEM shall have registered office in India at least from last 05 Years and shall have development centre in India. Shall have Quality Management System ISO 9001 OR Environmental Management System ISO 14001 Quality Certifications.	
	<b>Standard Operating Procedures</b>	
76	Integrated Command & Control Centre shall provide for authoring and invoking un-limited number of configurable and customizable standard operating procedures through graphical, easy to use tooling interface.	
77	Standard Operating Procedures shall be established, approved sets of actions considered to be the best practices for responding to a situation or carrying out an Operations based on use cases defined as per city and solution requirement.	
78	Ability to edit the SOP, including adding, editing, or deleting the activities.	
79	The users shall be able to also add comments to or stop the SOP (prior to completion).	
80	There shall 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.	
81	Platform must be able to create SOP workflows	
82	Workflow must support both automated and manual activities (tasks) and each of the activity should be configurable	
83	The SOP Tool shall have capability to define the following activity types:	
84	Manual Activity - An activity that is done manually by the owner and provide details in the description field.	
85	If-Then-Else Activity - A conditional activity that allows branching based on specific criteria. Either enter or select values for Then and Else.	
86	Notification Activity - An activity that displays a notification window that contains an email template for the activity owner to complete, and then sends an email notification.	
87	SOP Activity/Trigger - An activity that launches another standard operating procedure.	

S. No.	Functional Parameters/ Description	Compliance (Yes/No)
	<b>Events Processing</b>	
88	Platform should support event processing in real time.	
89	Platform be able to create event processing templates	
90	Platform must be able to raise events based on thresholds	
91	Platform must be able to raise events based on conditions happening in a time window	
92	Platform must map SOP workflows with event	
93	Platform should provide an ability to request an approval before SOP workflow is executed	
94	Platform should provide an ability to create and manage distribution lists for emails, SMS.	
	<b>Mobile App</b>	
95	Platform should provide a mobile app for the field staff to view real time events, manage their tasks, assign tasks, report incidents and collaborate with back-office and other field officers to address a SOP task	
96	Mobile application should only display events and tasks based on pre-configurable access rules based on department and region	
97	Mobile application should support escalation hierarchy of the tasks or events are not redressed with-in a defined SLA	
98	Mobile application should provide an ability to track field officers	
99	Mobile application should provide collaboration with the app for field officers and other staff to coordinate	
100	Mobile application should be available on iOS and Android latest versions	
	<b>Analytics/Analytical Engine</b>	
101	Artificial intelligence-based smart city/ICCC 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.	
102	Shall be flexible to integrate with other city and government software applications.	
103	Analytics Engine module shall have below intelligence capabilities;	
103.1	a) Advanced Predictive Analytics shall be part of the solution.	
103.2	b) The solution shall be deep learning based	
103.3	c) The solution should support supervised, semi-supervised or unsupervised Machine learning	
103.4	d) The solution shall be able to predict insights consuming data from city infrastructure viz., Traffic, Parking, Lighting etc.	
103.5	e) The solution shall have predictions with confidence level of at least > 90%	

S. No.	Functional Parameters/ Description	Compliance (Yes/No)
103.6	f) The solution shall be able to predict and integrate with Smart City solutions helping in driving operational policies creation.	
103.7	g) The solution shall be robust, secure and scalable.	
103.8	h) The solution shall have a visualization platform to view historic analytics	
104	The application shall enable the customers to discover, compare, and correlate data across heterogeneous data sources. When working with the application, system shall perform the following functions:	
104.1	a) Connect to a variety of data sources	
104.2	b) Analyse the result set	
104.3	c) Visualize the results	
104.4	d) Predict outcomes	
105	Analytics Engine shall support multiple Data Sources. At least below standard data sources shall be supported – CSV, TSV, MS Excel , NOSQL, RDBMS	
106	Analytics Engine shall provide analysis of data from a selected data source(s).	
107	Analytics engine shall provide capability to check analysis with multiple predictive algorithms.	
108	The Platform must be able to do change-over-time predictive geo-spatial analytics	
109	The Platform must be able to do predictive analysis of city elevation data with outcomes during disasters	
110	The platform must be able to provide actionable insights	
111	The platform must provide pre-built outcome models for rapid deployment with minimal changes	
112	The platform must have capability to do textual, geo spatial analytics	
113	The platform must be able to predict data anomalies in sensor data	
114	The platform must be able to impute values and make predictions	
115	The platform must be able to make predictions with IT, IoT and OT data	
116	The platform must be able to consume data from across domains and provide a single insightful outcome.	
	<b>Reports</b>	
117	The platform shall have capability to provide access to real time data and historical data from various connected devices for reporting and analytics.	
118	The platform must provide a user interface for reporting	
119	System shall allow dashboard to generate reports and have provision to add reports in favourites list.	
120	Platform must have the capability to create self-service reports	
	<b>Report Engine Visualizations</b>	

S. No.	Functional Parameters/ Description	Compliance (Yes/No)
121	Reports Engine shall provide visualizations dashboard.	
122	In the visualization workspace it shall allow to change visual attributes of a graph.	
123	User shall not be allowed to alter the graph/visualization definition.	
124	In the visualization's workspace, user shall able to do the following Operations:	
124.1	a)Change the graph/visualization type	
124.2	b) Print the graph	
124.3	c) Export the graph	
124.4	d) Narrow/Drill down on the value ranges	
124.5	e) Toggle and change the axis labels	
124.6	f) Integrate with other 3 <sup>rd</sup> party applications seamlessly	
125	Reports Engine shall support multiple Data Sources. Min below standard data sources shall be supported – CSV, TSV, MS Excel , NOSQL, RDBMS	
126	System shall allow export the report into min following formats: a) XML/JSON b) Excel/CSV c) PDF	
	<b>Video Display and integration capabilities with VMS Solution</b>	
127	Integrates with existing cameras and new cameras. Shall support multiple video sources from multiple locations. Platform shall have no limitation in displaying the number of CCTV video sources.	
128	Integrate and assess inputs from different sources such as CCTV, Video Analytics, and sensors further to assist with actionable intelligence.	
129	Smart City Operations Centre shall support 20 to 30 camera feeds in display.	
130	Must be able to display video streams on all browsers	
	<b>Technical support centre</b>	
131	ICCC OEM shall have 24x7x365 technical assistance support centre (TASC) in India. TASC shall provide online website and phone number to register service request, service request can be raised by partner and customer.	
	<b>CCC Operations</b>	
132	The solution shall be implemented and compliant to industry open standard commercial-off-the-shelf (COTS) applications that are customizable.	
133	The solution shall integrate with GIS and map information and be able to dynamically update information on the GIS maps to show status of resources.	



S. No.	Functional Parameters/ Description	Compliance (Yes/No)
134	The solution shall also provide an integrated user interface for all the smart elements implemented.	
135	The solution shall provide operators and managers with a management dashboard that provides a real time status and is automatically updated when certain actions, incidents and resources have been assigned, pending, acknowledged, dispatched, implemented, and completed. The above attributes shall be colour coded.	
136	The solution shall provide the “day to day Operations”, “Common Operating Picture” and situational awareness to the centre and participating agencies during these modes of Operations.	
137	It shall improve scalability for large and geographically distributed environments.	
138	It shall provide complete view of sensors, facilities, video streams and alarms in an easy-to-use and intuitive GIS-enabled graphical interface with a powerful workflow and business logic engine.	
139	It shall provide a uniform, coherent, user-friendly and standardized interface.	
140	It shall provide possibility to connect to workstations and accessible via web browser.	
141	The dashboard content and layout shall be configurable, and information displayed on these dashboards shall be filtered by the role of the person viewing dashboard.	
142	The solution shall allow creation of hierarchy of incidents and be able to present the same in the form of a tree structure for analysis purposes.	
143	The solution shall be available via a VPN as a web-based interface or a thin-client interface.	
144	m) It shall be possible to combine the different views onto a single screen or a multi-monitor workstation.	
145	The solution shall maintain a comprehensive and easy to understand audit trail of read and write actions performed on the system.	
146	The solution shall provide ability to extract data in desired formats for publishing and interfacing purposes.	
147	The solution shall provide ability to attach documents and other artifacts to incidents and other entities.	
148	The solution is required to issue, log, track, manage and report on all activities underway during these modes of Operations: <ul style="list-style-type: none"> <li>· anticipation of incident</li> <li>· incident or crisis</li> <li>· recovery</li> <li>· incident simulation</li> </ul>	
	<b>API &amp; Interface Security</b>	

S. No.	Functional Parameters/ Description	Compliance (Yes/No)
149	The access to data shall be highly secure and efficient.	
150	Access to the platform API(s) shall be secured using API keys.	
151	Software shall support security standards: OAuth 2.0, HTTPS over SSL, and key management help protect the data across all domains.	
152	Shall support security features built for many of its components by using HTTPS, TLS for all its public facing API implementations. For deployment where CCC Software API(s) exposed to application eco system, API Management, API security features and API Key management functions are required.	
153	The platform should be based on open API for various data & IOT providers to integrate with platform	
154	The platform should also publish API to consume the data from the smart city platform	
155	The platform should be providing an ability to restrict access to certain API	
156	The platform should provide API documentation for public access	
157	The platform should provide an ability to view access logs, API usage metrics	
	<b>Unified Communication Platform for Smart ICCC Operation</b>	
158	The proposed Communication Platform should streamline communications and enhances productivity with integrated presence, Chat, voice and video, desktop sharing, UHF/ VHF Communication and conferencing capabilities. The System must be capable of calling between operator, UHF/ VHF, VoIP and PSTN or mobile network. The system should have capabilities of achieving collaboration between any users of control room. the system should have capabilities enabling HD Video meetings between Smart City Team and other departments like Fire, Ambulance, Police, Traffic, etc.	
	<b>ICCC operator communication tool</b>	
159	Ability to bring multiple stake holders on to a common voice conference call as a standard operating procedure in response to event	
160	Ability to bring in multiple stake holders automatically into a common collaboration platform like chat rooms/etc. in response to a SOP defined to handle a particular event	
161	The platform should allow stakeholders to share content relevant to the issue in the Chat Rooms/etc.	
162	Ability to bring multiple stake holders on a Common Video Conference Call and share content on the call	
163	Details specification is mentioned below in “unified communication client” section.	
	<b>Dispatch System for Command and Control Operations</b>	

S. No.	Functional Parameters/ Description	Compliance (Yes/No)
164	Integrates Push-To-Talk (PTT) with IP-based communications in a single integrated environment	
165	Integrates disparate push-to-talk systems with other voice systems	
166	Integration provide on-demand incident communications across multiple groups. The users in the group can be on IP Phone, UHF/ VHF, Mobile network or PSTN	
167	Integrated different frequencies and protocols such as P25, TETRA, UHF, VHF and others	
168	PTT functionality should be enabled on Dispatch Console in ICCC, IP Phones in ICCC	
169	Dispatch Console should be able to track the location on Field operator with Mobile PTT application	
170	The system shall provide the ability to select multiple channels at the same time to make an outbound communication to all selected channels. Channels can be combination of IP Phone, UHF/ VHF, Mobile network or PSTN	
171	The system shall create virtual talk groups (VTGs) to facilitate Push-to-talk (PTT) communication between users of multiple types and technologies of Land Mobile Radios with users of desktop PCs, landline phones, cellular phones, smart phones, and IP phones	
172	The system shall utilize cluster redundant servers on the main authenticating server and media servers to provide high availability (1+1 or N+1) with no single point of failure. The system server software should have the ability to run on bare metal or in virtualized environments.	
173	The system should automatically identify potential audio loops and resolve them before they cause any audio issues so that audio channels and talk groups shall remain clear without feedback	
174	The system shall enable the dispatcher to combine resources, including users and channels, to create Virtual Talk Groups (VTGs) and be able to quickly add or remove resources depending on incident status	
175	The system should automatically identify potential audio loops and resolve them before they cause any audio issues so that audio channels and talk groups shall remain clear without feedback	
176	The system shall provide a web service API to integrate with third party applications, such as Command and Control systems, surveillance command and control center and Computer Aided Dispatch (CAD) applications.	
177	The system shall support role-based management for System Administrator, Operator, Dispatcher and Users	
178	The system shall provide license management to manage system feature licenses and to support upgrades or feature additions.	

S. No.	Functional Parameters/ Description	Compliance (Yes/No)
179	The system shall provide an audit trail for analysis and operations management	
180	The system shall perform audio mixing functions server that is scalable. The HA servers shall be geographically separated or located together in the same data center.	
181	The system should support an E&M interface to radio systems. In case the radio systems have a serial interface such as TETRA PEI, the system should have ability to support the serial interface to control radio channels on the respective radio system.	
182	As PTT base station radios will be physically integrated with in datacentre so there is no requirement to replicate this solution in DR.	
<b>IP-based dispatch console</b>		
183	The dispatch console shall be a Microsoft Windows program with Windows 10 support.	
184	The Dispatch Console shall provide control of radio resources through an on-screen interface.	
185	The dispatch software shall run on a standard PC platform, and extend existing push-to-talk (PTT) radio channels so that users with a variety of communication devices can participate in incident communication	
186	It shall enable users to monitor and coordinate emergency response across incompatible radio systems and between multiple departments and agencies.	
187	It shall have a separate tab for Virtual Talk Group's, Policies, and Incidents.	
188	It shall have a multi-line dialer where each dispatcher can patch up to 10 phone calls to channels.	
189	It shall have the ability to tear away the parts of the Graphic User Interface (GUI) so that they can be dragged to other screens	
190	The GUI shall provide access to all dispatch features	
191	The dispatch console shall provide rich media incident management support, giving the ability to share data such as video, Archived videos, Photos & Alarm monitoring.	
192	Ability to see a live map showing all the GPS coordinates of the mobile field user	
<b>Data Center Security &amp; Visibility</b>		
193	The solution should provide secure analytics which gives Complete visibility and contextual awareness of users, workloads and application behaviour. The analytics and forensics tool should detect Malicious activity and provide isolation of devices after the attack vector has been identified.	

S. No.	Functional Parameters/ Description	Compliance (Yes/No)
194	The solution should provide monitoring and display of each and every process, process ID, Process owner, Process mapping running on all virtual servers hosting applications., it should have the capability to detect suspicious behaviour based on process behaviour deviations and map this behaviour deviations instantaneously to malware execution patters	
195	The solution should provide accurate inventory of the installed software packages on the workloads to quickly identify any known vulnerabilities and exposures. It should then provide actions to quarantine or restrict communications based on vulnerabilities or vulnerability score.	
196	The solution should detect multiple forms of process behaviour deviations such as shellcode, raw socket creation, user Login suspicious behaviour, interesting File Access, file Access from a different user, unseen Command etc	
197	The solution should provide Micro Segmentation capability (application by port, application tier, workload) on application end host and should enforce unwanted communication between compute resources in application	
<b>Deployment Automation</b>		
198	The solution should provide application centric deployment automation platform that is premise agnostic, cloud-independent and portable model that defines each application's deployment and management requirements.	
199	The solution should provide automation capabilities of application modules of command and control center, it must include an application modeler through which administrator can open templates and model cloud agnostic application profile. It should also include a common library for OS images, application services, that can be used to model an application profile.	
200	The solution must provide visibility and show back for all the VM's that are not deployed through Cloud Portal. System must provide management actions like resize, snapshot, reboot, power on/off etc for existing VM's not deployed through the automation tool.	
<b>Workload Automation Tool</b>		
201	The solution should provide workload automation that provides full stack visibility and control:- resources aware, Application aware, Database aware	
202	The solution should Provide Accurate What/if Capacity Planning based on the real time understanding of resource requirements and should provide Visibility into cost & configuration of each workload	
<b>Application Performance Monitoring</b>		

S. No.	Functional Parameters/ Description	Compliance (Yes/No)
203	The solution should provide Quick and seamless resolution of application problems. It should Provide code level diagnostics (class & method-level visibility) of poorly performing application services and application errors & exceptions	
204	The solution should have single product and architecture to address Application Performance Management (end user experience monitoring, architecture discovery modelling and display, transaction profiling, deep-dive monitoring, analytics)	
205	The solution should provide an online virtual collaboration space, where remote IT Ops, Support, and Dev across can participate in a virtual "war room" session for analysis to be shared without having to export data from the UI. Users can share the exact views they are seeing to increase collaboration across groups.	
206	It should be able to provide end user monitoring which should include mobile and browser-based analytics including crash analytics, user tracing, usage and performance analytics basis versions, track user sessions flow & behaviour.	
207	The solution should have integrated and correlated monitoring data exchange between mobile, computing resources, providing a single pane of glass.	

### 5.2.2.2 Video-Wall Specifications

The network-based control room solution should consist IP enabled DLP based Video wall cubes. They should be able to show signals over IP without the need of separate decoders. Each of these Video wall cubes should be able to display up to 60 sources per display. It should be possible to show any of the input sources or all the input sources in any position on the wall, in any size and any configuration. The system should support automatic format detection for plug and play simplicity.

1. The OEM should be an established multinational in the field of video walls and should have at least 1000 DLP cube installations in India.
2. Only those OEM's would be considered who also manufacture the Projection/Optical engine as well apart from the whole cube. Companies claiming to be OEM's but not manufacturing their own Projection/Optical engines shall not be considered
3. Video-Wall size is **6.5 Meter (Width) X 2.5 Meter (Height)** for Temporary Locations as well as in permanent ICCC building.

#	Parameters	Minimum Specifications	Bidder Compliance (Yes/No)	Product Documentation Reference
1	Make	<to be provided by the bidder>		
2	Model	<to be provided by the bidder>		
3	Technology	DLP Based cube on video wall with base stand .The network-based control room solution should consist IP enabled DLP based Video wall cubes. They should be able to show signals over IP without the need of separate decoders. Each of these Video wall cubes should be able to display up to 60 sources per display		
4	Screen Size	(6.5 x2.5 Meter) Should fit into 6.5 Meter x 2.5 Meter wall size		
5	Cube & Controller	Cube & controller should be from the same manufacture		
6	Total Resolution	Minimum resolution of video wall 15000 x 6000		
7	Brightness uniformity	>98%		
8	Light Source Type	Shall be Laser light source technology. Light Source Shall be Individual cube should be equipped with multiple laser banks and each laser bank should have an array of diodes. Single or multiple diode failure should not impact image display on the screen.		
9	Brightness of Projection engine	Shall be minimum 2300 lumens		
10	Brightness of Cube	Shall be minimum 600 nits and should be adjustable for lower or even higher brightness requirements		
11	Dynamic Contrast	Shall be 1000000:1 or more		
12	Control	IP Based control should be provided		
13	Remote	IR remote control should be provided for quick access		
14	Screen to Screen Gap	0.2 mm (or less) @ temperatures between 20~25 Degrees C		
15	Screen Support	Screen should be minimum 3 layers with a Hard Backing to prevent bulging		

#	Parameters	Minimum Specifications	Bidder Compliance (Yes/No)	Product Documentation Reference
16	Control BD Input terminals	Input: 1 x Digital DVI, Input: 1 x HDMI, Input: 1 x Display Port, Input: 1 x analog Dsub-15,		
17	Power Supply	Dual Redundant and Hot Swappable Power Supply. This should be built inside the cube for fail safe operation. Power supplies extended or kept outside the cube are not acceptable		
18	Cooling Inside Cube	Shall be By Means of a sealed heat pipe or better technology		
19	Cube Depth	Total Cube depth including screen module should be less than 500 mm or lower		
20	Protocol	System should support industry standard network protocols: DHCP, UDP, TCP /IP		
21	Monitoring of critical parameters to ensure stable operation of the system 24 x 7	Internal Temperature Brightness Cooling Light Source Status Should be possible to demonstrate these parameters through an active monitoring interface		
22	Dust Protection	Critical component of Videowall cube (i.e. Projection engine) must follow Industry standard IEC / EN 60529 in designed to avoid the entry of dust to ensure longer life of system. System should be tested and certified by any 3rd party lab to confirm anti dust design.		
23	Operating Hours	24x7 Hours x365 Days continuous working.		
24	LED bezels size	Less than 6 mm		
25	OEM Criteria	<ul style="list-style-type: none"> <li>• OEM without any JV/ Distributor Should have their own registered office in India since Last 7 years.</li> <li>• OEM without any JV/ Distributor Should have their own service center in India since Last 7 years.</li> <li>• Video-wall should have MTBF of minimum 5 years .</li> </ul>		



### 5.2.2.3 Specifications of Video-Wall Controllers:

#	Parameters	Minimum Specifications	Bidder Compliance (Yes/No)	Product Documentation Reference
1	Make	<to be provided by the bidder>		
2	Model	<to be provided by the bidder>		
3	Input	DVI-I Connector with HDCP support		
4	Input Color Depth	Color Depth 8 bits per pixel		
5	Input Channels	Channels 1		
6	Output	HDMI 1.3 Support to loopback progressive VGA or HDMI input signal		
7	Output Channels	Channels 1		
8	Ethernet	Ethernet Gigabit 1000 BASE-T		
9	Interface	2x RJ-45, Redundant LAN port		
10	Protocols	Protocols DHCP, UDP, TCP/IP		
11	IP Address	IP Address Static IP address, Automatic IP address		
12	Power on Ethernet	Support POE		
13	KVM	Support IP KVM function		
14	MTBF	> 100,000 Hours		
15	Supported Resolutions	Minimum Up to 3840 x 2160 @ 60 Hz		
16	Power Requirement	100-240 VAC		
17	Operation Temperature	Minimum range 0-40 deg. C		

### 5.2.2.4 Specifications of Display Wall Management Software

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

#	Parameters	Minimum Specifications	Bidder Compliance (Yes/No)	Product Documentation Reference
3	Client & Server based Architecture	Wall management software should be based browser & Server based Architecture. User should be able to login the server with Internet Explorer. There should be no need to install any additional software on the control computer.		
4	Scaling and display	Should have function for static layout and automatic layout creation, editing, loading, and deleting. Any layout should be loaded in under 1 sec (irrespective of size of display & number of windows)		
5	Controls	Software should able to manage multiple displays simultaneously including status monitoring, video window control and properties setup. Software should able to preview video signals before opening window on display wall		
6		Should be able to control & monitor individual cube, multiple cubes and multiple video walls		
7	Layout Management	Operator should be able to preview the content of video/RGB signal by dragging the signal source into the signal preview window should be possible		
8	Support	The system software should support at least 5 RGB / Video signals preview at the same time.		
9	Scenarios	Software should support multiple users managing a display wall or more display walls at the same time.		
10	Framework	Video wall cube should be use Python-Django framework for monitoring the system		
11	Monitoring	Provide videowall status including Source, light source, temperature, fan and power information		
12	System Control	System should have a quick monitor area to access critical functions of the videowall		
13	Remote control	Should provide a virtual remote on the screen to control the video wall		

#	Parameters	Minimum Specifications	Bidder Compliance (Yes/No)	Product Documentation Reference
14	Scheduler	Input sources can be scheduled in "daily", "periodically" or "sequentially" mode per user convenience		

### 5.2.2.5 Specifications of Video-Wall Server

#	Parameters	Minimum Specifications	Bidder Compliance (Yes/No)	Product Documentation Reference
1	Make	<to be provided by the bidder>		
2	Model	<to be provided by the bidder>		
3	Type	Rack /Blade Type (Suitable for 42U Rack Installation)		
4	CPU	Quad Core, 3.40 GHz, 8M Cache, 80W) or above;		
5	Memory	8GB UDIMM, 2400MT/s, Single Rank, x8 Data Width or above;		
6	Network	1000-M LAN port*2		
7	OS	Windows Server 2008/2012/2016 (64 bits		
8	HDD	240GB SSD SATA Mix Use 6Gbps 512n 2.5in Hot-plug Drive or above;		
9	Others	A. System should also be capable of decoding 50 Full HD streams @30fps and displaying these on the screen simultaneously B. System should also be capable to show high resolution graphic of at least 19000 x 6000 resolution on the screen through this controller system		

### 5.2.3 Workstation with Joystick Controller

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

#	Parameters	Minimum Specifications	Bidder Compliance (Yes/No)	Product Documentation Reference
2	Model	<to be provided by the bidder>		
3	Processor	Latest generation 64-bit x86 Dual core CPU with 3.33GHz or more		
4	Memory	Minimum 8 GB Memory		
5	Graphics card	Graphics card with 2 GB video memory (non shared)		
6	HDD	6 TB - Minimum 3 x 2 TB SATA 7200 RPM		
7	Media Drive	NO CD / DVD Drive		
8	Network interface	1000BaseT, Gigabit Ethernet (10/100/1G auto sensing)		
9	Audio	Line/Mic IN, Line-out/Spr Out (3.5 mm)		
10	USB ports	Minimum 6 USB ports (out of that 2 in front). These would be disabled for data transfer.		
11	Keyboard	104 keys minimum OEM keyboard		
12	Mouse	2 button optical scroll mouse (USB)		
13	PTZ joystick controller	• PTZ speed dome control for IP cameras		
		• Minimum 10 programmable buttons		
		• Multi-camera operations		
		• Compatible with all the camera models offered in the solution		
		• Compatible with VMS /Monitoring software offered		
14	Monitor	22" TFT LCD monitor, Minimum 1920 x1080 resolution, 5 ms or better response time, TCO 03 (or higher) certified		
		• For command Control Centres: 3 LCD Monitors		
		• For Viewing Centres: 1 LCD Monitor		
15	Operating System	64-bit pre-loaded OS with recovery disc		
16	Anti-virus feature	Advanced antivirus, antispymware, 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)		

## 5.2.4 Desktop PC for ICCC

#	Item Name	Minimum Specifications	Bidder Compliance (Y/N)	Product Doc. Reference
1	Processor	Latest Generation (x86 architecture with 65W TDP or lower) minimum 6 dedicated CPU cores , 4.00 GHz or higher maximum clock frequency and minimum 8 MB L3 cache or higher .Processor should have been launched in Q4'17 or later by Processor Manufacturer.		
2	Chipset	Latest Generation business class Chipset compatible with the above processor.		
3	Motherboard	Motherboard make from the same Desktop OEM (OEM logo must be embossed in the motherboard)		
4	Memory	Minimum 8 GB with support for expansion up to 32 GB or higher.		
5	RAM Type	DDR4 with 2666 MHz or higher.		
6	DIMMs & Expansion Slots	2 DIMM slots or higher (At 2 PCIe series expansion slots ).		
7	Hard Disk Controller	Serial ATA - III with minimum 7200 RPM (Integrated On-Board Hard Disk Controller supporting Serial ATA Interfaces).		
8	Hard Disk Capacity	At least one single disk of Min 1 TB with 7200 rpm or higher.		
9	Graphics	Integrated Graphics (UHD / 4K).		
10	Network	10/100/1000 on-board integrated Network Port.		
11	USB / HDMI / VGA Ports	Integrated USB Port: Minimum 8 no's (Min 4 no's of 3.1 Gen-1), out of 8 Nos minimum 4 in front, 4 in back and should be easily accessible.		
		Integrated VGA / Display Port : Minimum 1 no; Should be easily accessible.		
12	Audio	Integrated Audio controller with Internal speaker		
13	Cabinet	Tool less Small form Factor chassis with 8 liters or lesser in volume		
14	SMPS	Minimum 200 W or above. Should be capable of supporting fully configured PC.		

#	Item Name	Minimum Specifications	Bidder Compliance (Y/N)	Product Doc. Reference
15	Operating system + SW	Windows 10-Professional 64 Bit to be preloaded with latest build. + MS Office 2016		
18	Security	Hardware based TPM 2.0, chassis Intrusion switch / Intrusion Sensor with chassis physical security cable lock slot.		
19	Monitor / Display	Monitor with LED Backlight with minimum Screen size: 18.5" or higher, Resolution 1366 x 768 should have at least one VGA / Display port and one HDMI port.		
20	OEM	CPU & Monitor must be of same OEM make.		
21	Keyboard	USB Business Keyboard (Same Desktop OEM Make)		
22	Mouse	USB Business Mouse (Same Desktop OEM Make)		
23	Locking Arrangement	Provision for lock the cabinet.		
24	Production Unit, Certification and Compliance	Windows 10 Pro Certification for the quoted desktop model		
		EPEAT Gold India for the quoted desktop model		
		ROHS for the quoted desktop model.		
		Minimum Energy Star 5.0 & TCO Certification for Monitors and quoted Desktop model		
		ISO 9001 and 14001 Certified India Unit (Proof of Certification of India unit to be submitted).		
25	Warranty	5 years onsite comprehensive OEM warranty (OEM supplied model warranty must be visible in the website in respect to each product serial number)		

### 5.2.5 Structured Cabling

#	Parameters	Minimum Specifications	Bidder Compliance (Yes/No)	Product Documentation Reference
---	------------	------------------------	----------------------------	---------------------------------

#	Parameters	Minimum Specifications	Bidder Compliance (Yes/No)	Product Documentation Reference
1	Make	<to be provided by the bidder>		
2	Model	<to be provided by the bidder>		
3	Standards	ANSI TIA 568 C for all structured cabling components		
4	OEM Warranty	OEM Certification and Warranty of 15-20 years as per OEM standards		
5	Certification	UL Listed and Verified		
		Bidders may visit SDC site for getting a clear picture of the exact requirement		

### 5.2.6 Electrical Cabling Components

#	Parameters	Minimum Specifications	Bidder Compliance (Yes/No)	Product Documentation Reference
1	Make	<to be provided by the bidder>		
2	Model	<to be provided by the bidder>		
3	Standards	All electrical components shall be design manufactured and tested in accordance with relevant Indian standards IEC's		

### 5.2.7 Unified Threat Management System (UTM)

SI shall provide UTM system for internet browsing at ICCC for the 50 concurrent users.

#	Parameters	Minimum Specifications	Bidder Compliance (Yes/No)	Product Documentation Reference
1	Make	<to be provided by the bidder>		
2	Model	<to be provided by the bidder>		
3	NGFW throughput (with IPS + App Ctrl +WebFilter license enabled)	1 Gbps		

#	Parameters	Minimum Specifications	Bidder Compliance (Yes/No)	Product Documentation Reference
4	New connections/sec	25000		
5	Maximum licensed users	No user based license		
6	Storage	integrated SSD/HDD for log storage		
7	Ethernet interfaces	2x1Gbps SFP and 4x1Gbps RJ45		
8	I/O ports	1xConsole and Dedicated Management Port		
9	Power supply	Redundant 230V AC		
10	Mounting	Rack Mounting Kit		
11	OEM Warranty and Support with IPS + App Ctrl +WebFilter License	for 5 years with advance hardware replacement warranty		

### 5.2.8 Internet Switch (L-3)

SI shall provide Internet Switch (L-3) at ICCC for the internet browsing.

#	Parameters	Minimum Specifications	Bidder Compliance (Yes/No)	Product Documentation Reference
1	Make	<to be provided by the bidder>		
2	Model	<to be provided by the bidder>		
3	Routing Throughput	Line Rate		
4	Number of interfaces	48x10/100/1000 Mbps RJ45 ports 2xSFP Ports (dedicated)		
5	Switching Protocol	RSTP, MST, LACP		
6	Routing Protocol	Static Routing (IPv4 and IPv6)		
7	VLAN	1096 VIDs		
8	I/O ports	1xConsole/Dedicated Management Port		
9	Power supply	230V AC PSU		
10	Mounting	Rack Mounting Kit		



#	Parameters	Minimum Specifications	Bidder Compliance (Yes/No)	Product Documentation Reference
11	OEM Warranty and Support	for 5 years		

### 5.2.9 Internet Lease Line (ILL)

A dedicated Internet Lease Line (ILL) shall be provided at ICCC locations with 1:1 contention ratio and unshared bandwidth on dual protection path of 50 Mbps speed.

### 5.2.10 Helpdesk

SI shall provide the operational support for all the locations, through a suitable helpdesk system, to ensure that the solution is functioning as intended and that all problems associated with operation are resolved satisfactorily during the contract period. The SI shall provide a web enabled helpdesk management system with SMS and email based alert system for the Helpdesk Call management and SLA reporting. SI shall be required to setup a centralized helpdesk at two locations i.e. one at Command Control Center specifically for City Surveillance, and one at City Operation Center for rest of the solutions.

SI shall provision for the infrastructure necessary for managing the Help Desk including rent charges for Toll-free telephone line(s) at the Help Desk location. SI shall provide multiple channels to log a complaint such as Toll-free lines, landlines, helpdesk tool, E-mail, direct walk-in etc. Outage of any component shall be calculated as a time between logging the call and closing the call.

A helpdesk is envisaged to be provided for the resolution of technical queries by internal users. Typical helpdesk activities (indicative) shall include, but not limited to:

1. Deployment of sufficient manpower to attend the helpdesk requests for extending technical support on hardware, network, application etc. to users
2. Deployment of web-based tool for the helpdesk
3. Provide Help Desk facility for agreed SLAs for reporting technical incidents / issues / problems with the system. Help desk facility shall be provided through Toll-free lines, landlines, helpdesk tool, E-mail, direct walk-in etc.
4. Implement a call logging system in line with the severity levels as per the SLAs. The Help desk shall log user calls related to system and assign an incident/ call ID number. Severity shall be assigned to each call as per the SLAs.
5. Track each incident / call to resolution.
6. Escalate the calls, to the appropriate levels, if necessary, as per the escalation matrix agreed upon with Authority/authorized entity

7. Analyze the incident / call statistics and provide monthly reports including but not limited to:
  - i. Type of incidents / calls logged
  - ii. Incidents / calls resolved
  - iii. Incidents / calls open
8. Helpdesk Solution shall further have the capability to upload frequently asked questions and solutions.

Helpdesk becomes the central collection point for service staff contact and control of the problem, change, and service management processes. This includes both incident management and service request management. This shall be the first level of support (L1).

It is also expected that a second level of centralized support (L2) shall also be maintained at the same location from where the various zones/wards can be serviced in case of problem escalation. If a problem is not resolved by telephone/help desk tool and the User declares the problem to be of an emergency nature, SI shall dispatch a Field Service Staff member who shall provide On-site Support Service according to service levels given.

The Helpdesk shall act as a single point of contact for all users whether for service requests, incidents or problems. It shall encompass Helpdesk, Asset Management and Vendor Management. In addition, it shall offer a focused approach for delivering integrated Service Management and provide an interface for other functions in IT Services Continuity Management like Maintenance Contracts, Software Licenses etc.

SI shall implement effective Helpdesk Management procedures to leverage the knowledge gained in providing faster and better solutions, create knowledge bases and prevent recurrence of problems.

**i. Helpdesk Capacity**

SI is required to provide a minimum 10-seater helpdesk at Command Control Center during all operation hours as specified in the RFP. However, if the SI believes that in order to meet the SLAs, additional capacity is required, the same may be provided by the SI. It is also to be noted any supervisors required for the Helpdesk Operators shall be over and above the minimum operators mentioned above.

**ii. Shift Timings**

The SI shall operate the Central Helpdesk for the entire tenure of the Contract as follows:

Category	Shift	Type of Helpdesk Support	Type of Field Support
Helpdesk at Control	Shift 1	On-premise	On-call

<b>Command Center</b>	Shift 2	On-premise	On-call
	Shift 3 (night shift)	On-premise	On-call
<b>Helpdesk at City Operation Center</b>	Shift 1	On-premise	On-call
	Shift 2	On-premise	On-call
	Shift 3 (night shift)	On-Premises	On-call

### iii. Helpdesk Operators

The SI is required to provide Operators at Helpdesk for operating and managing the Helpdesk as specified in this RFP. The Operators shall perform various activities including:

Understanding the query/issue in the reported request. Query could be related to the following:

- a) hardware including issues related to desktop/laptop, printer/multi-function device, local server, routers/switches
- b) application including login and password issues, accessing a module, navigation assistance, report generation assistance
- c) network including internet/intranet and end-user device connectivity

Providing information / clarification on the spot in case of an informational query or providing necessary troubleshooting assistance in case of a logged issue

In case of technical issues for which a resolution is not possible instantly, the operator shall submit the request into the system for escalation and further action by the SI's team

Process all service requests, dispatch them to field personnel who shall perform the follow up

### iii. Field Support Staff

The SI is required to provide Field Support Staff for undertaking all activities on field to complete a call logged by a User. SI is expected to deploy enough number of Field Support Staff to ensure that SLAs as specified in the RFP are met.

### iv. IT / Non-IT Infrastructure and application software for Helpdesk

The SI shall be responsible for procurement, installation, commissioning and operations & maintenance of helpdesk including supply & installation of IT / Non-IT infrastructure along with necessary application software (as per indicative BOM) required for the smooth functioning of the Central Helpdesk at both the location

## 5.2.11 Technical Specification of ICT Components & Accessories at ICCC

### 5.2.11.1 IP Phones for ICCC

Parameter	Minimum Requirements	Compliance
Display	2 line or more, Colour display for viewing features like messages, directory, Video	
Integral switch	10/100 mbps for a direct connection to a 10/100 BASE-T Ethernet network through an RJ45 interface	
Speaker Phone	Yes	
Headset	Wired, Cushion Padded Dual Ear-Speaker, Noise Cancelling headset with mouthpiece microphone, port compatibility with IP Phone	
VoIP Protocol	SIP V2 VoIP supported	
POE	IEEE 802.3af or better and AC Power Adapter (Option)	
Supported Protocols	SNMP, DHCP, DNS	
Codecs	G.711, G.722, G.729	
Speaker Phone	Full duplex speakerphone with echo cancellation Speaker on/off button, microphone mute	
Volume control	Easy decibel level adjustment for speaker phone, handset and ringer	
Phonebook/ Address book	Minimum 100 contacts	
Call Logs	Access to missed, received, and placed calls. (Minimum 20 overall)	
Clock	Time and Date on display	
Ringer	Selectable Ringer tone	
QoS	QoS mechanism through 802.1p/q	

### 5.2.11.2 IP PABX and Communication System with Contact Center Solution

S.N.	Minimum Requirements	Compliance
------	----------------------	------------

S.N.	Minimum Requirements	Compliance
1.	The contact centre solution shall include VoIP based EPBAX, IVRS, Automatic Call Distribution (ACD), Voice Logger Server. Using the contact centre solution, citizens can contact city administrator through the emergency communications system or through the contact center helpline number including Dial 100/112.	
2.	Solution should be designed and implemented for up to 50 agents	
3.	IVRS should be modular and scalable in nature for easy expansion without requiring any change in the software.	
4.	The contact center solution should be able to route voice/ VOIP calls from centralized Interactive Voice Response System (IVRS) to respective call center (s).	
5.	The callers should be able to access the various services through state-of-art centralized integrated Interactive Voice Response System (IVRS).	
6.	IVRS should support various means of Alarm indications in case of system failures, e.g. Functional error, missing voice message prompt, etc., and shall generate error Logs. SI has to identify other required services from IVR solution.	
7.	IVRS shall be able to get information /text/data from databases, convert to voice, and speaks it back to the caller in relevant/desired language, including English and Hindi both	
8.	<p>Solution should provide pre-integration with industry standard IVRS servers and enhance routing &amp; screen pop by passing forward the information. Interactive Voice Response System (IVRS) should -</p> <ol style="list-style-type: none"> <li>1. play welcome messages to callers Prompts to press and collect DTMF digits</li> <li>2. be able to integrate with backend database for self-service, as and when required</li> <li>3. Offer GUI based tool to be provided for designing the IVR and ACD call flow.</li> <li>4. support Voice XML for ASR, TTS, and DTMF call flows</li> <li>5. be able to Read data from HTTP and XML Pages be able to run outbound campaigns</li> </ol>	
9.	<p>Automatic call distribution (ACD) solution should -</p> <ol style="list-style-type: none"> <li>1. be able to route the call to any remote call center agent using IP phones</li> <li>2. have an ability to queue or hold the call for an agent if none</li> </ol>	

S.N.	Minimum Requirements	Compliance
	<p>is immediately available</p> <ol style="list-style-type: none"> <li>3. have an ability to keep the callers informed as to the status of the call and providing information to callers while they wait in queue</li> <li>4. be able to perform prioritized call routing</li> <li>5. support skill-based routing and it should be possible to put all the agents into a single skill group and different skill groups</li> <li>6. Support routing of incoming calls based upon caller input to menus, real-time queue statistics, time of day, day of week, ANI, dialed number etc.</li> <li>7. support call routing based on longest available agent, circular agent selection algorithms</li> <li>8. Maintain log of all services offered which can be used for audit and analysis purpose.</li> <li>9. support the playing of customizable queuing announcements based upon the skill group that the call is being queued to, including announcements related to position in queue and expected delay</li> <li>10. allow agents to chat with other Agents or supervisor from the Agent desktop software</li> <li>11. allow supervisor to see the real-time status of agents, supervisors should be able to make agent ready or logout from the supervisor desktop</li> <li>12. support Queuing of calls and playing different prompts depending on the type of call and</li> <li>13. time in the queue</li> </ol>	
10.	System shall provide for 100% recording of calls using a call logger. The recording shall contain detailed call information and the solution must provide advanced searching capabilities.	
11.	Solution should have automatic identification of incoming number based on landline and mobile number mapping. The recording shall be secure with AES 256-bit encryption. The system shall have maker checker profile with MD5 fingerprinting.	
12.	Solution should support call recording mapped to incident tickets	

S.N.	Minimum Requirements	Compliance
13.	Solution should offer customizable agent and supervisor desktop layout	
14.	Solution should offer Inbound and outbound capability	
15.	Solution should provide facilities for outbound calling list management, and software based predictive or preview dialing	
16.	<p>The agent's desktop shall have an application which shall fulfil the following functionalities:</p> <ul style="list-style-type: none"> <li>● It should provide consistent agent interface across multiple media types like fax, SMS, telephone, email, and web call back. The agent's desktop should have a "soft-phone" – an application that enables standard telephony functions through a GUI.</li> <li>● It should provide the agents with a help-desk functionality to guide the agents to answer a specific query intelligently.</li> <li>● It should also provide an easy access to agents to previous similar query which was answered successfully.</li> <li>● It should also be possible to identify a request to be a similar request made earlier.</li> <li>● It should be possible for agents to mark a query as complex/typical and put in to database for future reference by other agents.</li> <li>● It should be possible for agents to escalate the query.</li> </ul>	
17.	System should be able to integrate with email / SMS gateway so that appropriate messages can be sent to the relevant stakeholders after the interaction and any updates thereon.	
18.	Should intelligently and automatically responds to email inquiries or routes inquires with skills-based routing discipline to agents	
19.	Live data reporting gadgets	
20.	Multiline support	
21.	Speed dial in IP phones	
22.	<p>Solution should provide CTI services such as:</p> <ul style="list-style-type: none"> <li>● CTI link should allow a computer application to acquire control of the agent resources on the IP EPABX &amp; change state of the agent phone through commands on the CTI link.</li> <li>● CTI link should pass events &amp; information of agent states &amp; changes in agent states as well as incoming calls to the computer applications.</li> </ul>	

S.N.	Minimum Requirements	Compliance
	<ul style="list-style-type: none"> <li>● CTI link should allow a computer application to take control of the call flow inside the IP EPABX &amp; also allow the computer application to decide the most suitable action / agent for an incoming call.</li> <li>● automatic display (screen pop) of information concerning a user/customer on the call agent</li> <li>● screen prior to taking the call based on ANI, DNIS or IVR data</li> <li>● Synchronized transfer of the data and the call to the call centre agent</li> <li>● Transfer of data corresponding to any query raised by any agent regarding a query raised by <ul style="list-style-type: none"> <li>○ a caller whose call is being attended by the agent</li> <li>○ Call routing facilities such as business rule-based routing, skills-based routing etc.</li> </ul> </li> </ul>	
23.	<p>Supervisor Module - The call center should provide a graphical console application program for the supervisor's workstation. This position shall facilitate the following features: -</p> <ol style="list-style-type: none"> <li>1. Any supervisor shall be able to monitor or control any group in the call Centre</li> <li>2. It shall show the live activity of each agent in details as well as in a summarized fashion including information like total number of calls received, calls answered, average response time etc.</li> <li>3. Supervisor console shall also graphically display live status of the call session summary, number of calls waiting in the queue, call traffic etc.</li> <li>4. Live status of the group shall be shown, including waiting calls and calls being answered currently.</li> <li>5. Access to the supervisor console shall be restricted.</li> <li>6. It shall be possible for a supervisor to attend calls whenever necessary.</li> </ol>	
24.	Reporting:	



S.N.	Minimum Requirements	Compliance
	<ol style="list-style-type: none"> <li>1. System to provide report of IVR Application Performance Analysis, Call by Call details for all the calls, Traffic analysis reports etc.</li> <li>2. Reporting platform to support Agent level reports, Agent login, logout report, report on agent state changes</li> <li>3. Queue reports abandon call reports all the reports should be summary, tabular and detailed report format to be available for the agents.</li> <li>4. Reporting platform to support custom reports using a combination of the Crystal Reports Developer's Toolkit and SQL stored procedures.</li> <li>5. Users of the Historical Reports should be able to perform the following functions View, print, and save reports. Sort and filter reports Send scheduled reports to a file or to a</li> <li>6. printer. Export reports in a variety of formats, including PDF, RTF, XML, and CSV.</li> </ol>	
25.	<p>Solution should offer audit trail with the following features -</p> <ol style="list-style-type: none"> <li>1. Solution should have a comprehensive audit trail detailing every user activity including system/security administrators with before and after image</li> <li>2. Audit trails presented by the system shall be very detailed with all the related fields, such as User ID, time log, changes made before and after, Machines ID etc.</li> <li>3. It shall have the facility to generate security report(s) and audit the whole process from logs reports at any future date. The system shall have complete audit trail of any changes to the system e.g. alert generated, system configuration etc.</li> <li>4. System shall not allow audit log to be deleted and any attempts to delete must be logged.</li> <li>5. System shall have at a minimum following standard report: <ol style="list-style-type: none"> <li>a. List of users, user privileges and status</li> <li>b. User sign-off and sign-on</li> <li>c. User violation – unsuccessful login attempts</li> </ol> </li> </ol>	

S.N.	Minimum Requirements	Compliance
	d. User additions, amendments and deletions with before & after image	

#### 5.2.11.3 Printer at ICCC

S. N	Parameter	Minimum Requirements	Compliance
1	Printer Type	Laser	
2	Functionality	All-in-One (Print, Scan, Copy)	
3	Printer Output	Colour	
4	Connectivity	USB/Ethernet	
5	Pages per minute	24 pages	
6	Page size supported	A4, Letter, Executive, Legal, Folio; Duplex Print - Auto; Max Print resolution - 1200 x 1200 dpi	
7	Supported OS	Windows and Mac	
8	Scan Resolution	Up to 300 dpi	

#### 5.2.11.4 Access Control System for ICCC

#	Parameter	Minimum Specification	Compliance
1	Credential Support	Finger print, Card, PIN	
2	User Capacity	Minimum 1000	
3	Template Storage Capacity	Minimum 9999	
4	Communication	Ethernet	
5	Features	Attendance, Door Access Control	

#	Parameter	Minimum Specification	Compliance
6	Supported Card	EM Prox, Mifare, and HID iCLASS	
7	Reader Interface	RS-232 and Wiegand	
8	Certification	CE, FCC PART 15B(VOC), BIS, ROHS	
9	Event Buffer	50,000	

#### **5.2.11.5 Fire Detection and Suppression System - ICCC**

The facility shall be equipped with adequate and advanced Fire Detection and Suppression system. The system shall raise an alarm in the event of smoke detection. The system shall have proper signage, response indicators and hooters in case of an emergency. The system shall be based as per NFPA standards.

As ICCC is on temporary location and we need only Fire Detection Alarm System.

#### **5.2.11.6 Access control system - ICCC**

The Biometric/Access card-based Access Control System shall be deployed with the objective of allowing entry and exit to and from the premises to authorized personnel only with appropriate door locks and controller assemble connected with BMS system. The system deployed shall be based on proximity as well as biometric technology for critical areas and proximity technology for non-critical areas.

#### **5.2.11.7 CCTV system - ICCC**

The SI shall provide CCTV system within the Integrated Command and Control Center on 24X7 bases. All important areas of the Integrated Command and Control Center along with the non-critical areas like locations for DG sets, entry exit of Command Center, Entry and Exit of building premises need to be under constant video surveillance. Monitoring cameras shall be installed strategically to cover all the critical areas of all the respective locations.

#### **5.2.11.8 Water leak detection system - ICCC**

The Water Leak Detection System 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 alarm module. The cable shall be installed in the ceiling and floor areas around the periphery.

### 5.2.12 UPS 50 KVA at ICC

#	Parameter	Specification	Compliance
1	Capacity	50 KVA - modular UPS with external Isolation Trans-former and 60 Mins Power Backup.	
2	Input Voltage (V)	380/400/415 V (Three-phase + Neutral)	
3	Frequency (Hz)	45 – 65 Hz	
4	Input Power Factor	Up to 0.99	
5	THDI	4% for 15-40 kVA or better	
6	Nominal Output Voltage (V)	380/400/415 V	
7	Overload Capacity in Normal Operation	110 %: for 10 Minutes 130% - 150%: One minute	
8	Output Voltage Tolerance	+/-1.5% static	
9	Battery	Sealed Maintenance Free batteries with 1hour backup with full load	
10	Battery Racks	To be sized to adequate dimension	
11	Accessories	Copper Interlink connector and Battery isolators	
12	SNMP Support	Should have IP based SNMP feature from day-1.	
13	Parallel Connectivity	UPS should work with redundant mode	
14	Quality Standard Compliance	Quality: ISO 9001, ISO 14001, OHSAS 18001, Safety: IEC 62040-1 EMC: IEC 62040-2, Performance: IEC 62040-3 Environment: RoHS	

#	Parameter	Specification	Compliance
15	OEM Criteria	UPS OEM should have their own engineer with service centre with adequate stock of spares at Guwahati for providing 24 x 7 x 365 On-site support.	

### 5.2.13 KVM Switches

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

### 5.2.14 Structured Cabling

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

#	Parameters	Minimum Specifications	Bidder Compliance (Yes/No)	Product Documentation Reference
2	Model	<to be provided by the bidder>		
3	Standards	ANSI TIA 568 C for all structured cabling components		
4	OEM Warranty	OEM Certification and Warranty of 15-20 years as per OEM standards		
5	Certification	UL Listed and Verified		
		Bidders may visit SDC site for getting a clear picture of the exact requirement		

### 5.2.15 Electrical Cabling Components

#	Parameters	Minimum Specifications	Bidder Compliance (Yes/No)	Product Documentation Reference
1	Make	<to be provided by the bidder>		
2	Model	<to be provided by the bidder>		
3	Standards	All electrical components shall be design manufactured and tested in accordance with relevant Indian standards IEC's		

### 5.2.16 Diesel Generator Set (DG) 75 KVA - ICC

#	Parameter	Minimum Specification	Compliance
1.	General	Auto Starting DG Set Mounted on a common based frame with AVM (Anti-Vibration) pads, residential silencer with exhaust piping, complete conforming to ISO 8528 specifications and CPCB certified for emissions. KVA rating as per the requirement.	
2.	Capacity	75 KVA	
3.	Fuel	High Speed Diesel (HSD) With 100Ltr. Tank Capacity or better. It should be sufficient and suitable for containing fuel for 12 hours	

#	Parameter	Minimum Specification	Compliance
		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 strokes 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.	Acoustic Enclosure	The DG set shall be provided with acoustic enclosure / canopy to reduce the sound level and to house the entire DG set (Engine & Alternator set) assembly outside (open-air). The enclosure shall be weather resistant powder coated, with insulation designed to meet latest MOEF/CPCB norms for DG sets, capable to withstand local climate. The enclosure shall have ventilation system, doors for easy access for maintenance, secure locking arrangement.	
8.	Output Frequency		

#### 5.2.16.1 DG Set General Requirements

- a) The equipment shall be complete with all necessary accessories and components as required as per IS standard for trouble free installation & operation.
- b) The generator shall have output rating enough to evacuate the output of the engine at rated power factor over complete range of site ambient conditions.

- c) The DG set shall be supplied with acoustic enclosure conforming to relevant standards.
- d) The generator shall be capable of satisfactory continuous operation at rated kVA and power factor at any voltage from 90% to 110% and within a frequency range of 47.5 Hz to 52.5 Hz.
- e) The generator shall have overload capacity as per applicable standards. The generator shall be capable of withstanding a three-phase short circuit at generator terminals when operating at rated kVA and power factor, 5% over voltage and with fixed excitation for 3 seconds.
- f) In DG, 4-point earthing system are to be considered out of which 2 points are for body earthing with GI strip and 2 point is for alternator neutral earthing with Copper strip.
- g) DG sets up to 1000 KVA capacity are required to be supplied with acoustic enclosure as per CPCB norms. DG Set with acoustic enclosure shall preferably be installed outside the building (including terrace subject to structural feasibility) & location should be finalized in consultation with the Architect. However, DG set should be as near to the substation as possible i.e. as near to Essential LT Panel as possible. Associated AMF panel of the DG Set can be located inside the acoustic enclosure or outside the acoustic enclosure as per manufacturer standard. In case, AMF has to be installed outside the acoustic enclosure, location of room to house AMF should be decided in consultation with the Architect so that it shall be as near to the acoustic enclosure as possible. Specially, in case of connection through bus trunking, care should be taken for aesthetics.

#### **5.2.16.2 DG Set Engine**

- a) The engine shall be of standard design of the original manufacturers. It should be 4 stroke cycles, water cooled, naturally aspirated/ turbo charged (as per manufacturer standard), diesel engine developing suitable BHP for giving a power rating as per ISO 8528- Part-1 in KVA at the load terminals of alternator at 1500 rpm at actual site conditions.
- b) The engine shall be capable for delivering specified Prime Power rating at variable loads for PF of 0.8 lag with 10% overload available in excess of specified output for one hour in every 12 hours. The average load factor of the engine over period of 24 hours shall be 0.85 (85%) for prime power output.
- c) The engine shall conform to IS: 10000/ ISO 3046/ BS:649/ BS 5514 amended up to date.
- d) Necessary certificate indicating the compliance of the above capacity requirement for the engine model so selected along with compliance of Noise and Emission norms as per latest CPCB guidelines for DG set capacity up to 1000 KVA, should be furnished from the manufacturers along with the technical bid. However above 1000 KVA DG set, manufacturers shall furnish certificate that the Engine for the DG set complies with the CPCB Emission norms.



- e) The engine shall be fitted with following accessories subject to the design of the manufacturer:
  - I. Dynamically balanced Fly wheel.
  - II. Necessary flexible coupling and guard for alternator and engine (applicable only for double bearing alternator).
  - III. Air cleaner (dry/ oil bath type) as per manufacturer standard.
  - IV. A mechanical/ electronic governor to maintain engine speed at all conditions of load.
- f) Daily fuel service tank of minimum capacity as per Table below, fabricated from M.S. sheet with inlet, outlet connections air vent tap, drain plug and level indicator (gauge) M.S. fuel piping from tank to engine with valves, unions, reducers, flexible hose connection and floor mounting pedestals, twin fuel filters and fuel injectors. The location of the tank shall depend on standard manufacturers design.

### **5.2.16.3 AMF Panel, Battery & Electrical System for DG**

#### **A. Battery/ Electrical System**

- a) Batteries supplied with Genset are generally dry and uncharged. First charging of uncharged batteries is very important and should be done from authorized battery charging centre. Initial charging should be done for 72-80 hours.
- b) Batteries should be placed on stands and relatively at cool place.
- c) Battery capacity and copper cable sizes for various engine capacity are recommended as indicated in the table below. Cable sizes shown are for maximum length of 2 m. If length is more, cable size should be selected in
- d) Battery capacity and copper cable sizes for various engine capacity are recommended as indicated in the table below. Cable sizes shown are for maximum length of 2 m. If length is more, cable size should be selected in such a way that voltage drop does not exceed 2 V. However, capacity as recommended by manufacturer may be taken.
- e) For AMF applications, a static battery charger working on mains supply is always recommended to keep the batteries charged.
- f) 1.5 sq.mm copper wire should be used for wiring between junction box and Control Panel.

#### **B. Cabling**

- a) Power cabling between alternator and control panel and control panel and change over switch to mains should be done with recommended cable sizes.
- b) Overheating due to loosen thumbing / undersize cables causes most of electrical failures, hence correct size of cable and thimbles should always be used, if cable is specified.

- c) While terminating cables, avoid any tension on the bolts/ busbars (if cable is specified). While terminating R, Y& B phase notations should be maintained in the alternator and control panel for easy maintenance.
- d) Crimped cables should be connected to alternator and control panel through cable glands, if cable is specified.
- e) Multi-core copper cables should be used for inter connecting the engine controls with the switchgear and other equipment.
- f) For AMF application, multicore 1.5 sq.mm flexible stranded copper cable for control cabling should be used.
- g) It is recommended to support output cables on separate structure on ground so that weight of cables should not fall on alternator/ base rail.
- h) External wirings, when provided for remote voltage / excitation monitoring/ droop CT etc. shall be screened sheathed type. Maximum length of such wiring shall not exceed 5 meters.

**C. Alternator Termination Links**

- a) For proper terminations between links and switchgear terminals, the contact area must be adequate. The following situations should also be avoided as they lead to creation of heat sources at the point of termination:
  - b) Point contact arising out of improper position of links with switchgear terminals.
  - c) Gaps between busbars / links and terminals being remedied by connecting bolt/stud. In such cases the bolt will carry the load current. Normally these bolts / studs are made of MS and hence are not designed to carry currents.
  - d) Adequate clearance between busbars / links at terminals should be maintained (IS 4232 may be referred to for guidelines).
  - e) Improper termination will lead to local heat generation which may lead to failure.

**5.2.17 Electrical work for Data Center & ICC**

The electrical cabling work shall include the following:

- h) Main electrical panel in ICC
- i) Power cabling
- j) UPS distribution board
- k) UPS point wiring
- l) Power cabling for utility component and utility points etc.
- m) Online UPS
- n) Separate Earth pits for the component
- o) The SI shall use fire retardant cables of rated capacity exceeding the power requirements of existing and proposed components to be used at maximum capacity.
- p) All materials to conform to IS standards as per industry practice

## 5.2.18 General: Post implementation requirements:

### 5.2.18.1 Quality Assurance plan

The Quality Assurance Management process will be implemented in a structured and professional manner throughout various stages of the Project. It is intrinsically linked with the provision of safe and reliable systems since the application and control of applicable processes is the fundamental mitigation against systematic error. Achievement of ISO 9000 is the most common metric available to companies and an ISO 9001 compliant design methodology provides a high level of confidence that Quality Management is adequately implemented

### 5.2.18.2 System configuration management:

- a) The system configuration management activity shall be carried out by the SI and will comply with the principles depicted in the System Configuration Management Plan.
- b) The SI shall produce a System Configuration Management Plan to cover change control that occurs during the development phases and at the same time monitor the system configuration.
- c) The System Configuration Management Plan shall address the configuration management in terms of configuration, change control, problem reporting, media control and appropriate configuration management tools.
- d) Reliability Critical Items list should be made. Critical items are defined as System/Subsystem/Component, failures, which result into the highest disruption to service when ranked with other equipment in any system. This ranking will be based on the RAM (reliability, accessibility and manageability) analyses. Ranking severity will be considered for the number of instances, which would delay a service, due to the failure of the equipment. The length of the delay in any smart city schedule and the time taken to fix the failure would affect the criticality. The criticality of the item will also be based on the effect of that single item on the entire system.
- e) The assessments include Failure Mode, Effects and Criticality Analysis (FMECA), Interface Hazard Analysis, Quantified Risk Analysis and quantitative analyses. It is recommended that the quantitative analyses be performed using Event Tree Analysis, Fault Tree Analysis or availability simulation modeling.

Class	Types of failures and incidents	Definitions
4	Significant	The failure leads to an incident that requires evacuation or immediate attn. to people, while restoration of the operation could take a long time, or lead to a delay greater than 30 min.
3	Major	The failure leads to a disturbance of the operation with a significant loss of missions degrading regularity and "offered service". A delay greater or equal to 3 min but less than 30 min

		is suffered.
2	Minor	The failure leads to a disturbance of the operation with a delay. A delay greater or equal to 1 min but less than 3 min is suffered.
1	Negligible	The failure has no immediate consequence on the pursuit of the missions but may lead to an intervention in corrective maintenance.

### 5.2.18.3 Electrical Distribution System

- a) The SI contractor shall coordinate with City Electric Power Distribution authority for power supply arrangements to remote sensors/ field devices of different systems.
- b) UPS system with battery bank for critical loads.
- c) Connection between UPS system and the network switch racks shall be redundant. No single point of failure shall exist in the power connectivity between network racks and UPS system.

### 5.2.18.4 Air Conditioning and Natural Connection

Since ICCC are a critical area, precision air conditioning system shall be exclusively installed to maintain the required temperature. The A/C shall be capable of providing sensible cooling capacities at ambient temperature and humidity with adequate air flow. The task of the SI shall include (but not limited to):

- a) Connecting the indoor unit with the mains electrical point
- b) Connecting indoor and outdoor units mechanically (with 18 G hard gauge copper piping)
- c) Connecting indoor and outdoor unit electrically

The air conditioner shall be linked to secondary power supply as well to prevent them from shutting down in case of power outage.

### 5.2.18.5 UPS requirements and features

UPS system shall provide a redundant power supply to the following needs:

- Servers and important network and storage equipment
- Access control, Fire Detection & suppression system and surveillance system

The system shall be automatic with power supply from the mains and automatic switchover to DG set as secondary source for the ICCC.

### **5.2.19 Handholding and Training**

In order to strengthen the staff, structured capacity building Program shall be undertaken for multiple levels in the organizational hierarchy like foundation process/ soft skills training to the staff for pre-defined period. Also, refresher trainings for City Operation Centre, City Operation Staff and designated the Authority & Police staff shall be a part of Capacity Building. It is important to understand that training needs to be provided to each and every staff personnel of such operation centers. These officers shall be handling emergency situations with very minimal turnaround time.

- a) SI shall prepare and submit detailed Training Plan and Training Manuals to Authority/authorized entity for review and approval.
- b) Appropriate training shall be carried out as per the User Training Plan prepared in detail stating the number of training sessions to be held per batch of trainees, course work for the training program, coursework delivery methodologies and evaluation methodologies in detail.
- c) SI shall be responsible for necessary demonstration environment setup including setup of cameras, Wi-Fi, Smart lighting, Smart traffic, smart parking, smart public transport solutions to conduct end user training. End user training shall include all the equipment including but not limited to all the applications and infrastructure at Operation centers data centers & field Locations. End user training shall be conducted at a centralized location or any other location as identified by Authority with inputs from the SI.
- d) SI shall conduct end user training and ensure that the training module holistically covers all the details around hardware and system applications expected to be used on a daily basis to run the system.
- e) SI shall impart operational and technical training to internal users on solutions being implemented to allow them to effectively and efficiently use the surveillance system.
- f) SI shall prepare the solution specific training manuals and submit the same to Authority for review and approval. Training Manuals, operation procedures, visual help-kit etc. shall be provided in English language.
- g) SI shall provide training to selected officers of the Authority covering functional, technical aspects, usage and implementation of the products and solutions.
- h) SI shall ensure that all concerned personnel receive regular training sessions, from time to time, as and when required. Refresher training sessions shall be conducted on a regular basis.
- i) An annual training calendar shall be clearly chalked out and shared with the Authority along with complete details of content of training, target audience for each year etc.
- j) SI shall update training manuals, procedures manual, deployment/Installation guides etc. on a regular basis (Quarterly/ Biannual) to reflect the latest changes to the solutions implemented and new developments.
- k) The SI shall ensure that training is a continuous process for the users. Basic computer awareness, fundamentals of computer systems, basic, intermediate and advanced application usage modules shall be identified by the SI.

- l) Systematic training shall be imparted to the designated trainees that shall help them to understand the concept of solution, the day-to-day operations of overall solution and maintenance and updating of the system to some extent. This shall be done under complete guidance of the trainers provided by the SI.
- m) Time Schedule and detailed program shall be prepared in consultation with GSCL and respective authorized entity (Police). In addition to the above, while designing the training courses and manuals, SI shall take care to impart training on the key system components that are best suited for enabling the personnel to start working on the system in the shortest possible time.
- n) SI is required to deploy a Master Trainer who shall be responsible for planning, designing and conducting continuous training sessions.
- o) Training sessions and workshops shall comprise of presentations, demonstrations and hands-on mandatorily for the application modules.
- p) Authority shall be responsible for identifying and nominating users for the training. However, SI shall be responsible for facilitating and coordinating this entire process.
- q) SI shall be responsible for making the feedback available for the Authority/authorized entity to review and track the progress, in case, after feedback, more than 30% of the respondents suggest that the training provided to them was unsatisfactory or less than satisfactory then the SI shall re-conduct the same training at no extra cost.

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

#### **A. Basic IT training**

This module shall include components on fundamentals of:

- Computer usage,
- Network,
- Desktop operations,
- User admin,
- Application installation,
- Basic computer troubleshooting etc.

#### **B. Initial Training as part of Project Implementation**

##### **I. Functional Training**

1. Basic IT skills
2. Video Management Software, Video Analytics, ANPR, smart' solutions etc.
3. Software Applications (City Operation Center and Command & Control Center)
4. Mobile Surveillance Vehicle
5. Networking, Hardware Installation
6. Centralized Helpdesk
7. Feed monitoring

### **C. Administrative Training**

1. System Administration Helpdesk, FMS, BMS Administration etc.
2. Master trainer assistance and handling helpdesk requests etc.

### **II. Senior Management Training**

1. Usage of all the proposed systems for monitoring, tracking and reporting,
2. MIS reports, accessing various exception reports

### **D. Post-Implementation Training**

1. Refresher Trainings for the Senior Management
2. Functional/Operational training and IT basics for new operators
3. Refresher courses on System Administration
4. Change Management programs

## **5.3 COMPONENT 3 – DATA CENTER**

### **5.3.1 Data Centre (DC)**

1. The DC will be co-located in the State Data Centre Building. Rack Space & Power will be provided by SDC. Any charges related to this will be directly paid by GSCL to State Data Centre.
2. SI is required to implement all the hardware/software and related items as per the design offered for the smart city infrastructure including SLA monitoring and Help desk management, in a Tier III or above data Center complying to standard guidelines as per Telecommunications Infrastructure UPTIME/TIA-942.
3. The Data center shall be available for 24x7x365 operation.
4. The smart city infrastructure shall have built in redundancy and high availability in compute and storage to ensure that there is no single point of failure.
5. The SI shall submit to Authority adequate documentation/ evidences in support of the choice of the data center to meet the project requirements.
6. Min Guiding factors for the Data Center: Following are the benchmark requirements which should act as guiding factors for the SI;
  - a) There will be dedicated rack space available in the State Data Center for the entire Smart City project Infrastructure.

- b) Access to the Data Centre Space where the Smart City Project Infrastructure is proposed to be hosted should be demarcated and physical access to the place would be given only to the authorized personnel.
- 7. Min 30 days Data Backup of the video feeds and the transaction data for min 1 year shall be stored within the Data Center infrastructure preferable in a cost effective and innovative manner.
- 8. In case the data center services are to go down due to any unforeseen circumstance, the Integrated Command Center should have access to the video feeds of previous 30 days and the transaction data for min 3 months from this data backup facility.
- 9. Access logs to be stored for the entire duration of contract and handed over to Authority upon termination/expiry of the contract.

#### 5.3.1.1 Technical Specifications of State Data-Center

Following sections highlight the indicative facilities are readily available at State Data Centre (SDC).

- 1. Design Standard: Tier-III or above (certification in process)
- 2. The availability of Power/Cooling/Internet bandwidth should be guaranteed as per Tier III Data Center requirement
- 3. Receiving Power: SDC redundant UPS
- 4. UPS: UPS system with N+N redundancy
- 5. Generator: Gen-set with N+1 redundancy
- 6. Power Provision: Dual power feed, PDU sources to each rack, minimum 5KW Power supply to each rack or as per requirement. Rack PDUs should be arranged by Bidder if existing PDUs at SDC are not enough.
- 7. Cooling Features available at SDC:
  - a) System: In-row Air-cooling system with N+1 redundancy, Management of temperature and humidity
  - b) Blow-out Type: In-row air conditioning system, with -horizontal air flow
- 8. **Fire Protection:** Highly Sensitive Smoke Detectors, Fire Suppression System available at SDC.



9. **Security:** CCTV surveillance cameras, 24x7 on-site security presence, building Access (Photo Id Card must) along with biometric authentication will be available at SDC.

### 5.3.1.2 IT Infrastructure for Data centre

Following sections highlight the indicative scope of work of the SI and not limited for Design, Supply and Deployment of IT Infrastructure for Data Center

#### 1. Hardware and Network Provisioning

- a) SI shall be responsible for the following but not limited to:
- b) Appropriate sizing and provisioning of IT infrastructure like servers/storage, network devices (like routers/switches etc.), security equipment including firewalls, etc. with the required components/modules considering redundancy and load balancing in line with minimum technical requirements
- c) Warranty for all the IT hardware assets procured to comply with the requirements as defined in this RFP.
- d) Size the bandwidth requirements across all locations considering the application performance, replication, data transfer, internet connectivity for Data center and other requirements.
- e) Furnish a schedule of delivery of all IT Infrastructure items
- f) Ensure all the hardware requirements of the application suite (including third party applications), databases, OS and other software are met.
- g) Authority may at its sole discretion evaluate the hardware sizing. The SI needs to provide necessary explanation for sizing to Authority
- h) Ensure that the proposed servers are able to accommodate newer versions of processors, memory, etc. that support enhanced capability (e.g. lower power footprint, higher working temperature, smaller process architecture, higher frequency) of operation if required, whenever they are available. To further clarify, motherboard, controllers, etc. provided shall be of latest architecture available that supports such newer version.
- i) The proposed server models wherever applicable shall be Blade Mount servers with key board, monitor, etc. shared to minimize the requirement of rack space in Data

center considering any space constraints. The model however shall not pose constraints in performance.

## **2. Provisioning switches**

- a) The SI shall size and propose requisite switch at Data center with the required components/modules considering redundancy and load balancing.
- b) The SI shall size and propose additional switches if required for interconnecting various segments, operations center, work area, etc.
- c) Minimum requirement provided in the RFP. In case any other switch/module/transceiver/cables/features, if required, should be mentioned by the bidder in their proposal.

## **3. IP address schema (both IPv4 and IPv6)**

- a) The SI shall design suitable IP Schema for the entire Wide Area Network including Data center and interfaces to external systems/network. The SI shall ensure efficient traffic routing irrespective of link medium.
- b) The SI shall maintain the IP Schema with required modifications from time to time during the project period.
- c) SI should provide the unique identity schema similar to addressing schema for all hardware components.

## **4. Sub-Networks & Management of Network operation**

- a) The proposed architecture of Data center shall be divided into different sub-networks. These networks shall be separated from other networks through switches and firewalls. The logical separations of these sub-networks shall be done using VLANS.
- b) A separate VLAN shall be created to manage the entire network. This network shall have systems to monitor, manage routers, switches, Firewalls, etc. The SI shall provide necessary hardware / server for loading the monitoring software if required.

## **5. Provisioning Storage**

- a) Storage requirements for the application suite shall have to be assessed by the SI and the storage solution shall be sized and procured accordingly. SI shall propose appropriate storage mechanism in order to accommodate proposed application suite requirement of the Authority
- b) The proposed storage shall be configured with appropriate redundancy to maintain business continuity.
- c) Minimum requirement provided in the RFP. In case any other components/features, if required, should be mentioned by the bidder in their proposal.

## **6. Network Equipment level redundancy**

- a) The SI shall provide real-time redundancy at the network equipment level in Data center, and there shall not be any single point of failure.
- b) All equipment shall be provided with dual power supply modules. Each of the two supply modules shall be connected to alternate power strips of the network rack (two power strips to be provided in each network rack).
- c) The Network Equipment redundancy stipulations wherever prescribed are the minimum requirements that the SI needs to consider. However, SI needs to estimate and plan actual requirements considering service level requirements specified in this RFP.

## **7. Provisioning IT Security Equipment**

- a) The SI shall size and propose firewalls with the required components/modules for Data center. Minimum specification provided in the RFP. In case any other component/feature required for Firewalls or overall Security of the project should be mentioned by the bidder in their proposed solution.
- b) Both Internal Firewall and External Firewall should be from different OEMs.
- c) Necessary mechanism shall be adopted by selected SI for monitoring the traffic of all the VLANs at Data center.
- d) Necessary devices for log capture from servers, network equipment and other devices shall be provisioned and provided.
- e) The SI shall implement DNS server so that the URL can be used instead of accessing web server using IP address directly. The required Hardware and Software for DNS server at Data center shall be provisioned by the SI.

- f) SI shall implement management systems and procedures that adhere to Authority's security policies.
- g) SI shall secure network resources against unauthorized access from internal or external sources.
- h) SI shall also provide a mechanism for tracking security incidents and identifying patterns, if any. The tracking mechanism shall, at a minimum, track the number of security incident occurrences resulting in a user losing data, loss of data integrity, denial of service, loss of confidentiality or any incident that renders the user unproductive for a period of time
- i) SI shall ensure that all firewall devices are staged and comprehensively tested prior to deployment. In addition, SI shall conduct a vulnerability scan and analysis of the network to ensure that the optimal policies are instituted on the firewall.
- j) SI shall ensure that all firewall management is initiated from a segregated management rail on the network.
- k) SI shall provide intrusion management services to protect Authority's resources from internal and external threats.
- l) SI shall provide Authority with the necessary hardware/software required for efficient intrusion management.
- m) DC shall have built in redundancy and high availability in compute and storage to ensure that there is no single point of failure. There shall be no loss of video recording in an ICCC in case of failure of any single server and storage component.
- n) DC shall work in an Active-Active mode.
- o) The SI shall design the DC Solution with the necessary load balancing, replication and recovery solution that provide zero RPO (Recovery Point Objective) and RTO (Recovery Time Objective) of 10 minutes.
- p) The DC shall be periodically audited for vulnerabilities; updated and mock drills shall be performed. Along with the findings, the improvements /corrective steps to be taken to eliminate the noncompliance and record of the same shall be maintained.
- q) The bidder shall submit the detailed solution document for DC solution with justification for the proposed design meeting the requirements along with the bid.
- r) The security Audit of vulnerability assessment, Access Control assessment for entire system shall be performed half yearly and the report with corrective & preventive actions shall be provided. COC application shall be audited for SOPs, KPIs and Policies half yearly and updates shall be done in the SOPs, KPIs and Policies with prior approval from the Authority.

- s) Minimum requirement provided in the RFP. In case any other components/features, if required, should be mentioned by the bidder in their proposal.

Technology refresh is to be considered at the end of five years and SI must submit the report for the same.

### 8. System Integration

The SI shall ensure seamless integration of City Surveillance system with an external Geographical Information System (GIS). The GIS console shall allow operators to get an overview of the entire system and access to all system components. GIS shall enable dynamic view of the location and status of resources and objects/sensors. System shall enable authorized user to open a new incident and associate the incident with its geographic location automatically, via the GIS display.

The proposed City Surveillance System shall also provision for seamless integration with other government datasets like Vaahan, Sarathi, Dial-100, e-challan etc. as and when they are available from respective agencies.

### 5.3.2 Data Center Spine & Leaf Switching Solution

S. No	Minimum Specification from Day 1	Specification proposed by bidder with Page No of Data Sheet/Product Brochure/Configuration Guide/etc.	Compliance (Y/N)
	Spine Switch: Make: Model: Part Code:		
	Leaf Switch: Model: Part Code:		
1	19" rack mountable with kits		
2	Active switching throughput should be minimum I) Spine Switch - 6.4 Tbps ii) Leaf (ToR) Switch – 1.44 Tbps		
3.1	Spine Switch – i) 32 x 40/100GbE QSFP28 ports. Populated with		

S. No	Minimum Specification from Day 1	Specification proposed by bidder with Page No of Data Sheet/Product Brochure/Configuration Guide/etc.	Compliance (Y/N)
	24 numbers of 40 GbE QSFP+ MPO transceivers (multimode) ii) additional cables/transceivers to be proposed for interconnecting all Data Center components required to complete Smart City design requirement.		
3.2	Leaf Switch – i) 24x 1000BaseT Ports ii) 24 x 10GbE SFP+ Fiber ports. Populated with 24 numbers of 10 Gig SFP+ transceivers (multimode) iii) 2x40GbE QSFP+ ports for uplink connectivity to each Spine Switches. iv) additional 4x40GbE QSFP+ ports for future scalability.		
4	Leaf and Spine Switches should be from a single OEM.		
5	The solution should provide IPV4 and IPV6 compliant without any performance degradation.		
6	Should have 32MB buffer.		
7	Should have redundant Power Supply.		
8	Layer 2 switch ports and VLAN trunks (IEEE 802.1Q VLAN encapsulation)		
9	Support for at least 4000 VLANs.		
10	Spanning-Tree Protocols - 802.1d, 802.1s & 802.1w		
11	Support for 200,000 or more MAC addresses		
12	The solution must support static MAC address assignment for interface.		
13	The solution must support per VLAN MAC address filtering.		
14	The solution must support Jumbo frames up to 9216 bytes		
15	VRRPv3/HSRPv3 or equivalent		
16	Static IP routing		
17	Dynamic Routing -		

S. No	Minimum Specification from Day 1	Specification proposed by bidder with Page No of Data Sheet/Product Brochure/Configuration Guide/etc.	Compliance (Y/N)
	i) OSPF, OSPFv3 ii) BGPv4 iii) Route redistribution among above routing protocols		
18	Should support DHCP		
19	IEEE 802.1p class-of- service (CoS) prioritization		
20	IEEE 802.3ad		
20.1	UL 60950-1, EN 60825-1/ EN 55022 Class A/FCC Class A		
20.2	RoHS / WEEE compliant.		
21	The solution must support IEEE 802.1Qbb Priority-based Flow Control (PFC).		
22	The solution must support IEEE 802.1Qaz.		
23	The solution must support Data Center Bridging Exchange Protocol (DCBX)		
24	Should support Unidirectional Link Detection Protocol (UDLD)		
25	Shall support Redundant Fans		
26	Shall support On-line insertion and removal for transceivers, Power Supply units and Fans.		
27	Shall support storage requirements of multiple images and configurations.		
28	The solution should support NSSU/ISSU or equivalent.		
29	The solution must support 6 hardware unicast queues		
30	Should have IGMPv1/v2/v3, ICMPv6		
31	Must support the following Access Control Lists (ACLs):		
	- Port-based ACL (PAACL) – Ingress and Egress		
	- VLAN-based ACL (VACL) – Ingress and Egress		
	- IP-based ACL– Ingress and Egress		

S. No	Minimum Specification from Day 1	Specification proposed by bidder with Page No of Data Sheet/Product Brochure/Configuration Guide/etc.	Compliance (Y/N)
32	The solution must support min of 2000 ACL entries.		
33	The solution must support the ability to add/remove/change/insert ACL entries		
34	Shall have support for CLI, Telnet and SNMPv1, v2, v3		
35	Shall support SSH		
36	Should support multiple levels of administration roles to manage and monitor the device.		
37	Should support Network Time Protocol.		
38	Should be able to send and receive Syslog and SNMP traps from devices.		
39	The solution must have virtualization feature.		
40	Should support VXLAN or other virtualization techniques from day 1		
41	Should support Open Flow/ Open Contrail/ Open Day Light/ Open Stack.		
42	All sub-components should be from same OEM as that of the Switches.		
43	The bidder should propose complete BoM with part codes of sub-components, warranty, license, subscription etc.		
44	The OEM should be available in India Market for last 5 years.		
45	The OEM should have TAC support in India.		
46	The OEM should have service Center in Eastern part of India.		
47	The OEM Should have spare warehouse in Eastern Part of India for speedy replacement of spares.		
48	Any other component/feature/ required to fulfill the Smart City design requirement. (if any to be mentioned by Bidder). Proposed solution should be complete in all respect.		



Note: 48 nos. of Multimode Fiber Patch Cord of length 1m, 2m, 5m, 10m etc. as required to interconnect Internal Firewalls, Blade Servers and Storage Units with Leaf and Spine Switches to be submitted in the Bill of Material. OEM Make/Mode with Product Part Codes to be clearly mentioned.

### 5.3.3 Data Center Out of Band Switches

S. No	Minimum Specification from Day 1	Specification proposed by bidder with Page No of Data Sheet/Product Brochure/Configuration Guide/etc.	Compliance (Y/N)
(a)	Make (To be provided by bidder)		
(b)	Model (To be provided by bidder)		
1	19" rack mountable with kits		
2	Active switching throughput should be minimum		
3	48 x 1000BaseT ports with 2xSFP+ Uplinks		
4	SFP - Should be from same OEM as that of Leaf and Spine Switches.		
5	The switch should provide IPV4 and IPV6 compliant without any performance degradation.		
6	Should support minimum 8MB buffer.		
7	Should have redundant Power Supply.		
8	Layer 2 switch ports and VLAN trunks (IEEE 802.1Q VLAN encapsulation)		
9	Support for at least 256 VLANs.		
10	Spanning-Tree Protocols - 802.1d, 802.1s & 802.1w		
11	Support for 8,000 or more MAC addresses		
12	Must support static MAC address assignment for interface.		
13	Must support per VLAN MAC address filtering.		
14	Must support Jumbo frames up to 9216 bytes		
15	Static IP routing		
16	Should support DHCP		

S. No	Minimum Specification from Day 1	Specification proposed by bidder with Page No of Data Sheet/Product Brochure/Configuration Guide/etc.	Compliance (Y/N)
17	IEEE 802.1p class-of- service (CoS) prioritization		
18	IEEE 802.3ad		
19.1	UL 60950-1, EN 60825-1/ EN 55022 Class A/FCC Class A or equivalent		
19.2	RoHS / WEEE regulations.		
20	Must support IEEE 802.1Qbb Priority-based Flow Control (PFC).		
21	Shall support storage requirements of multiple images and configurations.		
22	System should support NSSU/ISSU or equivalent.		
23	Must support the following Access Control Lists (ACLs):		
	- Port-based ACL (PAACL) – Ingress and Egress		
	- VLAN-based ACL (VACL) – Ingress and Egress		
	- IP-based ACL– Ingress and Egress		
24	The Switch must support min of 200 ACL entries in hardware.		
25	The Switch must support the ability to add/remove/change/insert ACL entries		
26	Shall have support for CLI, Telnet and SNMPv1, 2, v3		
27	Shall support SSH		
28	Should support multiple levels of administration roles to manage and monitor the device.		
29	Should support Network Time Protocol.		
30	Should be able to send and receive Syslog and SNMP traps from devices.		
31	All sub-components should be from same OEM as that of the Switches.		
32	The bidder should propose complete BoM with part codes of sub-components, warranty, license, subscription etc. for 5 years.		

S. No	Minimum Specification from Day 1	Specification proposed by bidder with Page No of Data Sheet/Product Brochure/Configuration Guide/etc.	Compliance (Y/N)
33	The OEM should be available in India Market for last 5 years		
34	The OEM should have TAC support in India		
35	The OEM should have service Center in Eastern part of India		
36	The OEM Should have spare warehouse in Eastern Part of India for speedy replacement of spares.		
37	Any other components required to fulfill the proposed design requirement including Cat6/Cat6A Patch Cord.		

#### 5.3.4 Network Management System / Enterprises Management System (NMS/EMS)

Bidder should include the hardware and software required to complete the proposed – NMS/EMS/ solution without any additional cost.

S. No.	Minimum Specifications	Compliance (Yes/No)
1	Network Management Software is a graphical network monitoring and management tool for all component.	
2	Should automatically create a complete topology map for switches, firewalls and wireless Access Points (APs), Camera etc.	
3	Should Facilitate simple management of many, or all, network devices at once. It should monitor up-to-date network status, and provides actionable reporting for the timely resolution of any network problems	
4	Support add intuitive usability, with an overview dashboard, simplified navigation and more network information	
5	Should automatically-generated network topology map show a device list, and gives the ability to search for specific devices	
6	Should have Status display for all devices alerts users of any problems	
7	Should provide direct connectivity to one, many, or all devices for configuration updates	
8	Should provide management of device backup and firmware upgrades	
9	Should be additional wireless APs can be registered and configured	

S. No.	Minimum Specifications	Compliance (Yes/No)
10	Should support comprehensive log management	
11	Comprehensive event log provides network issue resolution. Solution should be inclusive with hardware, OS, patches, database and any other licenses for their monitoring etc.	
12	The solution should be scalable to meet the requirement for the entire project period. And the cost for scalability for the period of the project should be built-in.	
13	Should be SNMP v1, v2, v3 and MIB-II compliant.	
14	Should be ITIL 2011 compliant in at-least incident, problem, change, knowledge, Service Level, service asset (hardware, software) and configuration management.	
15	Filtering of events should be possible, with advance sort option based on components, type of message, time etc. Automated trend analysis of unstructured data.	
16	Should support Web / Administration Interface.	
17	Should provide accessibility to database of the EMS via the Application GUI	
18	Solution should be open, distributed, and scalable and open to third party integration.	
19	Should provide fault and performance management for multi-vendor TCP/IP networks	
20	Should be able to provide secured windows-based consoles /secured web-based consoles for accessibility to EMS.	
21	Should have web browser interface with user name and Password Authentication.	
22	Administrator/ Manager should have privilege to create/modify/delete user.	
23	Support discriminated polling.	
24	Should be able to update device configuration changes such as re-indexing of ports.	
25	Should be able to get fault information in real time and present the same in alarm window with description, affected component, time stamp etc.	
26	Should be able to get fault information from heterogeneous devices — routers, switches, servers etc.	
27	Event related to Servers should go to a common enterprise event console where a set of automated tasks can be defined based on the policy.	
29	Should have ability to correlate events across the entire infrastructure components of SDC.	
30	Should support automatic event correlation in order to reduce events occurring in SDC.	

S. No.	Minimum Specifications	Compliance (Yes/No)
31	Should support advanced filtering to eliminate extraneous data / alarms in Web browser and GUI.	
32	Should be configurable to suppress events for key systems/devices that are down for routine maintenance or planned outage.	
33	Should be able to monitor on user-defined thresholds for warning/critical states and escalate events to event console of enterprise management system.	
34	Should be able to document connectivity changes that were discovered since the last update.	
35	Should provide out of the box root cause analysis with multiple root cause algorithms inbuilt for root cause analysis.	
36	Should have self-certification capabilities so that it can easily add support for new traps and automatically generate alarms	
37	Should provide enough reports pertaining to asset and change management, alarms and availability of critical network resources as well as network response times for critical links	
38	The tool shall integrate network, server and database performance information and alarms in a single console and provide a unified reporting interface for network and system components. The current performance state of the entire network and system infrastructure shall be visible in an integrated console.	
39	Should provide an integrated performance view for all the managed systems and networks along with the various threshold violations alarms in them. It should be possible to drill-down into the performance view to execute context specific reports	
40	Should provide the following reports for troubleshooting, diagnosis, analysis and resolution purposes like Trend analysis, utilization, forecasting reports or equivalent etc.	
41	Should be able to auto-calculate resource utilization baselines for the entire managed systems and networks and allow user to set corresponding upper and lower threshold limits	
42	Should provide accurate discovery of layer 3 and heterogeneous layer 2 switched networks for Ethernet	
43	Manual discovery can be done for identified network segment	
44	Should be able to discover links with proper color status propagation for complete network visualization.	
45	Should support dynamic object collections and auto discovery. The topology of the entire Network should be available in a single map.	
46	Should give user option to create his /or her map based on certain group of devices or region.	
46	Should provide custom visual mapping of L2 and L3 devices connectivity and relationships.	

<b>S. No.</b>	<b>Minimum Specifications</b>	<b>Compliance (Yes/No)</b>
47	Should monitor various operating system parameters such as processors, memory, files, processes, file systems etc. where applicable on the servers to be monitored.	
48	Provide performance threshold configuration for all the agents/monitors to be done from a central GUI based console that provide a common look and feel across various platforms in the enterprise. These agents/monitors could then dynamically reconfigure them to use these threshold profiles they receive.	
49	Should be able to monitor/ manage large heterogeneous systems environment continuously.	
50	Should monitor / manage following	
50.1	Event log monitoring	
50.2	Virtual and physical memory statistics	
50.3	Paging and swap statistics	
50.4	Operating System	
50.5	Memory	
50.6	Logical disk	
50.7	Physical disk	
50.7	Process	
50.8	Processor	
50.9	Paging file	
50.10	IP statistics	
50.11	ICMP statistics	
50.12	Network interface traffic	
50.13	Cache	
50.14	Active Directory Services	
51	Should be capable of view/start/stop the services on windows servers	
51.1	Unix / Linux	
51.2	Should monitor with statistics	
51.3	CPU Utilization, CPU Load Averages	
51.4	System virtual memory (includes swapping and paging)	
51.5	Disk Usage	
51.6	No. of nodes in each file system	
51.7	Network interface traffic	
51.8	Critical System log integration	
51.9	IIS / Tomcat / Web server statistics	
51.10	HTTP service	
51.11	HTTPS service	
51.12	FTP server statistics	
51.13	POP/ SMTP Services	
51.14	ICMP services	

S. No.	Minimum Specifications	Compliance (Yes/No)
52	Database Services – Monitor various critical relational database management system (RDBMS) parameters such as database tables / table spaces, logs etc.	
53	Should able to generate reports on predefined / customized hours.	
54	Should be able to present the reports through web and generate “pdf” / CSV / ASCII reports of the same.	
55	Should provide user flexibility to create his /or her custom reports based on time duration, group of elements, custom elements etc.	
56	Should provide information regarding interface utilization and error statistics for physical and logical links.	
57	Should create historical performance and trend analysis for capacity planning.	
58	Should be capable to send the reports through e-mail to pre-defined user with pre-defined interval.	
59	Should have capability to exclude the planned-downtimes or downtime outside SLA.	
60	Should be able to generate all sorts of SLA Reports.	
61	Should be able to generate web-based reports, historical data for the systems and network devices and Near Real Time reports on the local management console.	
62	Should be able to generate the reports for Server, Application, infrastructure services and Network devices in SDC environment	
63	Availability and Uptime – Daily, Weekly, Monthly and Yearly Basis	
63.1	Trend Report	
63.2	Top N report	
63.3	Custom report	
63.4	MTBF and MTTR reports	
63.5	Device Performance – CPU and Memory utilized	
63.6	Interface errors	
63.7	Server and Infrastructure services statistics	
63.8	Trend report based on Historical Information	
63.9	Top N report	
63.10	Custom report	
63.11	SLA Reporting	
63.12	Computation of SLA for entire SDC Infrastructure	
64	Automated Daily, Weekly, Monthly, Quarterly and Yearly SLA reports	
65	For reporting, required RDBMS to be provided with all licenses.	
66	Should have enough Storage capacity should to support all reporting data for the period of the Project	
67	Should be able to receive and process SNMP traps from infrastructure components such as router, switch, servers etc.	
68	Should be able integrate with Helpdesk system for incidents.	

S. No.	Minimum Specifications	Compliance (Yes/No)
69	Should be able to send e-mail or Mobile –SMS to pre-defined users for pre-defined faults.	
70	Should trigger automated actions based on incoming events / traps. These actions can be automated scripts/batch files.	
71	The Network Management function must monitor performance across heterogeneous networks from one end of the enterprise to the other.	
72	It should proactively analyze problems to improve network performance.	
73	It should provide traffic management capabilities	
74	The Network Management function should create a graphical display of all discovered resources.	
75	The Network Management function should have extensive reporting facility, providing the ability to format and present data in a graphical and tabular display	
76	The Network Management function should collect and analyze the data. Once collected, it should automatically store data gathered by the NMS system in a database. This enterprise-wide data should be easily accessed from a central location and used to help with capacity planning, reporting and analysis.	
77	The Network Management function should also collect traffic statistics on client/server sessions, which cross the LAN on which it is running.	
78	The Network Management function should also provide information on performance of Ethernet segments, including capacity utilization and error statistics for the segment and the top contributing hosts, WAN links and routers.	
79	Alerts should be shown on the Event Management map when thresholds are exceeded and should subsequently be able to inform Network Operations Center (NOC) and notify concerned authority using different methods such as pagers, emails, etc.	
80	It should be able to automatically generate a notification in the event of a link failure to ensure proper handling of link related issues.	
81	The Systems and Distributed Monitoring (Operating Systems) of EMS should be able to monitor:	
82	Processors: Each processor in the system should be monitored for CPU utilization. Current utilization should be compared against user-specified warning and critical thresholds.	
83	File Systems: Each file system should be monitored for file system space used, which is compared to user-defined warning and critical thresholds.	
84	Log Files: Logs should be monitored to detect faults in the operating system, the communication subsystem and in applications. The function should also analyze the files residing on the host for specified	



S. No.	Minimum Specifications	Compliance (Yes/No)
	string patterns.	
85	System Processes: The System Management function should provide real-time collection of data from all system processes. This should identify whether an important process has stopped unexpectedly. Critical processes should be automatically restarted using the System Management function.	
86	Memory: The System Management function should monitor memory utilization and available swap space.	
87	Event Log: User-defined events in the security, system, and application event logs must be monitored.	
88	EMS should integrate with the application software component of portal software that measures performance of system against the following SLA parameters:	
88.1	Response times of Portal;	
88.2	Uptime of data center;	
88.3	Meantime for restoration of Data Centre etc.;	
89	EMS should compile the performance statistics from all the IT systems involved and compute the average of the parameters over a quarter and compare it with the SLA metrics laid down in the RFP.	
90	The EMS should compute the weighted average score of the SLA metrics to help in arriving at the quarterly service charges payable to the Agency.	
91	The SLA monitoring component of the EMS should be under the control of the authority that is nominated to the mutual agreement of Director the partner to ensure that it is in a trusted environment.	
92	The Reporting and Analysis tool should provide a ready-to-use view into the wealth of data gathered by Management system and service management tools. It should consolidate data from all the relevant modules and transform it into easily accessible business-relevant information. This information should be presented in a variety of graphical formats that can be viewed interactively (slice, dice, drill-down, drill through).	
93	The tool should allow customers to explore the real-time data in a variety of methods and patterns and then produce reports to analyze the associated business and service affecting issues.	
94	The presentation of reports should be in an easy to analyze graphical form enabling the administrator to put up easily summarized reports to the management for quick action (Customizable Reports). The software should be capable of supporting the needs to custom make some of the reports as per the needs of the organization.	
95	Provide Historical Data Analysis: The software should be able to provide a time snapshot of the required information as well as the	

S. No.	Minimum Specifications	Compliance (Yes/No)
	period analysis of the same in order to help in projecting the demand for bandwidth in the future.	
96	Management layer should provide ability to determine which part of application is creating performance issue	
97	Ability to determine network roundtrip times of your user groups	
98	Ability to do usage trend analysis	
99	Effective service level management: Service levels are important measures of business performance. The management layer should provide the right measures for the service level agreements for business continuity and operational efficiency. It should monitor service availability, performance, usage, measure availability and performance from representative key user locations, determine root cause and impact of service failures on overall service level agreement.	
100	Application performance management: The management framework should help in enhancing system performance and reliability of the system to ensure improvement in the overall operational efficiency.	
101	Proactive monitoring: The management framework should provide for proactive, unattended monitoring of the database system	
102	Configuration and patch management: Management platform must provide a tool which tracks and analyzes hardware, database, OS and application server software configurations and lowers the cost of complex operations such as applying software patches, enforcing operational policies and cloning core IT infrastructure systems (such as databases and application servers).	
103	Heterogeneous platform Monitoring support: The management platform must provide support to monitor multiple middle tier application servers, multiple database servers, multiple directories servers, multiple Operating Systems and multiple firewalls.	
104	The Helpdesk system should provide flexibility of logging incident manually via windows GUI and web interface.	
105	The web interface console of the incident tracking system would allow viewing, updating and closing of incident tickets.	
106	The trouble-ticket should be generated for each complaint and given to asset owner immediately as well as part of email.	
107	Helpdesk system should allow detailed multiple levels/tiers of categorization on the type of security incident being logged.	
108	It should provide classification to differentiate the criticality of the security incident via the priority levels, severity levels and impact levels.	
109	It should maintain the SLA for each item/service. The system should be able to generate report on the SLA violation or regular SLA compliance levels.	
110	It should be possible to sort requests based on how close the requests	

S. No.	Minimum Specifications	Compliance (Yes/No)
	are to violate their defined SLAs.	
111	It should support work shifts for SLA & automatic ticket assignment	
112	It should support the holiday definition & SLA clock should stop on holiday or non-working days. SLA clock should stop after the analyst shift is over case of non 24x7 support environment.	
113	It should allow the helpdesk administrator to define escalation policy, with multiple levels & notification, through easy to use window GUI / console.	
114	System should provide a Knowledge base to store history of useful incident resolution.	
115	It should have an updateable knowledge base for technical analysis and further help end-users to search solutions for previously solved issues.	
116	It should be able to provide web-based knowledge tools that provides the flexibility to search based on filter noise words methods, list the commonly used security knowledge article methods and deduction methods using a series of questions and answers.	
117	It should the web-based knowledge tool would allow users to bookmark their favorite security knowledge articles for quick references.	
117	It should be possible to specify an expiration date to a document so that if the same becomes irrelevant for an organization it will be unpublished (removed/expired).	
118	The knowledge tools should provide grouping access on different security knowledge articles for different group of users.	
119	Provide seamless integration to generate events/incident automatically from NMS / EMS.	
120	It should be able to provide detail asset information on hardware and software inventory through seamless integration with asset management software.	
121	Each incident could be able to associate multiple activity logs entries manually or automatically events / incidents from other security tools or EMS / NMS.	
122	Allow categorization on the type of incident being logged.	
123	Provide classification to differentiate the criticality of the incident via the priority levels, severity levels and impact levels.	
124	Provide audit logs and reports to track the updating of each incident ticket.	
125	Proposed incident tracking system would be ITIL 2011compliant.	
126	It should be possible to do any customizations or policy updates in flash with zero or very minimal coding or down time.	
127	It should integrate with Enterprise Management System event management and support automatic problem registration, based on	

<b>S. No.</b>	<b>Minimum Specifications</b>	<b>Compliance (Yes/No)</b>
	predefined policies.	
128	It should be able to log and escalate user interactions and requests.	
129	It should support tracking of SLA (service level agreements) for call requests within the help desk through service types.	
130	It should be capable of assigning call requests to technical staff manually as well as automatically based on predefined rules, and should support notification and escalation over email, web etc.	
131	It should provide status of registered calls to end-users over email and through web.	
132	The solution should provide web-based administration so that the same can be performed from anywhere.	
133	It should have customized Management Reports for senior executives with live reports from helpdesk database.	
134	It should have an integrated CMDB for strong Change Management capabilities. Should integrate with existing Helpdesk deployed.	
135	CMDB should populate the relationship between CI (Configuration Items)	
136	The OEM should be available in India Market for last 5 years	

### 5.3.5 Intranet Firewall with IPS.

<b>S. No.</b>	<b>Minimum Specifications</b>	<b>Compliance (Y/N)</b>
(a)	Make (to be provided by bidder)	
(b)	Model (to be provided by bidder)	
1.1	Appliance must de-liver at least 20 Gbps Next Generation Intrusion Prevention throughput (with enabling Firewall and IPS feature simultaneously)	
1.2	Appliance must deliver at least 80 Gbps of Firewall throughput	
1.3	Appliance must Support at least 15 Million Concurrent firewall connections on device from day 1	
1.4	Firewall must support 400K of new connections/sec	
1.5	Support of at least deliver 10 Gbps IPsec VPN throughput)	
1.6	The Appliance must deliver the SSL/TLS inspection throughput of 4 Gbps.	
1.7	No limitation for client connecting using SSL VPN	

S. No.	Minimum Specifications	Compliance (Y/N)
1.8	Should support at least i) 8x1000BaseT ports ii) 8x10Gbps Ports. (Populated with 2x10G Single mode transceiver to SDC Internet Switch and 4x10G multimode transceiver) iii) 2x40G Ports (Populated with 2x40G multimode transceiver) for connectivity to both Spine Switches. iv) Should have additional 2x40G ports for connectivity to both the Core Routers. v) 1x1000BaseT management port vi) 1xConsole Port	
<b>Platform Architecture</b>		
2.1	The Firewall should have Multi core processor-based/ASIC-based security architecture to process and mitigate day-to-day threats.	
2.2	The appliance must not have reported a backdoor vulnerability in OS in past five years	
2.3	The platform must have a centralized management to manage all firewalls in every site. Reporting solution must be quoted along with solution to generate Firewall and other next generation features logs. Firewall logs should be stored for 1 year	
2.4	The firewall shall not restrict number of IP addresses and users by licenses.	
2.5	The firewall shall not impose restriction on the numbers of policies or rules exist on the system.	
2.6	For future redeployment flexibility, the firewall shall be a dedicated appliance supporting multi product roles capable of switching between Layer 2 Firewall, Dedicated IPS or NGFW roles without change of licenses and without any additional cost.	
2.7	i) Firewall should have minimum 10 virtual contexts/VDOM ii) Firewall should be SD-WAN ready	
2.8	The firewall shall support proxy of services, which terminate connections at the firewall and make separate connections with each of the communicating hosts, to enforce protocol validation and to restrict the allowed parameters for each protocol.	
2.9	The firewall shall achieve the following industry recognized security certification standards: . Common Criteria Protection Profile . FIPS 140-2	

S. No.	Minimum Specifications	Compliance (Y/N)
2.1	The appliance must have inbuilt redundant power supply and fans	
2.11	Management or Controller must monitor the Network statistics, including continuous performance monitoring of jitters, latency, and packet loss for all network paths/ link utilization.	
2.12	Solution must support Documented API enabling easy third-party product and service integration Using REST architecture where data can be XML or JSON coded	
2.13	Solution must be able to define the Custom roles (in addition to predefined roles) to control permissions flexibly and accurately	
2.14	Admin must view log information as part of his Overviews or create reports based on the received data.	
<b>Security Specifications</b>		
3.1	Firewall Services with Access Lists and Time-based Access lists to provide supervision and control.	
3.2	Firewall for stateful blocking, Anti-Spoofing, IP Reputation, Geo-Protection, Dropping Invalid Connections	
3.3	Must support DDoS functionality and protect DDOS attack like UDP Flood, Ping of Death.	
3.4	Must support configuration rollback feature to detect and recover from software and configuration errors by reverting to previously active software or configuration.	
3.5	IPS must deliver more than 10000 fingerprint situations for detecting exploit attempts against known vulnerabilities in protocol specific TCP/UPD port number	
3.6	IPS/ Anti-Bot must employ the below inspection technologies 1. Multilayer traffic normalization 2. Vulnerability-based fingerprints 3. Evasion and anomaly logging 4. Decryption-based detection 5. Message length sequence analysis	
3.7	The IPS/Anti-Bot must be able to detect botnets based on signatures, cipher algorithms and analyst of communications channels C&C with bigger granularity of geolocation	
3.8	IPS must support Network traffic normalization and evasion prevention techniques against Stealth cyber-attack methods	
<b>High Availability Specifications</b>		
4.1	The firewall must include support for the following high availability feature. · Active-Active and Active-Standby	

S. No.	Minimum Specifications	Compliance (Y/N)
	· Stateful failover including VPN connections	
<b>Reporting Capabilities</b>		
5.1	The Solution should support granular Real-Time Monitoring and Historical Reporting	
5.2	Network statistics, including continuous performance monitoring of jitters, latency, and packet loss for all network paths/ link utilization.	
5.3	The Solution should provide automated, real-time event alert mechanism.	
5.4	The solution should be able to generate system events/logs for events that have taken place in the system such as a login, changes to configuration and system related errors or warnings.	
5.5	The Solution should have GUI (Graphical User Interface) for Report Generation.	
5.6	The Solution MUST provide following reports of Individual Link Quality/Virtual Link Quality on daily, weekly, monthly etc.	
5.7	The solution should provide option for scheduling reports.	
5.8	All Reports must be exportable in CSV format / PDF format	
5.9	The bidder should propose complete BoM with part codes of sub-components, warranty, license, subscription etc.	
5.10	The bidder should propose complete BoM with part codes of sub-components, warranty, license, subscription etc. for 5 years.	
5.11	The OEM should be available in India Market for last 5 years.	
5.12	The OEM should have TAC support in India	
5.13	Any other components required to fulfill the firewall design requirement should be mentioned.	
5.14	Should be able to integrate with the proposed SIEM solution.	

### 5.3.6 Next Generation Firewall

S. No.	Minimum Specification from Day 1	Compliance (Y/N)	Product Doc. Reference
<b>a</b>	Make: <to be provided by the bidder>		
<b>b</b>	Model: <to be provided by the bidder>		
<b>1</b>	Firewall Solution must have NDPP certification.		
	<b>Hardware Architecture</b>		

S. No.	Minimum Specification from Day 1	Compliance (Y/N)	Product Doc. Reference
2	The proposed solution/appliance MUST have up to Layer 7 protection. There should be no performance degradation in the overall transaction processing. The solution shall be deployed in HA mode in the DC. Mechanism for Layer 7 protection to be clearly mentioned in proposed solution and Bill of material and proposed design document.		
3	The appliance based security platform should be capable of providing firewall, deep packet inspection, application visibility & control, Anti APT features and VPN functionality in a single appliance.		
4	The proposed firewall appliance should have at least 12 ports of 10/100/1000 along with 8 ports of 10 Gig SFP+ ports with separate management port and 4 * 40 G ports from Day one.		
<b>Performance &amp; Scalability</b>			
5	Appliance should offer 40Gbps Firewall throughput & 20Gbps NGFW throughput (with enabling Firewall, IPS/Threat Prevention & AVC). This through-put must be under real world production Conditions.		
6	Should support 5 Gbps of IPSec VPN throughput and must support minimum 10000 VPN user.		
7	Firewall should support 8 Million concurrent sessions and 200K new connections per second.		
8	Firewall should support at least 1000 VLANs		
<b>Next Generation Firewall Features</b>			
9	Firewall should provide application detection for DNS, FTP, HTTP, SMTP,ESMTP, LDAP, MGCP, RTSP, SIP, SCCP, SQLNET, TFTP, H.323, SNMP		
10	Firewall should support creating access-rules with IPv4 & IPv6 objects simultaneously		
11	Firewall should support operating in routed & transparent mode		
12	Should support Static, RIP, OSPF, OSPFv3 and BGP		
13	Firewall should support manual NAT and Auto-NAT, static NAT, dynamic NAT, dynamic PAT		
14	Firewall should support Nat66 (IPv6-to-IPv6), Nat 64 (IPv6-to-IPv4) & Nat46 (IPv4-to-IPv6) functionality		
15	Firewall should support Multicast protocols like IGMP, PIM, etc		
16	Should support security policies based on security group names in source or destination fields or both		



S. No.	Minimum Specification from Day 1	Compliance (Y/N)	Product Doc. Reference
17	Should support capability to limit bandwidth on basis of apps / groups, Networks / Geo, Ports, etc		
18	The detection engine must be capable of detecting and preventing a wide variety of threats (e.g., malware, network probes/reconnaissance, VoIP attacks, buffer overflows, P2P attacks, zero-day threats, etc.).		
19	The solution must be capable of passively gathering information about network hosts and their activities, such as operating system, services, open ports, client applications, and vulnerabilities, to assist with multiple activities, such as intrusion event data correlation, elimination of false positives, and policy compliance.		
20	The solution must be capable of dynamically tuning IDS/IPS sensors (e.g., selecting rules, configuring policies, updating policies, etc.) with minimal human intervention.		
21	Should support Application Visibility and Control (AVC) supports more than 10000 application-layer and risk-based controls that can invoke tailored intrusion prevention system (IPS) threat detection policies to optimize security effectiveness.		
22	Proposed appliance should also provide Reputation- and category-based URL filtering offers comprehensive alerting and control over suspect web traffic and enforces policies on hundreds of millions of URLs in more than 50 categories		
23	The solution must provide a full-featured NBA capability to detect threats emerging from inside the network (i.e. ones that have not passed through a perimeter IPS). This includes the ability to establish “normal” traffic baselines through flow analysis techniques and the ability to detect deviations from normal baselines.		
24	The NBA capability must provide the option of supplying endpoint intelligence to the IPS for correlation against intrusion events to aid in event impact prioritization.		
25	The solution shall provide on-premise based sandbox technology where the objectionable content may be executed and inspected. On-premise Malware Behaviour Analysis appliance/Sandbox Solution should have integrated redundant power supply and mini-mum of 2 x 10 ports with populated transceivers as per design requirement.		
	<b>High-Availability Features</b>		

S. No.	Minimum Specification from Day 1	Compliance (Y/N)	Product Doc. Reference
26	NG Firewall should support Active/Active or Active/Standby failover.		
27	Firewall should support ether channel or equivalent functionality for the failover control & data interfaces for provide additional level of redundancy		
28	Firewall should support redundant interfaces to provide interface level redundancy before device failover		
29	Firewall should support ether channel or equivalent functionality for the failover control.		
	<b>Management</b>		
30	The management platform must be accessible via a web-based interface.		
31	The management platform must provide a highly customizable dashboard.		
32	The management platform must be capable of integrating third party vulnerability information into threat policy adjustment routines and automated tuning workflows		
33	The management platform must be capable of role-based administration, enabling different sets of views and configuration capabilities for different administrators subsequent to their authentication.		
34	Should support REST API for monitoring and config programmability		
35	The management platform must provide multiple report output types or formats, such as PDF, HTML, and CSV.		
36	The management platform must support multiple mechanisms for issuing alerts (e.g., SNMP, e-mail, SYSLOG).		
37	The management platform must provide robust reporting capabilities, including a selection of pre-defined reports and the ability for complete customization and generation of new reports.		
38	The management platform must risk reports like advanced malware, attacks and network		
39	The management platform must include an integration mechanism, preferably in the form of open APIs and/or standard interfaces, to enable events and log data to be shared with external network and security management applications, such as Security Information and Event Managers (SIEMs), and log management tools.		

### 5.3.7 End Host Anti – Virus

S. No.	Minimum Technical Specification	Compliance (Yes / No)
1.	AV Solution: Should have critical components for total security on the endpoint. (Antivirus, Antimalware, Vulnerability protection, Firewall, Device control & Virtual Patching.) in Box License supporting 100 nodes.	
2.	Personal Firewall: Firewall should block unwanted traffic, prevents malware from infecting endpoint systems, and makes them invisible to hackers.	
3.	Program Control with Program Advisor: Program Control ensures that only legitimate and approved programs can run on the endpoint. Program Advisor is a real-time Vendor knowledge base of over a million trustworthy applications and suspected malware used to automatically set the Program Control configuration.	
4.	Heuristic virus scan: Should Scan files and identifies infections based on behavioral characteristic of viruses	
5.	On-access virus scan: Should Scan files as they are opened, executed, or closed, allowing immediate detection and treatment of viruses	
6.	Deep scan: Should Scan Runs a detailed scan of every file on selected scan targets	
7.	Scan target drives: Should Specifies directories and file types to scan	
8.	Scan exclusions: Should Specify directories and file extensions not to be scanned	
9.	Treatment options: Should Enables choice of action agent should take upon detection of virus: Repair, rename, quarantine, delete	
10.	Intelligent quick scan: Should Check the most common areas of the file system and registry for traces of spyware	
11.	Full-system scan: Should Scans local file folders and specific file types	
12.	Deep-inspection scan: Should Scan every byte of data on the computer	
13.	Scan target drives: Should Specify which directories and file types to scan	
14.	Scan exclusions: should Specify directories and file extensions not to be scanned	
15.	Treatment options: Should Enable choice of action agents should take upon detection of virus: Automatic, notify, or confirm	

S. No.	Minimum Technical Specification	Compliance (Yes / No)
16.	Browser Security	
a.	Should Support latest versions leading web browsers i.e. IE, Mozilla, Chrome, Safari etc.	
b.	Endpoint security solution should provide vulnerability protection, which should scan the machine and provide CVE number visibility and accordingly recommend rule for virtual patch against vulnerability.	
c.	Should Allow users the freedom to surf with full protection against malicious software that is automatically downloaded and phishing attempts	
e.	Should Support Signature & Heuristic Phishing Protection	
f.	Should Support Site Status Check	
g.	Should Support Centralized Browser Security Policy Management	
h.	Should Support Centralized Browser Security Event Logging & Reporting	
17.	Management Platform Support	
a.	Support for latest Windows and Linux Platform	
b.	Support for latest Windows Server and Linux Server Platform may be opted	
c.	Client Platform Support	
d.	Should support Windows 8, 10 (32 & 64 bit), Mac	
18	Should be able to integrate with proposed NGFW/Anti-APT/Malware Behaviors Analysis/Sandbox solution.	

### 5.3.8 Load Balancer with Web Application Firewall

S. No.	Minimum Specification	Compliance (Yes/No)
1	It should be dedicated Appliance based solution with purpose-build hardware and the solution should not be a part of Router or UTM or NGFW.	
2	Minimum 4 nos. of 10 Gig Ethernet ports with required SFP+ multimode transceivers and separate port for management The appliance should have minimum 20 Gbps of Layer 7 throughput, 10 Gbps of SSL throughput, 20K SSL TPS (RSA 2K), 14K ECC TPS (ECDSA P256)	
3	Appliance should have minimum 4M Concurrent Sessions & 100K new sessions/sec	
5	Should support inbound/outbound load balancing, server load	

S. No.	Minimum Specification	Compliance (Yes/No)
	balancing and SSL offloading	
7	Load Balancing methods - Round Robin, Least Connections, Weighted RR, Weighted LC, Fastest Response, etc.	
8	IPv4 and IPv6 dual stack from day one, Layer 4 and Layer 7 Server Load Balancing, High Availability – Active-Active Standby configuration, Global Server Load Balancing, Next Hop Load distribution, Database Load Balancing, Support TCP and UDP applications, Perform ‘TCP Multiplexing’, ‘TCP Optimization’ functions.	
9	Minimum 10 virtual instances/ virtual routing domains with additional software license on same platform. The proposed solution shall have capability to dedicate hardware resources including CPU, memory, network. Bidder may propose alternate solution to meet the desired requirement of resource allocation.	
10	Should have separated environment for – i) viewing resources. ii) configuration and management. Bidder may propose alternate solution to meet the requirement.	
11	Web Application Firewall - Handle OWASP Security Attack Classification, WAF should support for IPv4 and IPv6 traffic, Support DNSSEC functionality,	
12	SNMP v2 and v3 support, Integration with SIEM, Support for LDAP/TACACS+ /RADIUS	
13	The solution should have integrated/external reporting solution	
14	The appliance should have Redundant Power Supply	
15	Application Level DDoS prevention	

### 5.3.9 SIEM solution

S. No.	Minimum Requirement	Compliance (Y/N)
1.	SIEM and Forensics Platform is required for complete visibility to identify and investigate attacks, the ability to detect and analyze even the most advanced of attacks before they can impact critical data, and the tools to take targeted action on the most important incidents. Complete visibility across logs, packets and end point is critical. Appliance based solution for better performance is required. The solution should collect, analyze, and archive massive volumes of data at very high speed using multiple modes of analysis. The platform should also be able to ingest threat intelligence about the latest tools, techniques and procedures in use by the attacker community to alert government on potential threats that are active.	
2.	Next generation platform should encompass log, packet and end point data with added context and threat Intelligence. Should provide complete network visibility through deep packet inspection high speed packet capture and analysis.	
3.	SIEM for Logs and deep packet inspection can be from different OEM but should be manageable from same console	
4.	The solution should be a physical appliance form factor with following components: a. Management & Reporting b. Normalization and Indexing c. Correlation Engine d. Data Management	
5.	There should be no limitation on number of devices to be supported. Any addition in no. of devices should have no cost impact on department.	

S. No.	Minimum Requirement	Compliance (Y/N)
6.	The SIEM & Log Monitoring solution should be from a different OEM than the Prevention Security solutions like FW, IPS, HIPS, AV, DLP, and Encryption.	
7.	The solution should provide an integrated SOC dashboard and Incident analysis system that could provide a single view into all the analysis performed across all the different data sources including but not limited to logs and packets. The Tool should have role-based access control mechanism and handle the entire security incident lifecycle.	
8.	Real time contextual information should be used at collection/normalization layer and be available at correlation layer where any events are matched during correlation rule processing. In addition, solution must provide contextual Hub at investigation layer for all relevant contextual awareness data regarding alerts/incidents available for any information asset like IP/Device etc.	
9.	All logs that are collected should be studied for completeness of information required, reporting, analysis and requisite data enhancement; normalization should be performed to meet the reporting and analysis needs.	
10.	A solution should support minimum 10,000 EPS and scalable up to 20,000 EPS.	
11.	Correlation Engine appliance should be consolidated in a purpose build appliance and should handle 20,000 EPS.	
12.	The solution should incorporate and correlate information that enables the Information Security Team to quickly prioritize its response to help ensure effective incident handling.	
13.	The solution should be storing both raw logs as well as normalized logs. The same should be made available for analysis and reporting. The proposed solution should be sized to provide both raw logs and normalized logs with minimum 20 TB of storage.	

S. No.	Minimum Requirement	Compliance (Y/N)
14.	The monitoring should be cross device and cross vendor and be both out of the box and scalable to cover additional devices and applications as required	
15.	Should be managed and monitored from SIEM unified console for Correlation, Alerting and Administration	
16.	Should be able to provide complete packet-by-packet details pertaining to one or more session of interest including Session replay, page reconstruction, image views, artefact & raw packet and object extractions.	
17.	Should be able to filter the captured packets based on layer-2 to layer-7 header information.	
18.	Should provide comprehensive deep packet inspection (DPI) to classify protocols & application.	
19.	The proposed solution must be able to provide the complete platform to perform Network forensics solutions.	
20.	The solution must be able to detect malicious payload in network traffic <ul style="list-style-type: none"> <li>• Detect and reconstruct files back to its original type</li> </ul>	
21.	The solution must have the ability to capture network traffic and import PCAP files using the same infrastructure.	
22.	Bidder should propose separate hardware for SIEM solution.	

Bidder should include the hardware and software required to complete the proposed – SIEM solution without any additional cost.



### 5.3.10 Authentication, Authorization and Accounting – Network Access Control (AAA – NAC)

Requirements	Description
General Requirements	Provide an easy-to-use BYOD ready granular secure access control solution that is context aware, identity enabled, location and device based. The proposed solution must combine Authentication, Authorization, and Accounting (AAA); Posture; Profiling; and Guest Access management services on to a single platform with a minimum endpoint footprint and supports the ability to be managed from a single management console.
Profiling / Visibility	The proposed NAC solution should be able to detect both new and existing endpoints and categorizes them based upon the type of endpoint (Ex: Windows, Printer, Network Device, IP Camera, Android, iPad, etc)
	Support the profiling of Android & iOS mobile devices, with the ability to detect: - - Manufacturer / Model - OS Type / Version - IMEI Identifier - Serial Number - Installed Applications
	The proposed NAC solution must support network- based profiling by targeting specific endpoints (based on policy) for specific attribute device scans, resulting in higher accuracy and comprehensive visibility of what is on your network
	The proposed solution should profile devices that uses MAC Authentication, 802.1X and SNMP protocol
	The proposed NAC solution should provide support for discovery, profiling, policy-based placement, and monitoring of endpoint devices on the network all within the same appliance
	The proposed NAC solution must support Profiling via SNMP, DHCP fingerprinting, HTTP-agent, NMAP, RSPAN, CDP, LLDP, WMI
	The proposed NAC solution must provide the ability to create custom profiling rules

Requirements	Description
	The proposed NAC solution must provide flexible filtering capabilities to sort out device information based on different attributes (e.g. MAC address, Manufacturer name, hostname, IP address, etc.)
	The proposed NAC solution should produce a real-time endpoint discovery with detailed information including which switch port the device is connected.
	The proposed NAC solution must provide device inventory in CSV exportable format.
	The proposed NAC solution must provide information on how many devices are not profiled, how many devices are newly seen in day/week/month, etc.
Role-based Access / Enforcement	The proposed NAC solution shall include the following key components: a) RADIUS server; b) NAC client agents; c) Policy Manager; d) Enforcement Manager; g) Integration Interfaces.
	The proposed NAC solution must be capable of supporting 802.1X authentication and shall work with endpoint devices (supplicant) and network devices (authenticator) that are enabled for IEEE 802.1X authentication.
	The proposed NAC solution must be capable of supporting SNMPv1/v2c/v3 enforcement and shall work with endpoint devices (without 802.1x supplicants) and network devices that are enabled SNMP to send traps to NAC server.
	The proposed NAC solution must make use of alternate authentication methods such as MAC address authentication or web authentication to authenticate endpoint devices that do not support 802.1X authentication
	The proposed solution NAC must support following credentials for authentication: a) User ID and password; b) Digital certificates only; c) Combination of User ID and password and digital certificates; or d) Combination of User ID and password and hardware token.
	The proposed NAC solution should integrate with multivendor Switches and Wireless Controllers to support enforcement actions such as Switch port Block Assign to VLAN and Port ACL on non-compliant / unknown users.

Requirements	Description
Clients	The proposed solution NAC must enforce security policies by blocking, isolating, and repairing noncompliant machines in a quarantine area without needing administrator attention. Once the user's machine is remediated, the user's machine shall be redirected automatically to the assigned network segment for access to the Site resources and the services that they are granted access.
	The proposed NAC solution when deployed without an agent must also be able to achieve enforcement of security policies by blocking, isolating, and repairing noncompliant machines in a quarantine area without needing administrator attention. Once the user's machine is remediated, the user's machine shall be redirected automatically to the assigned network segment for access to the Site resources and the services that they are granted access.
	The proposed NAC solution must be able to remotely install agents to corporate hosts without end-user interaction
	The proposed NAC solution must support automated provisioning and deployment clients remotely
	The proposed NAC solution must support a Unified NAC client shall support both NAC and VPN functionality.
	The NAC client must support installation onto the following operating systems: Microsoft, Mac OS, Android, iOS
	The proposed NAC solution should support clientless user access
Customized Device Templates	The proposed NAC solution should allow administrators to create their own device templates. These templates can be used to automatically detect, classify, and associate administrative-defined identities when endpoints connect to the network
	The proposed NAC solution should allow administrators can also associate endpoint-specific authorization policies based on device type
	The proposed NAC solution must allow administrators have the ability to encrypt and tunnel all communications channels for sensitive endpoints
Authentication Protocols	The proposed NAC solution must support the following authenticating protocols:
	Supports PAP, MS-CHAP, MS-CHAP-V2, EAP-MD5-Challenge, EAP-MS-CHAP-V2
	(EAP)-MD5

Requirements	Description
	Protected EAP (PEAP)
Guest Management	EAP-Transport Layer Security (TLS)
	EAP Generic Token Card (EAP-GTC)
	EAP State of Health (EAP-SOH)
	The proposed NAC solution must provide complete guest lifecycle management by allowing non-IT employees to provide controlled access to guests and consultant reducing the IT workload
	Guest management portal shall support self-onboarding for Guest/Contractor or Employees BYOD devices.
	Guest management portal shall support customizable guest web pages
	Guest registration shall support multiple credential notification methods (SMS, Email, webpage, etc.)
VPN	The proposed NAC solution must have the capability to support interfacing and integration with an IPsec or Secure Sockets Layer (SSL) virtual private network (VPN).
	The proposed NAC solution must allow Customer to: a) Apply to VPN connections the same access control policies as those for wired and wireless LAN; or b) Define a new set of access control policies that apply only to VPN connections.
Session Federation	The proposed solution should have an option to enable session migration between NAC and SSL Sessions in future for Seamless user experience accessing corporate resources from Home, Public or corporate Network
Eco-system Integrations	The proposed NAC solution should integrate with next-generation Firewalls (Palo Alto Networks, Fortinet, Checkpoint, Juniper SRX, etc.)
	The proposed NAC solution should integrate with MDM vendors (Airwatch, MobileIron, etc.)
	The proposed NAC solution should integrate with SIEM vendors (Splunk, IBM Q1Radar, Archsight, etc.)
	The proposed NAC solution should integrate with Identity providers (Duo, RSA, etc.)
	The proposed NAC solution should support enforcement through different switches (Cisco, Juniper, HP, etc.)
	The proposed NAC solution should support enforcement through different WLCs (Cisco, Aruba, Ruckus, etc.)

Requirements	Description
	The proposed NAC solution should support Active Directory server
	The proposed NAC solution should support Standards-Based LDAP server
Regulatory Compliance	The proposed solution must comply to the following industries recognized certifications: PCI-DSS FIPS-2 NDcPP
Redundancy Support	Support 1+1 High Availability Configuration with options for Hot Stand-by and Active/Active redundancy
Monitoring and Reporting	Support built-in monitoring, reporting, and troubleshooting console to assist helpdesk operators and administrators streamline operations
	NAC GUI should support Dashboard with contextual information (compliance, number of users, devices, etc.)
	NAC GUI should support Wizards for ease of configuration
	NAC GUI should support historical data on contextual information
Centralized Management System	The network access control policies should be managed and have the capability to be pushed down configuration centrally.
License Management System	The proposed solution should have a centralized license management system with capability to lease licenses to different appliances from a central pool
Platform Hardware	The proposed solution must be a purpose built 1U 19" rack-mountable appliance
	The proposed solution must support at least 8GB of RAM
	The proposed solution must support at least 500GB of Hard Disk Capacity
	The proposed solution must support at least 2 x 10/100/1000 GB Ethernet Copper Traffic Ports
	The proposed solution must support a 1 x 10/100/100 GB Dedicated Management port
	The proposed solution must support a dedicated RJ-45 Serial Console port
	The proposed solution must support at least 8,000 concurrent NAC users/devices in a single box

Requirements	Description
	<p>The proposed appliance must conform to the following Safety, EMI and EMC Certifications:</p> <p>USA: TuV SUD  Canada: TuV SUD European Union CE  Worldwide IEC 60950 CB Scheme Japan VCCI</p>
	<p>The proposed solution shall have the option to run virtually on:</p> <p>VMware  Kernel-based Virtual Machine (KVM) Hyper-V</p>
Software and Support Maintenance	<p>The proposed solution should have the options of RTF (Return to Factory), ND (Next Day), SD (Same Day) support directly from the OEM as part of its general support offerings and RMA should be from the OEM depots in country</p>
	<p>3 years OEM comprehensive Onsite Warranty and support for both hardware and software (24x7).</p>
	<p>Proposed solution should have 7 years of EOS (End of Support)/EOL (End of Life) from the date of UAT</p>

### 5.3.11 Storage Specifications

#	Parameters	Minimum Specifications	Bidder Compliance (Yes/No)	Product Documentation Reference
1	Make	<to be provided by the bidder>		
2	Model	<to be provided by the bidder>		
3	Solution/ Type	a) Storage Solution with NSPoF (No single point of failure) Architecture. The architecture should allow modular upgrades of hardware and software for investment protection. The system must support 12 Gbps SAS Disk Drives (Latest Drive interface) and SATA/NL-SAS Disk Drives (latest Drive interface).		
		b) Protocol Support - CIFS/SMB/ NFS/iSCSI/FC		
		c) If bidder is offering FCoE based solution, corresponding ports must be present in server as well as storage controller.		

#	Parameters	Minimum Specifications	Bidder Compliance (Yes/No)	Product Documentation Reference
4	Capacity	<p>a) Storage should be offered with minimum 3 PB usable capacity. (Primary- for 30 Days + 5 PB for 90 Days Secondary Flagged Data)</p> <p>b) Solution should have support for a minimum of Deployment more than 10 PB usable capacity.</p>		
5	Storage	a). Storage Capacity should be as per Overall Solution Requirement (usable, after configuring in offered RAID configuration)		
		b). Should support various RAID levels (0, 1, 6, 10/DP or equivalent)		
		c) Primary Storage – 3000TB or higher as per design requirement for 30 days backup. AND Secondary Storage – 5000TB or higher as per design requirement for 90 days backup.		
		d) .To store all types of data (Data, Voice, Images, Video, etc)		
		e). Should support disaster recovery mechanism natively The OEM should provide an undertaking that the pro-posed Storage solution should be able to capture data for the complete surveillance solution from day 1, as re-quired in the RFP.		
		f). Should be able to scale out without service interruption		
		g). Application and user must not be affected with underlying storage system's change		
		h). Storage should support automated tiering feature		
		i). Proposed Storage System should be scalable (vertically/horizontally) and		

#	Parameters	Minimum Specifications	Bidder Compliance (Yes/No)	Product Documentation Reference
		Solution should be elastic - can expand and shrink capacity based on demand.		
		j). The OEM should provide an undertaking that the proposed Storage solution should be able to capture data for the complete surveillance solution from day 1, as required in the RFP.		
6	Hardware Platform	a) Rack mounted form- factor		
		b) Modular design to support controllers and disk drives expansion. c) Support both IPv4 and Ipv6 d) Should have minimum of 8x10/40 Gbe or 8x16Gb FC Host ports. e) Storage shall have minimum front-end support for 16 Gb and backend support for minimum 12 Gb.		
7	Redundancy and High Availability	a) 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		
8	Management software	a) 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.		
		b) 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, up to max capacity of the existing controller/units.		
		c) A single command console for entire storage system.		
		d) Should also include storage performance monitoring and management software		



#	Parameters	Minimum Specifications	Bidder Compliance (Yes/No)	Product Documentation Reference
		e) Should provide the functionality of proactive monitoring of Disk drive and Storage system for all possible disk failures		
		f) Should be able to take "snapshots" of the stored data to another logical drive for backup purposes		
9	O/S Support	a) Support for multiple Operating Systems connecting to it, including of Windows and Linux		
		b) Warranty: 5 Years 24 X 7 Support with NBD Part Replacement comprehensive warranty.		
		c) The bidder should propose complete BoM with part codes of sub-components, warranty, license, subscription etc. for 5 years.		
		d) The OEM should be available in India Market for last 5 years		
		e) The OEM should have Service Center in Eastern part of India		
		f) The OEM should have TAC support in India		
		g) Any other components required to fulfill the Storage design requirement should be mentioned.		

**Note:** - For Secondary Storage, specification of Primary Storage may be considered changing the capacity to same or higher TB.

### 5.3.12 Hyper Converged Infrastructure (HCI)

S. No.	Minimum Specification from Day 1	Compliance (Y/N)	Product Doc. Reference
<b>a</b>	Make: <to be provided by the bidder>		
<b>b</b>	Model: <to be provided by the bidder>		
<b>1</b>	<b>Solution features</b>		

S. No.	Minimum Specification from Day 1	Compliance (Y/N)	Product Doc. Reference
1.1	The solution should provide hyperconverged software that allows delivery of enterprise-class storage services using latest x86 server infrastructures without dependence on a separate Storage Area Network & associated component such as SAN Switches & HBAs.		
<b>2</b>	<b>Minimum Configuration.</b>		
2.1	The proposed HCI solution should support scalability up to 32 nodes in a single cluster .Each node should have dedicated redundant hot swap power supplies & cooling fans.		
2.2	a). The solution should have minimum adequate number of nodes with each node having latest generation Dual Intel Xeon Scalable 2.2 GHz 24 cores processors. Each HCI Node shall provide 768GB Memory with 64 GB DIMM modules. b). HCI Solution should provide usable storage (without considering deduplication & compression) capacity of 100TB using Enterprise hot swappable SSD drives. c). The solution should be offered with redundancy of Compute, Hard disk and Connectivity.		
2.4	Each converged Node shall be provided with appropriate cache capacity additional to usable storage.		
2.5	Documentary evidence should be submitted confirming the additional resources required for HCI operations to achieve the mentioned usable resources.		
2.6	Min. 40G uplink Bandwidth per Server Node.		
<b>3</b>	<b>Networking Integration &amp; Automation</b>		
3.1	The hyper-converged system should include Redundant network switches, each providing minimum 48 (10Gbps) ports per switch with redundant power supplies and cooling fans. Each Switch should provide 12*10Gps SFP+ ports or equivalent Bandwidth for uplink connectivity to external LAN switch.		
3.2	The HCI should support connecting to external 3rd party Storage (FC,ISCSI,NFS) into the HCI cluster for capacity expansion and ease of migration from existing environment to HCI.		
<b>4</b>	<b>Management</b>		
4.1	Single dashboard to manage virtual machines, network, storage, monitor performance and manage events & alerts.		

S. No.	Minimum Specification from Day 1	Compliance (Y/N)	Product Doc. Reference
4.2	The solution should support Single click non-disruptive rolling upgrades of HCI software and system firmware's. The solution should Track, report, and view trends for compute, storage and database metrics like CPU, memory, IOPs, latency, and Database Transaction etc.		
4.3	The HCI solution should have Automated call home capability in the event of critical server failure or thresholds that are crossed which could impact server performance or customer SLA.		
4.4	Proposed solution shall be able to Track and manage firmware versions ,display & report inventory across all proposed Servers.		
4.5	The management tool should be able to provide global resource pooling and policy management to enable policy based automation.		
<b>5</b>	<b>Storage Architecture</b>		
5.1	The HCI solution should provide Inline Deduplication & compression across all storage tiers. Any license, hardware required to achieve the same should be provided from day 1.		
5.2	Proposed HCI solution shall include licenses for Maximum expansion w.r.t Memory / Storage capacity from day 1.		
5.3	The HCI software should pool all HDDs from all the nodes in the cluster to present a single storage resource pool to all server nodes in the cluster. There should not be any dependence on data locality		
<b>6</b>	<b>Virtualization</b>		
6.1	The vendor must provide all features and license applicable in common available Hypervisor on day 1. No purpose built Hypervisor is allowed. Proposed solution should support heterogenous hypervisor environment viz. Hyper-V & VMware.		
6.2	Virtualization software shall provide a Virtualization layer that sits directly on the bare metal server hardware with no dependence on a general purpose OS for greater reliability and security		

S. No.	Minimum Specification from Day 1	Compliance (Y/N)	Product Doc. Reference
6.3	Virtualization software should have the provision to provide zero downtime, zero data loss and continuous availability for the applications running in virtual machines in the event of physical host failure, without the cost and complexity of traditional hardware or software clustering solutions. This option should be supported for up to 4 virtual CPU per virtual machine.		
6.4	the virtualization software should have Integration of 3rd party endpoint security to secure the virtual machines with offloaded antivirus, antimalware, firewall and hips solutions without the need for agents inside the virtual machines.		
6.5	Solution should include VM Management software. Provided Software shall also be able to manage existing VM inventory running on the same Hypervisor.		
6.6	The solution should be quoted with a software that continuously analyses workload consumption, costs and compliance constraints and automatically allocates resources in real-time.		
6.7	The solution shall support provisioning across multi-hypervisor (e.g.: VMware ESXi 6.5 or higher, Microsoft Hyper-V 2016 or higher, System Center 2016 or higher) virtual and public cloud environments.		
6.8	The solution should model what-if scenarios based on the real-time environment to accurately forecast capacity needs. Shall have the capability to install on multiple Hypervisor's like VMware & Hyper-V.		
7	<b>Support and Warranty</b>		
7.1	Overall solution support should be provided for 5 years. All connecting cables & SFP's shall be included.		

### 5.3.13 GIS Map for Guwahati City

SI shall be responsible for providing GIS map of Guwahati city which shall be a common platform across all the solutions including, City Surveillance, Smart parking, Smart Pole, other solutions implemented in Guwahati, etc. SI shall also be responsible for appropriate geo referencing & geo tagging on the map covering all relevant assets like bus stops, bus routes, street poles, high masts, traffic signals etc.

- a) GIS maps shall be comprehensive and detailed up to roads, houses and building level.
- b) Solution shall ensure that the GIS Map provides complete details of the city in various digital vector layers and allows for zoom in/out, searching, and retrieving information capabilities.
- c) GIS details procured shall include the following data with attributes:
  - i. Road Network.
    - o City Arterial Roads.
    - o Streets
  - ii. Administrative boundaries
    - o District and Sub District Boundary.
    - o Town Boundaries.
  - iii. Building footprints and names
  - iv. Points of Interest data to include:
    - o Health services (Hospitals, Blood Banks, and Diagnostics center, Ambulance Services, Other Medical Services, etc.)
    - o Community services (fire stations, police stations, banks, ATMs, post offices, educational facilities, Govt. Buildings etc.)
    - o Business Centres (Shopping malls, markets, commercial complexes etc.
    - o Residential areas (Apartments, housing societies etc.)
    - o Transportation (bus stops/Terminus, parking areas, petrol bunks, metro stations, seaports, airports etc.)
    - o Recreation facilities (Restaurants, theatres, auditoriums etc.)
    - o Other utilities such as travel and tourism facilities, religious places, burial grounds, solid waste locations etc.
    - o Local landmarks with locally called names.
  - v. Land-Cover
    - o Green areas
    - o Open Areas
    - o Water bodies
  - vi. Address layers (Pin code, Locality, Sub-locality, House numbers/names)
  - vii. Geo referencing of all the assets pertaining to the solutions as required shall be provided by the SI
  - viii. All data procured shall be imported into a central database.
  - ix. System Functionalities:
    - The system shall have capability to perform attribute or spatial queries on data from selected sources.
    - the system shall support Mobile platform, Android and Windows
    - the system shall support clipping and/or downloading of raster and vector data by authorized users.
    - the system shall support server-side Geo-processing
    - The application shall have standard and modern map navigation tools of pan and zoom.
    - the application shall support client requests to print the spatial data.

- the system shall be able to support industry-standard data types,
  - Industry-standard data formats, unlimited file size or database size, unlimited number of files or tables, and unlimited number of users.
  - the system shall support geo-coding and reverse geo-coding
  - The system shall allow the users to perform advanced spatial analysis like geo-coding, routing, buffering and attribute-based analysis.
  - The application shall have standard and modern map navigation tools of pan and zoom.
  - The system shall have the facility wherein the user can opt to view in 2D or 3D environment.
  - The system shall be compatible with Google Maps, Bing™ Maps, Micro Station, AutoCAD, MGE, FRAMME, G/Technology, ODBC source.
  - The System shall support hierarchical legends, and watermarks
  - The application shall allow users to view the data with different symbology styles like differentiating feature records based on attributes or types, dynamic label generation with conflict detection, and translucency of all raster data and area colour fill.
  - The system shall allow the user to find Address
  - The system shall be able to consume real-time enterprise published spatial data. It shall be able to consume the third-party published OGC web-services.
- x. Application shall be OGC compliant for database and shall provision conversion to other database formats.
- xi. GIS base maps shall be installed on work stations at City Operation Centre and City Operation center. GIS maps and data replication shall happen from central system remotely.
- d) Provide GIS engine that shall allow operators to get an overview of the entire system and access to all the system components dynamically. GIS engine shall enable dynamic view of the location and status of resources and objects/sensors. System shall enable authorized user to open a new incident and to associate the incident with its geographic location automatically, via GIS display.

#### **5.4 COMPONENT 4 – INTEGRATED TRAFFIC MANAGEMENT SYSTEM (ITMS)**

Integrated Traffic Management System primarily will have the following systems for Guwahati city.

- a) Adaptive Traffic Signal Control (ATSC)
- b) Traffic Violation Detection Systems (TVDS) with ANPR & RLVD Camera
- c) Speed Violation Detection System (SVD) – Radar based system

d) Traffic Enforcement & E-Challan System

### 5.4.1 Adaptive Traffic Signal Control (ATSC) System

ATSC is a traffic responsive system which uses real-time data on vehicular traffic to optimize traffic signal settings and reduce vehicle delays, queue length of vehicles at the junctions/ intersections in order to enhance capacity and efficiency of the road network. Key benefits envisaged from installation of ATSC include:

- a) Reduce vehicular delays and related greenhouse gas emissions
- b) Improve operational planning, efficiency and capacity of road network
- c) Improve Incident Management System by creating green corridors through pre-emption and priority for emergency and special vehicles

#### 5.4.1.1 Indicative Solutions Architecture - Adaptive Traffic Signal Control (ATSC) System

The sections below highlight the key elements proposed in the smart solution and overall the process flow and high-level functionality of each hardware and software elements of the solution. The high-level schematic diagram of the proposed solution architecture for the ATSC project is presented below.

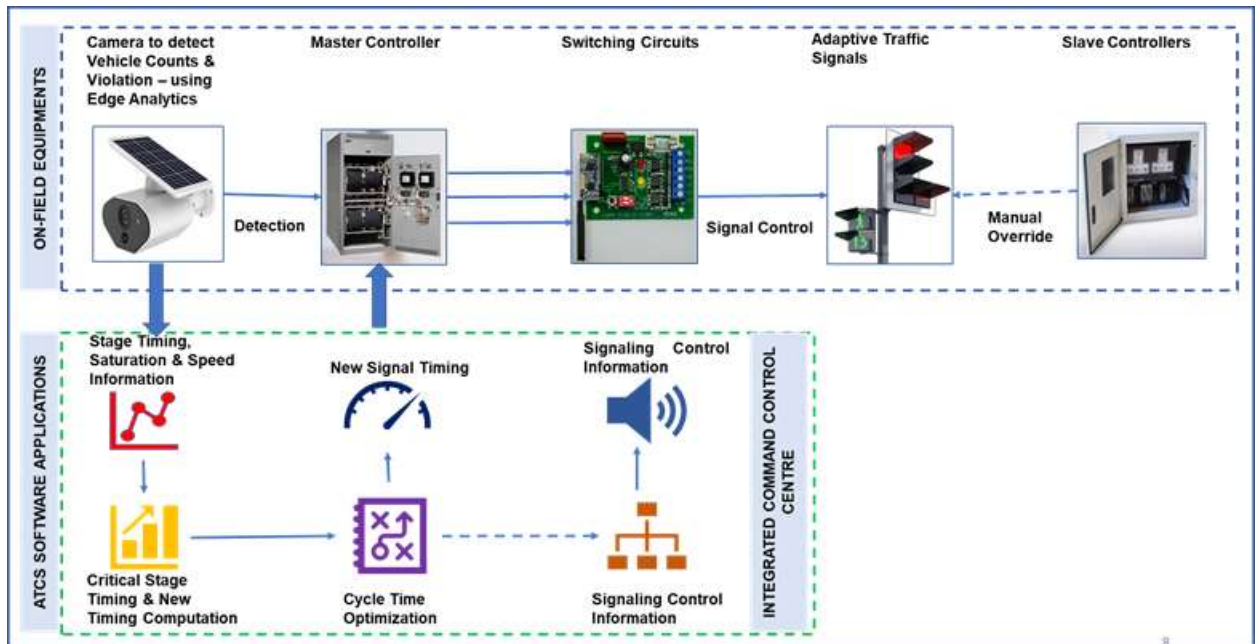


Figure 3 : Indicative Solutions Architecture - ATSC

#### **5.4.1.2 Functional Requirements of Adaptive Traffic Signal Control (ATSC)**

- A. The system would be used to monitor and control traffic signals, including signalized pedestrian crossings, using a traffic responsive strategy based on real time traffic flows obtained using vehicle presence sensors.
- B. All signal controllers under Adaptive Traffic Control System shall be provided with inputs from non-intrusive vehicle detection sensors/ cameras for detecting demand and communications equipment to send the demand data and to receive instructions on the control strategy in near real-time.
- C. The system should be scalable to add more signals whenever required.
- D. Any existing infrastructure at the junctions that might help in traffic control, where possible, should be integrated with ATSC.
- E. Adaptive traffic signal controller managed through the central traffic control centre at an individual junction or as part of group of traffic junctions along a corridor or a region for controlling the traffic signals deployed
- F. SYSTEM INTEGRATOR has to implement all the field infrastructure to support all Traffic and Pelican signals for long term sustainability and for all required instruments to support ATSC, not mentioned in RFP is in the scope of System Integrator implementation.
- G. Camera based vehicle detectors to assist operation of traffic signal controller and generate counts, demands and extensions for right-of-way for identifying optimal signal timings.
- H. The ATSC communication network shall enable remote monitoring and management of the intersection and provide for transmission of real-time data {i.e. Road Traffic Collision (RTC) time, stage timing, mode, events, etc.} from the traffic signal controller to the central computer in the Integrated Command and Control Center (ICCC).
- I. The central computer running the ATSC application shall send optimum signal timings to all intersections in the corridor leveraging the communication network.
- J. “Composite Signal Control Strategy” application (already proved in Indian environment) or equivalent will be used for optimizing the traffic signal timings.
- K. ATSC should be able to sense the volume of the Traffic automatically at each of the junction movement nodes through the means of camera algorithms and AI analytics



- L. ATSC should be able to control the Traffic signal to give way to the side of the traffic with high volumes.
- M. The system should have a provision of a manual override in case of use by the Traffic Police personnel in case of special VIP movement and system failures.
- N. The ATSC shall operate in real time with the capacity to calculate the optimal cycle times, effective green time ratios, and change intervals for all system traffic control signal controllers connected to it. These calculations shall be based on assessments carried out by ATSC application software, running on the Central computer based on data gathered by vehicle detectors. Key functionalities of the software application shall include:
  - I. Propose timing plans to every intersection under the ATSC in every Cycle.
  - II. Verify the effectiveness of the proposed timing plans in every cycle.
  - III. Identify Priority routes.
  - IV. Synchronize traffic in the Priority routes.
  - V. Manage and maintain communication with traffic signal controllers under ATSC.
  - VI. Maintain database for time plan execution and system performance.
  - VII. Maintain error logs and system logs.
  - VIII. Generate Reports on request.
  - IX. Graphically present signal plan execution and traffic flow at the intersection on desktop.
  - X. Graphically present time-space diagram for selected corridors on desktop.
  - XI. Graphically present network status on desktop.
  - XII. Make available the network status and report viewing on Web.
- O. Pedestrian Actuated Traffic Control Signals at places where a large number of people cross the road with heavy vehicular traffic (near Schools, Hospitals, Shopping Centers, places of worship and similar other establishments).
- P. The pelican signals shall be installed on two diagonally opposite corners of the Zebra Crossing and shall be supported with facilities for the pedestrians to actuate traffic signal control.
- Q. ATSC shall use UG405 or NTCIP or any other standard communication protocol. It should also provide the functionality of integration with on-ground hardware of any third-party traffic controller that is UG405 or NTCIP or any other standard communication protocol compliant.

#### **5.4.1.3 ATSC Software Application**

Objective of the ATSC would be to minimize the stops and delays in a road network to decrease the travel time with the help of state-of-the-art technology. The adaptive traffic control system shall operate in real time with the capacity to calculate the optimal cycle times, effective green time ratios, and change intervals for all system traffic signal

controllers connected to it. These calculations shall be based up on assessments carried out by the ATSC application software running on a Central Computer based on the data and information gathered by vehicle detectors at strategic locations at the intersections controlled by the system.

The ATSC application software shall do the following:

S. No.	Minimum Requirements	Bidder Compliance (Yes/No)	Product Documentation Reference
	Make		
	Model		
1	Identify the critical junction of a corridor or a region based on maximum traffic demand and saturation. For this purpose, identify the vehicles standing in the queue on the junction based on their presence on stop line using vehicle detectors and then optimize its timing to reduce the queue formation by capturing required data from Vehicle Detectors for ATSC functionality.		
2	The system shall have a distributed architecture of sub-systems and structured so that signalized junctions can be appropriately grouped into sub-areas or sub-systems (minimum 2 and up to 250). Sub-areas are to be controlled by a regional computer.		
3	Up to 100 users should be able to connect to the central ATSC system and up to 30 users to regional computer controlling sub-systems with varying levels of security and access at the same time the proposed ATSC system shall be scalable to include any additional junctions in the future.		
4	The critical junction cycle time shall be used as the group cycle time i.e. cycle time common to all intersection in that corridor or region.		
5	Stage optimization to the best level of service shall be carried out based on the traffic demand.		
6	Each junction operated as part of the System shall exist in one of three states, namely offline (OF), on-line Local (LO) or computer control (CC). Example of LO is cable-less linking and OF is semi-actuation or full actuation.		

S. No.	Minimum Requirements	Bidder Compliance (Yes/No)	Product Documentation Reference
7	When a junction is in the LO state, it shall be monitored and tested for correct operation and may be picked up by command for computer control (i.e., to the CC state). Monitoring activities shall be performed in a manner consistent with controller type and operating software requirements. The LO state can result from a local activity (e.g., preempt), operator directed activity, scheduled activity or system detected failure condition.		
8	Cycle optimization shall be carried out by increasing or decreasing the common corridor cycle time based on the traffic demand within the constraints of Minimum and Maximum designed value of cycle time. It shall use vehicle presence data provided by vehicle detector and Degree of Saturation for Cycle Length optimization.		
9	Offset correction shall be carried out to minimize number of stops and delays along the corridor for the priority route. Offset deviation measured using distance and speed between successive intersections shall be corrected within 5 cycles at a tolerance of +/- 5 seconds maximum.		
10	The system shall have provision to configure priority for upstream signals as default. The ATSC software shall continuously check the traffic demand for upstream and downstream traffic and assign the priority route to the higher demand direction.		
11	Develop appropriate stage timing plans for each approach of every intersection under the ATSC, based on real time demand		
12	In order to achieve coordination, subsystems operating on the same cycle time should have the provision to be linked so that a defined offset exists between the subsystems. This offset shall be defined as the number of seconds between the zero point of one subsystem and the end of a stage of a specified junction in the other subsystem. Linked subsystems must share the same subsystem cycle time but any or all the junctions in any subsystem may be specified to "double cycle".		

<b>S. No.</b>	<b>Minimum Requirements</b>	<b>Bidder Compliance (Yes/No)</b>	<b>Product Documentation Reference</b>
13	When a link is established between two subsystems, the cycle generator of the subsystem linking is speeded up or slowed down (i.e. the cycle time of the subsystem is increased or decreased) until the specified relationship between the two subsystems is achieved. If a junction in a subsystem is required to change its grouping frequently depending on traffic conditions, it should be dynamically linked or delinked with other subsystems.		
14	Propose timing plans to every intersection under the ATSC in every Cycle		
15	Shall include algorithm(s) which shall adjust the signal timing parameters.		
16	Verify the effectiveness of the proposed timing plans in every cycle		
17	Identify Priority routes and Synchronize traffic accordingly.		
19	Manage and maintain communication with traffic signal controllers under ATSC		
20	Shall be able to control & manage the traffic merging from highways to the city and vice versa using dedicated techniques.		
21	Maintain database for time plan execution and system performance and data should be made available to city planners for planning city traffic.		
22	Maintain error logs and system logs and generate desired reports.		
24	Graphically present signal plan execution and traffic flow at the intersection on desktop		
25	Graphically present time-space diagram for selected corridors on desktop		
26	Graphically present network status on desktop		
27	Make available the network status and report viewing on the desktop GUI as per RFP		
28	The ATSC shall be fully integrated with ICC platform to generate standard and custom reports for planning and analysis		
29	It shall be possible to interface the ATSC with a popular microscopic traffic flow simulation software for pre and post implementation analysis and study of the proposed ATSC control strategy		

S. No.	Minimum Requirements	Bidder Compliance (Yes/No)	Product Documentation Reference
31	Shall collect continuously information about current observed traffic conditions from a variety of data sources and of different kind (traffic states, signal states, vehicle presence) using vehicle detectors.		
34	Shall identify the traffic state with respect to current incidents in Real-time and traffic management strategies (e.g. traffic signal control or variable message displays), improving the decision- making capabilities of the operators even before problems occur.		
35	Shall calculate customizable Indicators to quickly assess the results		
36	Shall generate alerts to the operator that trigger on customizable conditions in the network (starting with simple drops in flow, up to total queue lengths along emission sensitive roads surpassing a definable threshold)		
37	Shall distribute both collected and calculated traffic information via a variety of communication protocols and channels, ensuring high interoperability degree and thus acting as a “traffic data and information hub”		
38	Shall provide calculated traffic flows and identify, queues and delays to Urban Control and Adaptive Signal Control Systems, allowing for proactive Traffic Management and Control		
39	Shall create a traffic data warehouse for all historic traffic information gathered from the hardware installed on the road network.		
40	Shall operate in real time that is continuously updating the estimates on the state of the network		
41	Shall operate the traffic lights with the adaptive traffic controls, based on the current traffic demand and the current incidents, thus optimizing the green waves continuously throughout the network		
42	The ATSC system shall be able to provide Ambulance / VIP / Fire brigade vehicles the priority in crossing the junction.		

S. No.	Minimum Requirements	Bidder Compliance (Yes/No)	Product Documentation Reference
43	The ATSC system should be capable of route pre-emption capability without any additional pre-emption hardware. It shall be capable of being applied to a single junction or to a series of junctions to allow green wave Pre-emption, or special arterial traffic control strategies that might be required. Route Pre-emption shall be capable of being requested from any system workstation by authorized operators		
44	The ATSC system shall be capable of simultaneous two or more pre-emption plans for each emergency. In the event that two or more conflicting route Pre-emption requests are received (i.e., the routes contain the same junction), the first request shall be honored and all subsequent requests for conflicting routes shall be disallowed, with appropriate notification made to the request initiator.		
45	The ATSC Application shall provide for full access and editing capabilities of the Route Pre-emption plans from any workstation (provided that the user has an appropriate security access level). It shall be possible that, if necessary, the downloaded Route Pre-emption plan may be terminated any time before activation or during the operation of any Pre-emption plan via the System from any of the workstations with appropriate user security access level.		
46	For emergency management, ATSC should be able to accept commands from workstations deployed in select areas of route-preemption or emergency route management.		
47	It shall also be possible to integrate the RFID reader-based Transit Signal Priority System in the ATSC system in near future for identifying the buses & other vehicles of significance near the junction to providing priorities.		
48	The system shall be able to determine the priority order of each vehicle when there are multiple priority vehicles simultaneously present at a given junction, and accordingly determine which get the priority first.		
49	The priority can be given either as an extension to green stage or a forced switching to a green stage depending on the current state of the signal.		

<b>S. No.</b>	<b>Minimum Requirements</b>	<b>Bidder Compliance (Yes/No)</b>	<b>Product Documentation Reference</b>
<b>50</b>	The system shall also compensate the other stages for the lost green after the passage of the priority vehicle in order to minimize congestion.		
<b>51</b>	ATSC system shall be capable to integrate with a smart public transport priority respecting the delays for all road users. Emergency Vehicle Priority Emergency Vehicle Priority Provision to make way for emergency vehicles like fire, police and ambulances during emergencies.		
	<b>Admin features</b>		
<b>1</b>	User login – Operator authentication shall be verified at this screen with login name and password		
<b>2</b>	Traffic Flow Display – This online display shall indicate the current traffic flow with animated arrows, mode of operation, stage number being executed and elapsed stage time. It shall also display traffic counts from each of the approach of all the junctions.		
<b>3</b>	Saturation Snapshot – This display shall show the current saturation levels of all intersections in a corridor.		
<b>5</b>	Reports Printing / Viewing – This link shall allow selection, viewing and printing of different reports available under ATSC		
<b>6</b>	Time-Space Diagram – The time-space diagram shall display the current stages being executed at every intersection in a corridor with immediate previous history		
<b>7</b>	Junctions shall be plotted proportional to their distance on one-axis and time elapsed for the stage in seconds on another-axis.		
<b>8</b>	Junction names shall be identified with each plot		
<b>9</b>	Currently running stage and completed stages shall be identified with different colors.		
<b>10</b>	Stages identified for synchronization shall be shown in a different color.		
<b>11</b>	Speed lines shall be plotter for stages identified for synchronization to the nearest intersection in both directions.		
<b>12</b>	It should be possible to freeze and resume online plotting of Time-Space diagram.		
<b>13</b>	The system shall have other graphical interfaces for configuring the ATSC, as appropriate.		

S. No.	Minimum Requirements	Bidder Compliance (Yes/No)	Product Documentation Reference
14	The ATSC system applications proposed by the Implementation Agency should have open APIs and should be able to integrate and share the data with other third- party systems like ICCC.		
<b>Report Generation</b>			
1	System shall generate Corridor based and Intersection based reports. The application software shall generate the following reports, but not limited to the below. All the reports shall be possible for selected dates.		
2	Stage Timing report – The report shall give details of time at which every stage change has taken place. The report shall show the stage sequence, stage timings and stage saturation of all stages of all cycles for a day. The saturation is defined as the ratio between the available stage timings to the actual stage timing executed by the traffic signal controller for the stage (stage preemption time).		
3	Cycle Timing report – The report shall give details of time at which every cycle has taken place. The report shall show the cycle sequence and cycle timings for all the cycles in a day.		
	Stage switching report – The report shall give details of time at which a stage switching has taken place. The report shall show the stage sequence, stage timings and stage saturation for a day.		
4	Cycle Time switching report – The report shall give details of time at which a cycle switching has taken place. The report shall show the cycle sequence and cycle timings for the cycle in a day.		
5	Mode switching report – The report shall give details of the mode switching taken place on a day.		
6	Event Report - The report shall show events generated by the controller with date and time of event.		
7	Power on & down: The report shall show time when the master is switched on, and last working time of the master controller.		
8	Intensity Change – The report shall show the brightness of the signal lamp is changed according to the light intensity either manually through keypad or automatically by LDR with time stamp.		



<b>S. No.</b>	<b>Minimum Requirements</b>	<b>Bidder Compliance (Yes/No)</b>	<b>Product Documentation Reference</b>
9	Plan Change – The report shall show the time of change of plan either through keypad or remotely through a PC or Server.		
10	RTC Failure – The report shall show the time when RTC battery level goes below the threshold value.		
11	Time Update – The report shall show the time when the Master controller updated its time either manually through keypad, automatically by GPS or through remote server.		
12	Mode Change – The report shall show the time when Master controller's operating mode is changed either manually through keypad or a remote server. The typical modes are FIXED, FULL VA SPLIT, FULL VA CYCLE, FLASH, LAMP OFF and HURRY CALL.		
13	Lamp Status Report – The report shall show lamp failure report with date and time of failure, color of the lamp and associated phase		
14	Loop Failure Report – The report shall show the date and time of detector failure with detector number and associated phase.		
15	Conflict – The report shall show the conflict between lamps (RED, AMBER, GREEN) in the same phase or conflict between lamps with other phase.		
16	Corridor Performance Report – The report shall show the saturation of all the intersections in a corridor for every cycle executed for the corridor and the average corridor saturation for a day		
17	Corridor Cycle Time Report – The report shall show the Corridor cycle time, Intersection cycle time, Mode of operation and degree of saturation of all the intersections in a corridor for every cycle for a day		

#### 5.4.1.4 Traffic Signal Controller

<b>S. No.</b>	<b>Minimum Requirements</b>	<b>Bidder Compliance (Yes/No)</b>	<b>Product Documentation Reference</b>
	Make		
	Model		

S. No.	Minimum Requirements	Bidder Compliance (Yes/No)	Product Documentation Reference
1	Appropriate controller technology shall be chosen to provide the operational levels and accuracy as required for successful function of the ITMS system as per the SLAs defined.		
2	The Traffic Signal Controller will be controlled centrally on real time (adaptive) as an individual junction or as part of group of traffic junctions along a corridor or a region. The Signal Controller will be designed flexible to accept the required commands for its adaptive operation easily from Traffic command control Center.		
3	Traffic Signal Controller must be chosen to provide the accuracy as required for successful function of the ITMS system as per the SLAs defined,		
4	Appropriate controller technology shall be chosen to provide the operational levels and accuracy as required for successful function of the ITMS system as per the SLAs defined.		
5	The Traffic Signal Controller shall be capable of communicating with the ITMS server located at Data Center through Ethernet on a secured managed communication network.		
	<b>Separate panel shall be provisioned with Traffic Signal Controller to operate switches by Traffic Police / monitoring personnel with lock and key arrangements at Junction. This should provide below features:</b>		
6	i. Junction Off Switch shall put on and off signal lamp without violating any safety clearances.		
	ii. Auto / Manual switch shall enable /disable manual operation of the controller without interruption.		
	iii. Activating the pushbutton switch shall terminate the currently running stage (signal plan timetable) and start the next without violating safety clearance.		
	iv. Emergency switch shall force the controller to define any stages as per requirement like passages to emergency vehicles, without violating safety clearances.		
	v. Flash switch shall force the signal to flash Amber /Red.		
	<b>The Traffic Signal Controller shall have the following mode of operation:</b>		

S. No.	Minimum Requirements	Bidder Compliance (Yes/No)	Product Documentation Reference
7	Fixed Time: The cycle time remains constant in every cycle execution for a given time period in this stage. The stage timings shall be executed according to the Junction specific Time table stored / maintained in the traffic signal controller FLASH memory ignoring input from vehicle detectors.		
8	Vehicle Actuation with all stage's preemption: In this mode, the traffic signal controller shall execute stage timing as per demand from vehicle detectors within the constraints of minimum Green, Maximum Green running period for the stage and cycle time stored in the traffic signal controller FLASH memory. Preemption shall be possible for the demand actuated stages Cycle time may vary in every cycle execution.		
9	Semi Actuation: In this mode, the traffic signal controller shall execute stage timings in the vehicle actuated stages as per demand from vehicle detectors within the constraints of minimum Green, Maximum Green running period for the stage and cycle time stored in the traffic signal controller FLASH memory. All other stages shall execute the Maximum Green time configured for the stage. Preemption shall be possible for all demand actuated stages. Cycle time may vary in every cycle execution.		
10	Stage Skipping: In this stage, the traffic signal controller shall not execute the stage enabled for skipping when there is no vehicle demand registered for the stage till clearance amber time of the previous stage.		
<b>Vehicle Actuation with Fixed Cycle Length:</b>			
11	In this stage, the traffic signal controller shall execute stage timing as per demand from video-based vehicle detector within the constraints of Minimum Green, Maximum Green running period for the stage and Cycle time shall be maintained constant during a given time slot.		
12	Pre-emption for all demand actuated stages except for priority stage shall be possible.		
13	The system shall have true real-time adaptivity. Adapts to traffic present at this very instant (not only statistically)		
<b>Total TSS mode:</b>			

S. No.	Minimum Requirements	Bidder Compliance (Yes/No)	Product Documentation Reference
14	In This mode, the traffic signal controller shall execute stage timings as per demand within the constraints of Minimum Green, Maximum Green running period for the stage and Cycle time specified by the central computer during every cycle switching.		
15	Pre-emption for all demand actuated stages except priority stage shall be possible in this mode. The traffic signal controller shall identify a communication failure with the central computer within a specified time period. In such an event the signal plan timing shall be executed from the local timetable stored in the traffic signal controller FLASH memory.		
<b>Operating Parameters of Traffic Signal Controller</b>			
16	It shall be possible to operate the filter green (turning right signal) along with a vehicular phase. The filter green signal shall flash for a time period equal to the clearance amber period at time when operated with a vehicular phase. It shall be possible to configure any phase to the given lamp numbers at the site.		
17	Stages- The controller shall have facility to configure minimum 16 stages using major and macro stages.		
18	Cycle Plans - The controller shall have facility to configure 10 cycle plans and the Amber flashing / red flashing plan. It shall be possible to define different stage switching sequences in different cycle plans. The controller shall have the capability for a minimum of 20 cycle switching per day in fixed mode of operation.		
19	Day Plan – The controller shall have facility to configure each day of the week with different day plan. It shall also be possible to set any of the day plans to any day of the week. The controller shall have the capability to configure 20 days plans.		
20	Special Day Plans- The controller shall have facility to configure a minimum of 20 days as special days in a calendar year.		
21	Starting Amber - During power up the controller shall initially execute the Flashing Amber / Flashing Red plan for a time period 3 seconds to 10 seconds. The default value of this starting Amber is 5 seconds. Facility shall be available to configure the time period of starting Amber within the given limits at the site.		

S. No.	Minimum Requirements	Bidder Compliance (Yes/No)	Product Documentation Reference
22	Inter green – Normally the Inter-green period formed by the clearance Amber and Red extension period will be common for all stages. However, the controller shall have a facility to program individual inter green period from 3 seconds to 10 seconds.		
23	Minimum Green – The controller shall allow programming the minimum Green period from 5 seconds to 10 seconds without violating the safety clearances. It should not be possible to preempt the minimum Green once the stage starts commencing execution.		
24	All Red – Immediately after the starting Amber all the approaches should be given red signal for a few seconds before allowing any right of way as a safe measure. The controller shall have program ability of 3 seconds to 10 seconds for all Red signal.		
25	Signal lamps monitoring – The controller shall have inbuilt circuitry to monitor the lamp status.		
26	Green – Green conflict monitoring – The controller shall have a facility to list all conflicting phases at an intersection. The controller should not allow programming of these conflicting phases in a stage. A hardware failure leading to a conflict condition (due to faulty devices or short circuit in the output) shall force the signal into flashing Amber / Flashing Red.		
<b>Technical Specifications of Traffic Controller</b>			
1	a) Power supply: 230 V AC at 50 Hz or 24 VDC operated		
2	b) The Traffic Signal Controller equipment should be 32/64-bit micro controller solid state traffic signal lamp switching module		
3	c) Real time clock with facility to update from central server (accurate to plus or minus 100 milli seconds)		
4	c) Signal head compatibility: LED 230VAC or 24VDC with dimming of various intensity levels		
5	d) 32bit processor with 2 MB or more flash as nonvolatile storage, 256 KB or more as RAM, with a provision of adding minimum 32 GB through an external SD Card/USB.		
6	g) Controller clock frequency of min of 100MHz.		
7	h) Junction Off Switch		
8	i) Stages- The controller shall have facility to configure 16 stages.		

S. No.	Minimum Requirements	Bidder Compliance (Yes/No)	Product Documentation Reference
9	j) The controller shall have facility to configure 10 cycle plans and the Amber flashing / red flashing plan		
10	The Traffic Signal Controller equipment should be 64-bit micro controller solid state traffic signal lamp switching module with the ability to program any combination of traffic signal stages, phases, and junction groups with conflict monitoring facility.		
11	The Traffic Signal Controller shall have conflict monitoring facility to ensure that conflicting, dangerous triggers are pre-flagged at the programming stage are disallowed even during manual override phase.		
12	The Traffic Signal Controller shall have real time clock with facility to update from central server (accurate to plus or minus 100 milli seconds) i.e. ITMS server GPS and through manual entry.		
13	Signal head compatibility: LED 230VAC or 24VDC with dimming of various intensity levels. The system should be capable to achieve any levels of dimming		
14	Power supply: 230 V AC at 50 Hz or 24 VDC operated		
15	<b>Standards compliance:</b>		
	EN 50556/AS/NZS		
	ISO 9001:1994 for design & servicing.		
	AND		
	EN 12675/IEC 60068 for functional safety,		
	EN 55024:2010 & AS/NZS 60950/BS EN 61000-3-3 or equivalent for voltage fluctuations, or equivalent		
16	Number of signal groups: minimum 24 or as per site requirement		
17	Number of signal head outputs: minimum 72 or as required		
18	Number of signal plans: Up to 10 in fixed time and unlimited in ATSC mode		
19	Number of stages in signal plans: minimum 16 using major and macro stages.		
20	Number of detector inputs: min 16		
21	Interfaces: Ethernet, RS232, USB, 3G/4G		
22	Real time clock with facility to update from central server (accurate to plus or minus 100 milli seconds)		
23	Signal head compatibility: LED 230VAC or 24VDC with dimming of various intensity levels		

S. No.	Minimum Requirements	Bidder Compliance (Yes/No)	Product Documentation Reference
24	Controller clock frequency of min of 100MHz.		
25	Junction Off Switch		
26	Stages- The controller shall have facility to configure minimum 16 stages using major and macro stages		
27	Temperature range: 0 – 70 deg. C		
28	Humidity: 95% without condensation		

#### 5.4.1.5 Camera /Thermal Vehicle Detector

S. No.	Minimum Requirements	Bidder Compliance (Yes/No)	Product Documentation Reference
	Make		
	Model		
1	The vehicle detector equipment shall be interfaced with Traffic Signal Controller. The output of the same i.e. presence of vehicles shall be used to influence the operation of the traffic signal controller, generate counts, demands and extensions for right-of way.		
2	IA shall be responsible for the position of the detector (upstream, downstream, stop-line, exit etc.) for independent straight and right turn signals. It shall be capable to detect the vehicles with 90% accuracy for non-lane based mixed traffic flow conditions in all light & weather conditions including FOG & complete dark		
3	Vehicle detector that does not change its status at least once during a stage execution shall be notified to the Central server (in ITMS mode) at the termination of the associated stage.		
4	Vehicle Detector camera should look at approaching traffic and should work in FOG and dirt on sensor should not impact performance		

#### 5.4.1.6 Traffic Light Aspects

S. No.	Minimum Requirements	Bidder Compliance (Yes/No)	Product Documentation Reference
	Make		
	Model		
1.	It shall have less power consumption for all colors, preferably maximum power should not exceed 14 watts for each color.		
2.	Shall preferably have temperature compensated power supplies for longer LED life.		
3.	Shall have uniform appearance light diffusing.		
4.	All units operate at voltage of - 12 / 24 volts DC.		
5.	LED shall be single source narrow beam type with clear lens & Luminance uniformity.		
6.	IP Rating: IP65		
	<b>LED aspects</b>		
7.	Red, Amber, Green-Full (300 mm diameter):		
8.	Green-arrow (300 mm diameter):		
9.	Red, Green – Pedestrian (300 mm diameter):		
10.	Pedestrian-Red and Green		
	<b>LED Retrofit Specifications</b>		
11.	Power supply shall be preferably 230 Vac +/- 10% and frequency 50 +/- 5Hz		
12.	Standards: EN 12368 compliant		
13.	Convex Tinted Lens, Fuse and Transients shall be available		
14.	Operating Temperature Range: As per NOIDA weather conditions Turn Off/Turn ON Time: 75 milli seconds max		
15.	Total Harmonic Distortion: <20%		
16.	Minimum Luminous Intensity (measured at intensity point) (cd): Red 400, Amber 400, Green 400		
17.	Dominant Wavelength (nm): Red 630, Amber 590, Green 490		
18.	Lamp conflict compatibility system: Compatible with lamp failure and conflict detection		



#### 5.4.1.7 Automatic Traffic Counting and Classification System (ATCC) – Video / Thermal

S. No.	Minimum Requirements	Bidder Compliance (Yes/No)	Product Documentation Reference
	Make		
	Model		
1	The ATCC System shall primarily be installed at important junctions and mid-blocks in the city. The ATCC System shall help in continuous monitoring of the traffic conditions in the city. The following are the functional Requirements related to the ATCC System.		
2	The ATCC system shall be deployed on city road primarily on city's entry, exit and at major points of intersection in NOIDA, the objective of the sub-system is to collect traffic data at major points.		
3	The data from ATCC shall be used by various Government and private organizations to understand the existing traffic volume trends & patterns		
4	The ATCC data collected shall be used by various stakeholders for extensive planning and traffic engineering exercises across the road stretches		
5	The real-time traffic data can be shared with 3rd party map solution providers and online navigation systems as per the discretion of authority.		
6	The software and solution of ATCC shall comply with all functional and business requirement as specified in this RFP, elsewhere.		
7	The ATCC System shall use video based non-intrusive technology for counting and classifying the vehicles in a real-time under live traffic conditions.		
8	The field of view of ATCC on a road stretch shall be able to cover from end to end of the traffic lane irrespective of the number of lanes on the particular road stretch.		
9	The number of ATCC sensors required to achieve a multi-lane road stretch shall be arrived at by the SI based on the technology being provided and other criteria.		
10	The ATCC System at any point of time, shall provide a minimum of 3 classification levels viz. 2-wheeler, 3-Wheeler/Auto Rickshaws, Bus/Truck/MAV at any given point in time.		

S. No.	Minimum Requirements	Bidder Compliance (Yes/No)	Product Documentation Reference
11	<p>The ATCC system shall meet the following accuracy levels when compared with actual data collected using other means at each location of all the installed locations (minimum accuracy requirements) in day and night &amp; in FOG &amp; poor visibility situations.</p> <ul style="list-style-type: none"> <li>• Counting of vehicles: &gt; 90%</li> <li>• Classification of vehicles (w.r.t. each class): &gt; 80%</li> </ul>		
12	The ATCC shall have built in algorithms to distinguish and classify non-linear traffic patterns and occlusion of traffic.		
13	There shall be an operator at central control room to operate the ATCC application on ATCC workstation.		
14	The data of ATCC shall also be available in open data source which can further be used in other applications.		
15	The overall system shall work in an integrated fashion whereby data from the ATCC shall be continuously recorded, processed and transferred to TCCC.		
16	The algorithm (software) shall be capable of adding configuration parameters for each of the vehicle classes based on the RTA standards and field conditions to achieve maximum accuracy		
17	Sensor should enable client to identify and classify vehicles visually for comparative analysis purposes in all type of light conditions dawn, dusk, day, night & bad weather situations like Fog bad weather etc.		
18	ATCC shall be able to process simultaneously at least 100 vehicles and parallel passages of the vehicles at that location at a given point of time and provide queue length estimation for minimum 85 meters		
19	Even though multiple sensors are required based on the number of actual lanes, the ATCC should provide processed data at each location lane wise and leg wise.		
20	The ATCC shall count and classify vehicles traveling in any or both the directions at a given location as per the requirement based on the field conditions.		
21	The ATCC should be able to count and classify the vehicles with minimum accuracy requirements for vehicles traveling between 20 kmph to 120 kmph speeds.		
22	The ATCC sub-system should be capable of capturing at a minimum the following primary data points for each vehicle at any point of time:		

S. No.	Minimum Requirements	Bidder Compliance (Yes/No)	Product Documentation Reference
a	• Unique ID		
b	• Vehicle Count		
c	• Leg / road Location		
d	• Classification in day, night and FOG conditions		
f	• Density		
g	• Headway		
h	• Occupancy		
i	• Queue Length for minimum 50 meters (including night and FOG conditions)		
j	• Speed		
23	The ATCC sub-system shall be capable of computing unlimited Derived fields/ data sets based on several mathematical computations on the primary data points collected. In general, all computations required for deriving several Traffic Engineering measures shall be supported by the ATCC reporting module.		
24	The ATCC sub-system provider shall work closely with client for modifying/configuring standard existing reports and data formats to suit client requirements. The vendor shall support client in developing any/ all reports and formats required by the agency for a period of at least 18 months from the system go-live date.		
25	The ATCC Sub-system shall be capable of sharing the data with any other sub-system in a real-time as per the requirement.		
26	The ATCC system shall have an operations monitoring dashboard, located at the TCCC & monitored by the operator.		
27	On this dashboard there shall be a schematic layout of the ATCC showing all the connected nodes on the GUI.		

#### 5.4.1.8 Pedestrian / Pelican Traffic Signal Controller

S. No.	Components	Minimum Requirements	Bidder Compliance (Yes/No)	Product Documentation Ref.
		Make		

S. No.	Components	Minimum Requirements	Bidder Compliance (Yes/No)	Product Documentation Ref.
		Model		
1	Type	Pedestrian Traffic Signal shall have pole mounted Push Button control panel to actuation traffic signal		
		System shall work on Low voltage DC operation for safety against voltage shock considering safety of pedestrian traffic		
		Shall be integrated with the proposed ATSC System.		
2	Indications	Visual indication: Indicator for call Register (Big push button unit having 2 Light Indicators for pedestrian signals & 1 for Call Confirmation Indication (call registration /wait)		
3	Voltage	Working voltage: 24 Volts DC or 110/220 Volts Ac.		
4	Body	Body Material: Plastic / Metal MS Powder coated.		
5	Mounting	Mounting: Pole mounted with help of brackets.		

#### 5.4.1.9 Pole at Junctions

S. No.	Minimum Requirements	Bidder Compliance (Yes/No)	Product Documentation Reference
	Make		
	Model		
	Cantilever Pole		
1.	Hot dip galvanized pole with silver coating of 86 micron as per IS:2629 min 10 cm diameter pole and suitable bottom and top thick HT plate along with base plate size 30x30x15 cms suitable for wind speed 120 km/hr with / without suitable arm bracket and with J type foundation bolts. Fabrication in accordance with IS 2713 (1980)		
2.	Mounting facilities: To mount Traffic signals, Pedestrian Signals, Switch, PA system etc.		

S. No.	Minimum Requirements	Bidder Compliance (Yes/No)	Product Documentation Reference
3.	Pipes, Tubes: All wiring must be hidden, through tubes/pipes. No wires shall be visible from outside.		
4.	All poles at junctions shall have earthing arrangement for protection against lightning and surge.		

#### 5.4.1.10 Cable for Traffic Signal Integration

S. No.	Components	Minimum Requirements	Bidder Compliance (Yes/No)	Product Documentation Ref.
		Make		
		Model		
1	Nos of core	As per design requirements		
2	Materials	As per design requirements		
3	Certification	ISI Marked		
4	Standards	Indian Electricity Act and Rules		
5	IS:1554	PVC insulated electric cables (heavy duty)		

#### 5.4.2 Traffic Violation Detection System (TVDS) with ANPR & RLVD Camera

##### 5.4.2.1 Functional Requirement – Traffic Violation Detections System

The functional requirements and technical specifications provided in the below sections are indicative and carry guiding rule. The SI is free to offer products and solutions which meet requirements of the RFP focusing on the outcome, future scalability, security, reliability and adherence to specified SLA under this RFP, in line with applicable standards & best practices adopted in the industry. The SI is encouraged to design an Optimized solution which is technically superior, innovative, proven, better in terms of functionality and is cost effective. Any specified parameters mentioned in the scope/technical requirement in the RFP may be considered if it is required for meeting current & future requirements during the contract period. The SI is fully responsible for the specified outcome to be achieved.

The traffic violation detection system should detect the following traffic rules violations:

1. Red Light Violation Detection (RLVD)
2. Speed Violation Detection (SVD)
3. Wrong Lane Driving / Stoppage with ANPR (WLD)
4. No Helmet Detection with ANPR (NHD)
5. Triple Ride Detection with ANPR (TRD)

Following are the pre-requisites for Traffic Violation Detection System Vendors;

- a) The system should support centralized or decentralized architecture.
- b) The ITMS OEM should have quality certification (nationally/internationally recognized) with R&D center in India for past 5 years. Necessary documentation to this effect must be submitted.
- c) The ITMS OEM should have supplied at least 2000 licenses (ANPR/RLVD/Speed or cumulative) in at least three projects in India.
- d) The system should be developed and built on operating system agnostic platform, should work on Commercially OFF THE SHELF (COTS) servers and storage solutions, and should be database agnostic.
- e) The system should support Microsoft SQL, MySQL, PostgreSQL and Oracle databases.
- f) The system should support virtual computing environment and should support virtualization platforms on Windows and Linux operating systems.
- g) The ITMS Software should be NABL accredited lab for accuracy

#### 5.4.2.2 Functional/General Requirements Red Light Violation Detection (RLVD) System

#	Minimum Requirements	Bidder Compliance (Yes/No)
<b>1</b>	<b>General</b>	
<b>a.</b>	The following Traffic violations to be automatically detected by the system by using appropriate Non- Intrusive sensors technology: The system should have both provisions to detect red light status by taking the signal feed from the traffic signal controller as well as by video analytics method using another camera (Evidence Camera) focused at the red light. The Evidence camera should also be used for evidence snap generation.	
	a) Red Light Violation	

#	Minimum Requirements	Bidder Compliance (Yes/No)
	b) Stop Line Violation	
<b>b.</b>	The system should be capable of capturing multiple infracting vehicles simultaneously in Different lanes on each arm at any point of time with relevant infraction data like:	
	a) Type of Violation	
	b) Date, time, Site Name and Location of the Infraction	
	c) Registration Number of the vehicle through ANPR	
	Camera system for each vehicle identified for infraction.	
<b>c.</b>	The system should be equipped with a camera system to record a digitized image and video of the violation, covering the violating vehicle with its surrounding and current state of signal (Red/Green/Amber) by which the system should clearly show nature of violation and proof thereof:	
	a) When it violates the stop line.	
	b) When it violates the red signal.	
	c) Besides, a closer view indicating readable registration number plate patch of the violating vehicle for court evidence for each violation.	
	The system shall have in-built tool to facilitate the user to compose detail evidence by stitching video clips from any IP camera in the junction (including but not limited to the red-light violation detection camera, evidence camera), and any other surveillance cameras in the vicinity of the spot of incidence. The entire evidence should be watermarked and encrypted to stand the court of law.	
<b>d.</b>	The system shall be able to detect all vehicles infracting simultaneously in each lane/ arm at the junction as per locations provided. It should also be able to detect the vehicles infracting serially one after another in the same lane. The vehicles should be clearly identifiable and demarcated in the image produced by the camera system.	
<b>e.</b>	The Evidence image produced by the system should be wide enough to give the exact position of the infracting vehicles with respect to the stop line and clearly indicate colour of the Traffic light at the instant of Infraction even if any other means is being used to report the colour of the light.	

#	Minimum Requirements	Bidder Compliance (Yes/No)
f.	The system should interface with the traffic controller to validate the colour of the traffic signal reported at the time of Infraction so as to give correct inputs of the signal cycle.	
g.	The Evidence and ANPR camera should continuously record all footage in its field of view to be stored at the local base station. This should be extractable onto a portable device as and when required. The option of live viewing of evidence cameras from the locations shall be available at the ICCC. The network should have the capability to provide the real time feed of the evidence camera to the ICCC at the best resolution possible on the available network.	
h.	The system shall be equipped with IR Illuminator to ensure clear images including illumination of the Number Plate and capture the violation image under low light conditions and night time.	
<b>2</b>	<b>Recording &amp; display information archive medium</b>	
a.	The recording and display of information should be detailed on the snapshot of the infracting vehicle as follows:	
b.	Computer generated unique ID of each violation	
c.	Date (DD/MM/YYYY)	
d.	Time (HH:MM: SS)	
e.	Equipment ID	
f.	Location ID	
g.	Carriageway or direction of violating vehicle	
h.	Type of Violation (Signal/Stop Line)	
i.	Lane Number of violating vehicle	
j.	Time into Red/Green/Amber	
k.	Registration Number of violating vehicle	
<b>3</b>	<b>On site-out station processing unit communication &amp; Electrical Interface</b>	
a.	The system should automatically reset in the event of a program hang up and restart on a button press. However, the system should start automatically after power failure.	
b.	The system should have secure access mechanism for validation of authorized personnel.	
c.	Deletion or addition and transfer of data should only be permitted to authorized users.	



#	Minimum Requirements	Bidder Compliance (Yes/No)
d.	A log of all user activities should be maintained in the system.	
e.	Roles and Rights of users should be defined in the system as per the requirements of the client	
f.	All formats of the stored data with respect to the infractions should be Non-Proprietary.	
g.	The communication between the on-site outstation processing unit housed in the junction box and the detection systems mounted on the cantilever shall be through appropriate secured technology.	
h.	The system should have the capability to transfer the data to ICCC through proper encryption in real time and batch mode for verification of the infraction and processing of challan. Call forwarding architecture shall be followed to avoid any data loss during transfer.	
i.	In the event that the connectivity to the ICCC is not established due to network/connectivity failures, then all data pertaining to the infraction shall be stored on site and will be transferred once the connectivity is re-established automatically. There shall also be a facility of physical transfer of data on portable device whenever required. There should be a provision to store minimum <b>one week</b> of data at each site on a 24x7 basis.	
<b>4</b>	<b>Mounting structure</b>	
a.	Should be cantilever mounted and shall have minimum 6 Meters. height with appropriate vertical clearance under the system from the Road surface to ensure no obstruction to vehicular traffic.	
b.	It should be capable to withstand high wind speeds and for structural safety, the successful bidder has to provide structural safety certificate from qualified structural engineers approved/ certified by Govt. Agency.	
c.	It shall be painted with one coat of primer and two coats of PU paint. The equipment including poles, mountings should have an aesthetic feel keeping in mind the standards road Infrastructure (e.g. Poles, Navigation boards etc.) currently installed at these locations. The equipment should look "one" with the surroundings of the location and not look out of place.	
d.	Rugged locking mechanism should be provided for the onsite enclosures and cabinets.	

#	Minimum Requirements	Bidder Compliance (Yes/No)
<b>5</b>	<b>RLVD Application</b>	
<b>a.</b>	It should be capable of importing violation data for storage in database server which should also be available to the Operator for viewing and retrieving the violation images and data for further processing. The program should allow for viewing, sorting, transfer & printing of violation data.	
<b>b.</b>	It should generate the photograph of violations captured by the outstation system which include a wider view covering the violating vehicle with its surrounding and a closer view indicating readable registration number plate patch of the violating vehicle or its web link on notices for court evidence.	
<b>c.</b>	All outstation units should be configurable using the software at the Central Location.	
<b>d.</b>	Violation retrieval should be sorted by date, time, location and vehicle registration number and the data structure should be compatible with Assam/ Guwahati Police database structure. It should also be possible to carry out recursive search and wild card search.	
<b>e.</b>	The operator at the back office should be able to get an alarm of all fault(s) occurring at the camera site (e.g. sensor failure, camera failure, failure of linkage with traffic signal, connectivity failure, Camera tampering, sensor tampering).	
<b>f.</b>	The automatic number plate recognition Software shall be part of the supplied system, Success rate of ANPR shall be taken as 80% or better during the day time and 60% or better during the night time with a standard number plate.	
<b>g.</b>	The application software should be integrated with the E-Challan software for tracing the ownership details of the violating vehicle and issuing/printing notices. Any updates of the software (OS, Application Software including any proprietary software), shall be updated free of cost during the contract period by the SI.	
<b>h.</b>	Image zoom function for number plate and images should be provided. In case the number plate of the infracting vehicle is readable only through the magnifier then in such cases the printing should be possible along with the magnified image.	

#	Minimum Requirements	Bidder Compliance (Yes/No)
i.	Various users should be able to access the system using single sign on and should be role based. Different roles which should be defined (to be finalized at the stage of SRS) could be Administrator, Supervisor, Officer, Operator, etc.	
j.	Apart from role-based access, the system should also be able to define access based on location.	
k.	Rights to different modules / Sub-Modules / Functionalities should be role based and proper log report should be maintained by the system for such access.	
l.	Components of the architecture should provide redundancy and ensure that there are no single points of failure in the key project components. Considering the high sensitivity of the system, design shall be in such a way as to be resilient to technological sabotage. To take care of remote failure, the systems need to be configured to mask and recover with minimum outage.	
m.	The architecture should adopt an end-to-end security model that protects data and the infrastructure from malicious attacks, theft etc. Provisions for security of field equipment as well as protection of the software system from hackers and other threats shall be a part of the proposed system. Using Firewalls and Intrusion detection systems such attacks and theft shall be controlled and well supported (and implemented) with the security policy. The virus and worms' attacks shall be well defended with Gateway level Anti-virus system, along with workstation level Anti-virus mechanism. There shall also be an endeavor to make use of the SSL/VPN technologies to have secured communication between Applications and its end users. Furthermore, all the system logs shall be properly stored & archived for future analysis and forensics whenever desired.	
n.	The evidence of Infraction should be encrypted and protected so that any tampering can be detected.	
o.	Ease of configuration, ongoing health monitoring, and failure detection are vital to the goals of scalability, availability, and security and must be able to match the growth of the environment.	
p.	System shall use open standards and protocols to the extent possible and declare the proprietary software wherever used.	

#	Minimum Requirements	Bidder Compliance (Yes/No)
q.	The user interface should be user friendly and provide facility to user for viewing, sorting and printing violations. The software should also be capable of generating query based statistical reports on the violation data.	
r.	The data provided for authentication of violations should be in an easy to use format as per the requirements of user.	
s.	User should be provided with means of listing the invalid violations along with the reason(s) of invalidation without deleting the record(s).	
t.	Basic image manipulation tools (zoom etc.) should be provided for the displayed image but the actual recorded image should never change.	
u.	Log of user actions be maintained in read only mode. User should be provided with the password and ID to access the system along with user type (admin, user).	
v.	Image should have a header/footer depicting the information about the site IP and violation details like date, time, equipment ID, location ID, Unique ID of each violation, lane number, Regn. Number of violating vehicle and actual violation of violating vehicle etc. so that the complete lane wise junction behavior is recorded including (Red Light violation and Stop Line Violation)	
w.	Number plate should be readable automatically by the software/interface. There should be user interface for simultaneous manual authentication / correction and saving as well.	
x.	Interface for taking prints of the violations (including image and above details).	

#### 5.4.2.3 Technical Specification - Red Light Violation Detection (RLVD) Systems

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

#	Parameters	Minimum Specifications	Bidder Compliance (Yes/No)	Product Documentation Reference
3	General	The system should be capable of generating a video & minimum 3 snapshots in any of the standard industry formats (MJPEG, JPG, avi, mp4, mov, etc.) with at least 10 frames per second. The video shall be from t-5 to t+5 sec of the violation and should also be recorded (being the instant at which the infraction occurred).		
4	Digital Network Camera			
a.	Video Compression	H.264, H.265 or better		
b.	Video Resolution	2-MP - 1920x 1080p		
c.	Frame rate	Min. 50 ~ 60 FPS		
d.	Image Sensor	1/3" ~ 1/2" Inch Progressive Scan CCD / CMOS or better to fit for solutions		
e.	Lens Type	Varifocal, C/CS Mount, IR Correction full HD lens		
f.	Lens	Auto IRIS 5~50mm /8 – 40 mm, F1.4		
g.	Minimum Illumination	Colour: 0.5 lux, B/W: 0.1 lux (at 30 IRE)		
h.	IR Cut Filter	Automatically Removable IR-cut filter		
i.	Day/Night Mode	Colour, Mono, Auto		
j.	S/N Ratio	≥ 50 Db		
k.	Auto adjustment + Remote Control of Image settings	Colour, brightness, sharpness, contrast, white balance, exposure control, backlight compensation, Gain Control, True Wide Dynamic Range		
l.	Local storage	Minimum 128 GB Memory card in a Memory card slot. 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.		

#	Parameters	Minimum Specifications	Bidder Compliance (Yes/No)	Product Documentation Reference
m.	Protocol	IPV4, IPV6, HTTP, HTTPS, FTP/SMTP, RTSP, RTP, TCP, UDP, RTCP, DHCP, UPnP, NTP, QoS, ONVIF Profile S		
n.	Security	Password Protection, IP Address filtering, User Access Log, HTTPS encryption		
o.	Operating conditions	As per Guwahati weather conditions		
p.	Casing	NEMA 4X / IP-66, IK10 rated		
q.	Intelligent Video	Motion Detection & Tampering alert		
r.	Alarm I/O	Minimum 2 Input & 1 Output contact for 3rd part interface		
s.	Certification	UL/EN, CE, FCC		
<b>5</b>	<b>On site-out station processing unit communication &amp; Electrical Interface (Junction Box)</b>			
a.	Data Storage on site	The system should be equipped with appropriate storage capacity for 7 days 24X7 recording, with overwriting capability. The images should be stored in tamper proof format only.		
b.	Network Connectivity	Wired/GPRS based wireless technology with 3G upgradable to 4G capability.		
c.	Minimum 2(two) USB Port to support the latest external mass storage devices and Ethernet (10/100) Port for possible networking. However, all logs of data transfer through the ports shall be maintained by the system.			
d.	The system should be capable of working in ambient temperature as per Guwahati weather conditions.			
e.	Lightening arrester shall be installed for safety of system (As per BIS standard IS 2309 of 1989).			
f.	The housing(s) should be capable of withstanding vandalism and harsh weather conditions and should meet IP66, IK10 standards (certified).			
<b>6</b>	<b>Violation Transmission and Security</b>			

#	Parameters	Minimum Specifications	Bidder Compliance (Yes/No)	Product Documentation Reference
a.		Encrypted data, images and video pertaining to Violations at the Onsite processing station should be transmitted to the ICCC electronically through GPRS based wireless technology with 3G upgradable to 4G, or wired connectivity if available in Jpeg format		
b.		Advanced Encryption Standard (AES) shall be followed for data encryption on site and ICCC, and its access will be protected by a password.		
c.		The vendor shall ensure that the data from the onsite processing unit shall be transferred to ICCC within one day.		
<b>7</b>	<b>Video Recording</b>			
a.		The system should be capable of continuous video recording in base station for 7 days. The system shall automatically overwrite the data after 7 days. It should be noted that at any point of time the local storage at the base station should have the data of previous 7 days.		
b.		Direct extraction through any physical device like USB flash drive, Portable Hard disk etc. shall be possible		

#### 5.4.2.4 Functional Requirements of Automatic Number Plate Recognition (ANPR) System

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

- The System should automatically detect a vehicle in the camera view using video detection and activate license plate recognition.
- The System should automatically detect the license plate in the captured video feed in real-time and the system should perform Optical Character Recognition (OCR) of the license plate characters.

- System should be able to detect and recognize the English alpha numeric license plate in standard fonts and formats for classes of vehicles such as cars, Heavy Commercial Vehicles, Three Wheelers and Two Wheelers.
- The system should capture standard vehicle's number plates with an accuracy of at least 70% at day time and at least with an accuracy of 60% at night time.
- The System should store JPEG image of vehicle and license plate and enter the license plate number into the database along with the date, time stamp and site location details.
- The system should detect the colour of all the vehicles on best effort basis, in the camera view during daytime and label them as per the predefined list of configured system colours. The system should store the colour information of each vehicle along with the license plate information for each transaction in the database.
- The system should identify the category of the vehicle such as cars, Heavy Commercial Vehicles, Three Wheelers and Two Wheelers and should store this information along with the license plate information for each transaction in the database.
- The system should have an option to store certain license plates of vehicles which are stolen or suspicious. The system should have the functionality to enter such license plate numbers to lists such as "Wanted", "Suspicious", "Stolen" termed as hot lists of vehicles. The system should allow the user to import the vehicle license plate data in the hot lists stored in Excel sheets for batch operation.
- The system should generate an automatic alert in the control room, when it detects the vehicle from the hot list/s through the ANPR camera. The system should give an instant alert in such case. The system should also have the functionality to send the alert via email and SMS to designated email addresses and mobile phone numbers.
- The system should allow the operator to change the hot list category of the vehicle and accordingly the new hot list category should be reflected in the records stored in the database. E.g. on retrieval of stolen vehicle, system entry should be changed from "Stolen" to "Retrieved".
- The system should be able to store license plates numbers of at least 10,000 suspected vehicles at a time and should generate an Alert if any one of the vehicles is found crossing the stop line (irrespective whether the signal is GREEN or RED) in form of Video popup at the Monitor and/or SMS on Cell phones.
- The system should have the functionality to trace the movement of a vehicle of interest on Google Map. The Function should show the trajectory of the vehicle drawn on the map. The vehicle of interest should be tracked for all the junctions where it is detected through ANPR.
- The system should give an option to the operator to edit the license plate number of the vehicle. The system should show the license plate of the vehicle in a zoomed window for easy inspection of the license plate number. The system should keep audit trail of any license plate number edited by the operator.



- The system should have function of quickly searching the number plate based on the following criteria:
  - full or partial number of the license plate,
  - colour of the vehicle,
  - classification of vehicle,
  - Junction Name
  - Event Type (e.g. ANPR, Red Light Violation, Speed Violation, etc.)

#### 5.4.2.5 Technical Specification - ANPR SW Requirements

#	Parameters	Minimum Specifications	Bidder Compliance (Yes/No)	Product Documentation Reference
1	<b>Make</b>	<to be provided by the bidder>		
2	<b>Model</b>	<to be provided by the bidder>		
3	<b>Vehicle Detection by Color</b>			
a	Colour Detection	The system shall detect the colour of all vehicles in the camera view during daytime and label them as per the predefined list of configured system colours. The system shall store the colour information of each vehicle along with the license plate information for each transaction in the database.		
b	History Record	The system shall have options to search historical records for post event analysis by the vehicle colour or the vehicle colour with license plate and date time combinations		
4	<b>Alert Generation</b>			
a	Inputs by Licence Plate	The system should have option to input certain license plates according to the hot listed categories like “Wanted”, “Suspicious”, “Stolen”, etc by authorized personnel.		
b	Auto Alarm	The system should be able to generate automatic alarms to alert the control room personnel for further action, in the event of detection of any vehicle falling in the hot listed categories.		
5	<b>Vehicle Status Alarm Module</b>			

#	Parameters	Minimum Specifications	Bidder Compliance (Yes/No)	Product Documentation Reference
a	Auto Alarm	On successful recognition of the number plate, system should be able generate automatic alarm to alert the control room for vehicles which have been marked as "Wanted", "Suspicious", "Stolen", "Expired". (System should have provision/expansion option to add more categories for future need).		
b	Auto Alarm	The Instantaneous and automatic generation of alarms. In case of identity of vehicle in any category which is define by user.		
<b>6</b>	<b>Vehicle Log Module</b>			
a	Quick Retrieval	The system shall enable easy and quick retrieval of snapshots, video and other data for post incident analysis and investigations.		
b	MIS Report	The system should be able to generate suitable MIS reports that will provide meaningful data to concerned authorities and facilitate optimum utilization of resources. <ul style="list-style-type: none"> <li>o Report of vehicle flow at each of the installed locations for Last Day, Last Week and Last Month.</li> <li>o Report of vehicles in the detected categories at each of the installed locations for Last Day, Last Week and Last Month.</li> <li>o Report of Vehicle Status change in different Vehicle Categories.</li> </ul>		
c	Search Options	The system shall have Search option to tune the reports based on license plate number, date and time, site location as per the need of the authorities.		
d	Save Report	The system shall have option to save custom reports for subsequent use. The system shall have option to export report being viewed to common format for use outside of the ANPRS or exporting into other systems.		

#	Parameters	Minimum Specifications	Bidder Compliance (Yes/No)	Product Documentation Reference
e	Advanced Search Option	The system should provide advanced and smart searching facility of License plates from the database. There should be an option of searching number plates almost matching with the specific number entered (up to 1- and 2-character distance)		
<b>7</b>	<b>Vehicle Category Editor</b>			
a	Inputs by Licence Plate	The system should have option to input certain license plates according to category like "Wanted", "Suspicious", "Stolen", "Expired" etc. by Authorized personnel.		
b	Add Information's	The system should have an option to add new category by authorized personnel.		
c	Updated Information's	The system should have option to update vehicle status in specific category by authorized personnel. e.g. on retrieval of stolen vehicle, system entry should be changed from "Stolen" to "Retrieved".		
d	Specify Information	System should have option to specify maximum time to retain vehicle records in specific categories.		
<b>8</b>	<b>General Specification:</b>			
a	Video Evidence	The system should be capable of generating a video and minimum 5 snapshots in any of the standard industry formats (MJPEG, JPG, avi, mp4, mov, etc) with at least 10 frames per second.		
b	ANPR & Alert	The system should be able to perform ANPR on all the vehicles passing the site and send alert on detection of any hot listed vehicle		
c	Numeric Character Generation	The system should have ANPR/OCR to address the alpha numeric character of irregular font sizes		
<b>9</b>	<b>Central Management Module</b>			
a	Central Management Module.	The Central Management Module shall run on the ANPR Central Server in control booth. It should be possible to view records and edit hotlists from the Central Server.		

#	Parameters	Minimum Specifications	Bidder Compliance (Yes/No)	Product Documentation Reference
b	ANPR Specification	Base Specification of Fixed Box Cameras (Section 6.2.2.2 of Annexure I) must be part of the		
c	Camera Housing	IP66 standard with sunshield vandal proof Housing		
<b>10</b>	<b>Systems requirement</b>			
a	Local Server at Intersection:	The system shall run on a Commercial Off the Shelf Server (COTS). Outdoor IP 66 Quad core processor-based server should be able to cover at least 8 lanes. Temperature rating of the server should be as per Guwahati weather conditions.		
b	Operating system:	The system shall be based on open platform and should run on Linux or windows Operating system.		
c	Workstation:	Workstation shall run on latest available OS.		

#### 5.4.2.6 ANPR HW Requirements

#	Parameters	Minimum Specifications	Bidder Compliance (Yes/No)	Product Documentation Reference
1	<b>Make</b>	<to be provided by the bidder>		
2	<b>Model</b>	<to be provided by the bidder>		
3	Lens & Resolutions	5-50mm Lens & 2-MP - 1920x 1080p		
4	Shutter Time	PAL: 1/20~ 1/30,000 sec.		
5	Image Sensor	1/3" ~ 1/2" Progressive Scan CCD / CMOS or better to fit for solutions		
6	Minimum Illumination	0.001Lux @ (F1.2, AGC ON), 0.0014Lux @ (F1.4, AGC ON), 0 Lux at IR ON		

#	Parameters	Minimum Specifications	Bidder Compliance (Yes/No)	Product Documentation Reference
7	Focus Width Range	1 vehicle lane		
8	BLC Mode	OFF, Low, Medium, High		
9	HLC Mode	Required		
10	WDR	Up to 140 dB		
11	White Balance	Indoor/Outdoor/Auto		
12	Video Noise Filter	3D, 1-10 levels		
13	S/N Ratio	>60db		
	<b>Compression Standard</b>			
14	Video Compression	H.264, H.265, MPEG-4 & MJPEG		
15	Bit Rate	64 Kbps ~ 7Mbps		
16	Audio Compression	G.711/AAC-LC		
17	Triple Stream	Required		
18	Image Resolution (Primary stream) Resolution (Secondary stream) Resolution (Mobile stream)	Mainstream: 2MP @50 FPS to 60 FPS, Sub stream: D1 @ 50FPS to 60 FPS		
19	Frame rate	50 to 60 FPS or Better		
20	Image Settings through client software or web browser	Saturation, Brightness, Contrast, Sharpness, Hue, Gain, Mirroring adjustable		
	<b>Interface</b>			
21	Communication Interface	1 RJ45 10M / 100M Ethernet interface		
22	Alarm Input / Output	1 Alarm Input, 1 Alarm Output		

#	Parameters	Minimum Specifications	Bidder Compliance (Yes/No)	Product Documentation Reference
23	Audio Interface	Microphone Input, Audio Output, Supports two-way audio		
24	Reset Button	Required		
25	IR Illuminator	850nm intensity adjustable IR with minimum 30 meters range, IR from same Camera OEM		
26	LED type	12 pieces dot matrix array LED or better		
27	Wavelength	850nm approx.		
28	Flexible angle adjustment	30°, 45°, 60°, 90°		
	<b>Network</b>			
29	Networking Features	Bandwidth utilization, UPNP based port forwarding		
30	Security	User authentication, Watermark		
31	Protocol	IPv4, IPv6, TCP/IP, SNMP, HTTP, HTTPS, UPnP, RTSP, RTP, RTCP, IGMP, SMTP, FTP, DHCP, NTP, DNS, DDNS, PPPoE and 802.1x		
32	System Compatibility	ONVIF		

#### 5.4.2.7 IR – Illuminator (In case of Separate IR)

#	Parameters	Minimum Specifications	Bidder Compliance (Yes/No)	Product Documentation Reference
1	Make	<to be provided by the bidder>		
2	Model	<to be provided by the bidder>		
1	IR control	Adjustable IR intensity		
2	Wavelength Type	850 nm semi-covert		
3	Beam Angles	10°, 20°, 30°, 60°, 80°, and 95°		
4	Casing	Aluminum and Polycarbonate		
5	IR Distance	80 meter or better		
6	Environmental Protection	IP66 Rated		

#	Parameters	Minimum Specifications	Bidder Compliance (Yes/No)	Product Documentation Reference
7	Operating Temperature	0°C to 50°C		
8	Standards	UL, CE, FCC, EN		
9	Approved Makes	The Camera and IR Illuminator shall be of the same make		

#### 5.4.2.8 Online UPS for Field Locations (ITMS Crossing)

#	Parameters	Minimum Specifications	Bidder Compliance (Yes/No)	Product Documentation Reference
1	<b>Make</b>	<to be provided by the bidder>		
2	<b>Model</b>	<to be provided by the bidder>		
3	Capacity	2 KVA		
4	Technology	IGBT based PWM Technology, True Online UPS		
5	Input Frequency Range	Preferably 45 to 55 Hz		
6	Output Frequency Range	Preferably 45 to 55 Hz		
7	Output Voltage	Preferably 220VAC - 230VAC		
8	Voltage Regulation	Preferably +/- 2% (or better) and with built-in Over Voltage Cut off facility in the Device		
9	Frequency	Preferably 50 Hz +/- 0.1% (free Run Mode)		
10	Harmonic Distortion (THD)	Preferably < 3% (linear load)		
11	Output Waveform	Pure Sine wave		
12	Output Power Factor	0.8 or more		
13	Battery Backup	60 Mins Power backup Required. Adequate and required battery backup to achieve required uptime of field device as well as SLA of the overall solution.		

#	Parameters	Minimum Specifications	Bidder Compliance (Yes/No)	Product Documentation Reference
14	Battery Type	Preferably Lead acid, Sealed Maintenance Free (SMF)		
15	General Operating Temperature & Humidity	Temp.: (-)10 Degree C to (+)70 Degree C or better Humidity: 10 - 90% (non-condensing) As per Guwahati weather conditions		
16	Alarms & Indications	All necessary alarms & indications essential for performance monitoring of UPS like mains fail, low battery & fault detection		
17	Bypass	Automatic, Manual Bypass Switch		
18	Certifications	For Safety & EMC as per international standard • BIS Certification for the specific model offered • CE Certification • ISO 9001, ISO 14001, OHSAS 18001 certified. • RoHS Compliance		
19	Service Support	UPS OEM should have their own established service center and Service Engineers in Guwahati to attend any issues on 24x7 basis. Service Center should be fully operational for last 5 years		
20	Remote Monitoring & Maintenance Ports & LED Indication	a) SNMP port for remote monitoring. b) RS232/Management Port for onsite servicing. c) LED indicators to be mentioned for Load/Backup/Overload/etc.		
21	Overall Protection	IP 55, Junction Box design should ensure to keep the temperature within suitable operating range for equipment's and should also avoid intentional watersplash and dust intake		

### 5.4.3 Speed Violation Detection System (SVD)

#### 5.4.3.1 Speed Violation Detection System (SVD)- General Requirements

- 1) SVD consist of Speed Detection Radar to capture speeds of vehicles passing on either direction at a location covering all traffic lanes and shall trigger High



Resolution Camera (Speed Enforcement Camera) to capture image of vehicles which are plying above threshold speed. The image will be transmitted over GPRS based wireless network to server located at Central control room. The captured image will be processed at Central control through software along with manual approval for identified number plate of violation vehicle for further processing.

- 2) The Supplier shall review specifications and requirements listed in this section to propose the necessary configuration to support the complete system requirements as well as performance requirements. The Supplier proposal shall specify clearly, the purpose of each of the system components proposed, as well as its available features and associated benefits.
- 3) The development/customization of the System shall be carried out at the Supplier site but from Acceptance Testing onwards, it shall be carried out at client's site.
- 4) The Supplier shall propose the Operating System (OS) and the appropriate platform that meets all the requirements stated in this section.
- 5) The status of the individual components of the system shall be monitored by the software through continuous scanning from Central Control room.
- 6) The supplier shall suggest optimum height for the system and should be based on the conditions between radar and camera. In general, they shall be mounted at heights of about 6m roadway level on a gantry/pole.

#### **5.4.3.2 Speed Violation Detection System Requirements:**

System Software connects to the camera unit and radar unit to evaluate sensor data and record images as required. The software receives data from the radar unit and tracks all vehicles moving near the speed enforcement camera. The software allows the configuration of enforcement rules by lane, such as the speed limit/threshold to be applied for each lane. The tracked data of vehicles is compared to the enforcement rules, and for vehicles violating a rule (for example travelling in a lane at a speed above the configured threshold for that lane), based on the RADAR information, an image capture process is initiated when a violation happens. The software controls the camera, ensuring that the camera exposure, aperture and gain settings are appropriate for the prevailing ambient light conditions to ensure image capture of vehicles up to 300km/h. When a speeding vehicle image capture process is initiated, the software controls the camera to take two images of the vehicle, spaced at a configured distance apart, and generates precise timestamps for those images and matches those images to the radar data. Furthermore, the software will perform data integrity checks on the data to ensure that the speed detection is likely to be accurate.

- 1) The System shall instantly detect speed limit violations committed by motor vehicles, ranging from small cars to long trucks. A speed violation is considered as any event where a vehicle passes an imaginary line perpendicular to the road axis at a speed above the local/posted speed limit.
- 2) The Manual Intervention of Speed enforcement through Radar Graphics to get more than 95% enforcement is also acceptable for E-Challan.
- 3) Speed enforcement capability should be enabled without requiring any change to the system hardware.
- 4) When a speed violation is detected, the system shall capture at least two high resolution still images of the event.
- 5) If there are two or more vehicles committing a violation in the same instant or very close together, the system shall capture images of both the violation vehicles and have a separate file for processing for each violating vehicle.
- 6) If there are two or more vehicles displayed in the still image, the system shall indicate the primary offending vehicle.
- 7) The System shall be capable of providing independent secondary checks on the violating speed captured by the primary speed check mechanism. This is so as to provide corroborative evidence in case of prosecution.
- 8) The system shall detect violations of approaching vehicles.
- 9) The system shall at least distinguish between two types of vehicles: car and Truck.

#### **5.4.3.3 Evidence Capturing Requirements**

- a) The images shall be at least 9 (Nine) megapixel full color and be of good enough quality for number plate recognition by normal naked human eyes through standard 23" computer monitor (under resolution of 1920 × 1080 pixels) and/or through hardcopy printout in A4 size paper
- b) The image of the offending vehicle shall be taken from the front/rear side of the vehicle, based on the actual site condition(s).
- c) The System shall be equipped with a white flash to ensure adequacy of evidential images. The flash shall be capable of at least 4 shots in one second to capture images violations occurring simultaneously in different lanes.

#### 5.4.3.4 Evidence Storage Functional Requirements

- a) The system shall be designed with sufficient processing power and storage capacity to process and handle the maximum number of vehicles per day. The estimated number of violation images is as follows:

• Average images per camera per day	• 2000
• Average images per camera per month	• 60000

- b) To ensure data integrity, the System shall provide means to perform digital fingerprinting when data/images are captured.
- c) The system shall be compiled with infringement packaging software; this Software will add metadata to images captured by the detection software, such as a data bar with the location, speed detected and other requested information. The packaging software will save data about the detected vehicle (such as the location, vehicle speed, timestamp etc.) in XML format. The images of the vehicle and the XML data will be combined into a file, which will be encrypted.
- d) The following data shall be embedded on to the bottom/top part of the images captured and shall also be digitally fingerprinted and encrypted before storage:
- Date of Offence
  - Time of Offence
  - Location of offence and direction of travel
  - Speed of violation
  - Set Speed threshold
  - Camera number
  - Speed permitted

#### 5.4.3.5 System Management Requirements

- a) The System shall be capable of recording test violations on manual command when triggered on-site or remotely from the back office or Central control room.
- b) The System shall provide an independent in-built test signal to simulate the following self-test measurement for:
- Camera calibration
  - Power supply to all modules
  - Network connectivity

- c) This test shall be carried out automatically at switch-on and also operate automatically once daily (schedule for daily self-test to be configurable by users). If the System detects a fault during self-test, it shall stop capturing offences and indicate a fault state at back-office or Central control room.
- d) A local controller shall be designed to monitor and control the health status of all components within the system and alarms and shall be sent back to the back-office or Central control room for any malfunction of the system.
- e) The System shall, when power is resumed, be capable of automatically resuming operation.
- f) The System shall be compiled with System Monitoring / Self-Test / Watchdog software; this software will continuously monitor the radar, camera, computer and detection software to ensure correct functioning of each of the components. In the event of a failure of any component, the monitoring software will perform either a soft or hard reset of the appropriate equipment or software to restore correct function.
- g) The System shall be equipped with security on the system enclosure, of at least double locking and/or electronic tamper proof locks.
- h) The System shall, in the event of an unauthorized entry to the system enclosure or failure to the system, alert the operator through the back-office or Central control room.
- i) The system shall be compiled with automated File Transfer Protocol (FTP) software; this software will push generated speeding incident files to the central control room automatically as they are generated. The software will use the FTP protocol.

#### **5.4.3.6 Radar Requirements**

- a) The proposed violation detection device shall be of 4D tracking radar
- b) The detection device shall automatically monitor the speeds of each and every individual vehicle up to 4 traffic lanes simultaneously.
- c) The detection device shall employ an auto trigger mechanism to target violation vehicles.
- d) The detection device shall not trigger false detections due to multipath reflections.
- e) The measurement data of the detection device shall contain the position of the violating vehicle on the road (lane indication)
- f) The detection device speed thresholds shall be able to be easily pre-set by authorized user from the back-office and speed adjustable in 1 km/h increments between 10 km/h to 300 km/h.

- g) The System shall be able to function on Detection Range of Car: 250m.
- h) The System shall be able to measure the speed of vehicles up to 300 km/h and the permissible error allow for monitoring Four (4) lanes shall not exceed the following:
- $\pm 3$  km/h for speeds < 100km/h
  - $\pm 3$  % for speeds > 100km/h
- i) The detection device shall be designed to be health safe. The Tenderer shall provide the certification to this safety standard, in accordance with the appropriate regulatory standards.
- j) To limit installation time on site, physical installation of the detection device shall not require complex alignment procedures.

S/N	Parameter	Minimum Specification
1.	Technology	4D Object Tracking (Range, Angle, Speed, Time) with UHD Resolution, independent discrimination of multiple targets at same speed and same range
2.	Speed Range	Measurement up to 300km/h or more
3.	Field of view	$\pm 20$ degrees or greater horizontal, $\pm 10$ degrees or greater vertical
4.	Frequency	24 GHz/ 77 GHz
5.	Interface	Ethernet/CAN
6.	Housing	IP67
7.	Simultaneously Tracked Objects	100 or higher
8.	Minimum Detect Range	120m or higher
9.	Operating Modes	Approach, Recede, Bidirectional
10.	Drift	Negligible, no re-calibration needed over 10 years life.

#### 5.4.3.7 Speed Detection Camera Specifications

- a) The bidder shall indicate the model and type of digital camera proposed to be in used in the system.
- b) The proposed digital camera shall be based on an industrial grade construction with an integrated CMOS imaging device, due to the camera life cycle being in outdoor weather conditions on a 24/7 continuous use.
- c) The digital camera shall be capable to make still images.

- d) The digital camera must be capable of producing high quality optical color images, without the need for digital image enhancement, over a minimum of 4 traffic lanes in any direction such that:
- The violation vehicle in its entirety, as well as its immediate surroundings should be clearly visible, not blurred, in focus, color balanced, and exposed correctly for color, brightness and contrast;
  - The camera image resolution should be able to provide images such that violation vehicle's registration plate is clearly visible;
- e) The data recorded on the image is clearly visible, in focus and legible.
- f) The camera shall auto adjust itself to suit the lighting conditions of the traffic roads. The images shall not display blooming or smear as a result of glare from vehicle's headlight and other lighting.

S/N	Parameter	Minimum Specification
1	Image sensor and Effective Pixels (Resolution)	1" or higher, CMOS, Global Shutter, Minimum 9 MP, 4096(H) x 2160(V)
2	Electronic Shutter	1/1000 s to 1/10,000 s or better
3	Frame Rate	15 to 20 FPS or better
4	Fixed Focal Length Lens	25, 35, 50mm option to suit application. Lens must focus visible.
5	Interface	RJ-45 for GigE Ethernet
6	Operational Temperature °C	0°C to 50 °C
7	Outer Casing	Vandal Proof, IP66 rated Housing, sunshield
8	Power	PoE OR 12-24VDC
9	Certifications	CE, FCC, EN/UL, RoHS
10	Image Compression	JPEG
11	Video Compression	MJPEG, H.264

#### 5.4.3.8 Flash Unit Requirements

- a) The System shall be completed with at least 1 flash unit to provide the necessary lighting for a visible photograph to capture vehicle on a minimum 4 lanes traffic road, and the intensity is based on the ambient light level detected by the system
- b) The proposed flash unit shall be suitable for day and night operation and synchronized with the supplied Speed Enforcement camera.

Technical Requirements for Flash unit		
1	Spectrum	White Light.
2	Flash Duration	Outputs required power over <1/1000th of a second
3	Recycling	<500ms
4	Power	>250 Watts
5	Sync Speed	better than 1/2000th of a second

#### 5.4.3.9 User interface

- a) The system shall not require a dedicated hardware user interface for operation and maintenance. The user interface shall be web-based, allowing secured access from any web enabled device.
- b) Access to the system user interface shall be protected by a username and password.
- c) It shall be possible to assign roles to each user, limiting the access rights
- d) It shall be possible to configure the user interface language through a modified language file
- e) It shall be possible to configure the setting of the alignment, enforcement and system parameters through the Web Based Instructions or Central control room.

#### 5.4.3.10 Encryption and digital fingerprinting

- a) The system shall provide means to perform encryption and digital fingerprinting when data/images are captured to prevent tampering of the images. The Supplier shall provide encryption standard in accordance with local security policies.
- b) To ensure data privacy, the System shall provide means to perform encryption when data/images are captured at the system so that only the intended party is able to open the images after decryption
- c) The encryption or digital fingerprinting must be built in the system by using a separate secure storage device. The system shall automatically destroy the encryption key if there is any attempt to tamper with it.

#### Enclosure requirements

- a) The proposed system shall be a self-contained unit. All system components storage, processing module, are to be fixed in a heavy-duty cabinet mounted at a minimum height of greater than 5m to minimize the occurrence of vandalism. The other

remaining equipment in the site is to be enclosed separately or combined as per the requirements. Therefore, no system or detection sensor elements are to be external to the outer enclosure or mounted on the ground.

- b) The outer enclosure must be double stainless steel of at least 1.5 mm thick. It has to have a mounting flange round poles between 100 and 250mm in diameter.
- c) The foundation mounting for the pole shall be concrete cast; the outdoor enclosure equipment box shall be clamped onto the pole
- d) The system enclosure shall be properly earthed in accordance with existing electrical earthing and bonding guidelines. An earthing bar shall be provided inside the enclosure box for earthing the installed equipment.
- e) All induced electrical surges on the electrical and data lines shall be properly channeled to the earth via the installed surge arresters
- f) The surge arrestor shall protect all electrical, digital and data devices from voltage spikes, and the proposed surge arrestor shall meet IEC 61643-1 standards.
- g) The supplier shall propose the system enclosure unit to be fitted with ventilation fans and ensure that the system components are able to function and withstand ambient temperatures up to 50 degrees Celsius.
- h) The design of the proposed system enclosure shall be reviewed and accepted by the local authority.

Requirements for System Enclosure		
1	Material	Stainless Steel, Corrosion Resistant
2	Thickness	1.5 mm Stainless steel + reinforcement Material if required
3	Protection Type	min. IP (Ingress Protection) 65 Rated
4	Mounting Flange	Round poles, 100-250mm

#### 5.4.3.11 Environmental

The System shall be capable of capturing speed violations up to 300km/h for 24hours a day without degradation under the following weather and physical conditions:

- a) Operating temperature of -5 ~ +55 Degree Celsius;



- b) Storage temperature of up to 85 Degree Celsius for prolonged periods consistent with the temperature inside an enclosed metal casing under direct sunlight;
- c) Humidity of up to 95% (non-condensing)
- d) Intermittent, light and heavy rain
- e) Dusty environment characterized by heavy vehicles carrying debris
- f) Vibration as a result of heavy vehicles moving along the roads at speeds exceeding 70km/h

#### 5.4.3.12 Power Requirement for Solution

All field equipment shall be energized by Electrical Power. Power requirement for SVD is about 1000wats per day. Supplier shall provide backup power support system which meets ½ hour power requirement of SVD.

#### 5.4.4 Traffic Enforcement & E-Challan System

##### 5.4.4.1 Technical Specifications E-Challan System

#	Minimum Requirements	Bidder Compliance (Yes/No)
<b>A.</b>	<b>General</b>	
<b>1</b>	E-challan software shall work in client - server mode, where 30 handheld devices units will act as clients connected to the server through cellular network for data transfer. The system should be scalable to 500 devices, which may be added later on,	
	server requirements to be calculated as per	
	scalability for 500 devices, which may be added later on.	
<b>2</b>	E-challan system shall be able to retrieve vehicle owners' details and vehicle data from RTO data base to minimize data entry	
<b>3</b>	Server should maintain log of all current devices. Any access to the system must be recorded along with date, time, user id and IP address	
<b>4</b>	Traffic officer should log in to the hand-held device through the unique user id and pass word or smart card issued for the purpose	

#	Minimum Requirements	Bidder Compliance (Yes/No)
5	A unique challan number should be generated through client software for each challan	
6	As soon as a vehicle registration number is entered, the handheld device should automatically check from the server if the vehicle is stolen, wanted in any criminal case or is in the list of suspicious vehicles	
7	The most frequent traffic offences should be kept at the top in the drop-down menu and offence ingredients should be available if required by officer	
8	Date, time and GPS coordinates of place of challan should be automatically populated in the relevant fields of client software	
9	Compounding amount must populate in the field automatically from master table	
10	The successful bidder should develop the GUI and functionality as per requirements of the Guwahati Police	
11	The GUI should be lingual i.e. English and local state language	
12	It should be possible to integrate payment gate way operator with the system for felicitation of payment	
<b>B.</b>	<b>Handheld Device Software</b>	
13	Once the application is loaded on the hand- held device there should be no possibilities to modify the application by the user.	
	Reloading and modifying of application should be possible only by an administrator.	
14	On switching on the hand-held device, the system must give access only after validation through user ID and password.	
15	The communication between the server and hand-held device would be through GSM/GPRS/ 3G/4G or better connectivity etc.	
16	Every challan created should have a unique self-populated number.	
17	The Handheld application shall be able to access information from the main Server and display upon request, pop- up tables/codes, vehicle and license details, all types of offences, compounding amount, challan types, vehicle details, court calendar etc. in order to minimize the typing by the prosecuting officer.	

#	Minimum Requirements	Bidder Compliance (Yes/No)
18	The Handheld device should be able to access data/ information on the basis of driving license number, vehicle registration number etc. from the main server data relating to previous offences.	
19	The hand-held application software should also suggest date of challan, place of challan, name of the Court and court date etc. to further reduce typing by the officer. These fields should be designed in consultation with Guwahati Police.	
20	When a challan is issued, the name and ID of the officer should be printed on the challan.	
21	The Handheld device shall be able to input and print multiple offences on the same challan.	
22	The Handheld software shall validate challan fields automatically before the challan is printed. The system shall ensure that certain fields are properly completed before allowing the challan to be printed.	
23	When downloading application software or pop-up tables or lists to the Handheld, or uploading challan records to the Server, synchronization of Handheld system must be automatic, in order to minimize human intervention.	
24	Uploading data to the Database Server should be automatic in consistent manner.	
25	The application should provide features wherein when a driving license/ vehicle registration number is entered; it should be able to pull from the server all the details relating to the driving license holder/ vehicle owner including history of previous offences.	
26	Software should capture the list of	
	documents seized during prosecution and	
	such list must be reflected on the printed court challan.	
27	The handheld application software shall allow the user to generate a summary report to facilitate evaluation of his daily work.	
28	Once the challan is complete and saved any further editing should not be possible unless so authorized by administrator.	
29	Each hand-held device should be provided with original printed user manual and appropriate carry case for Handheld device with charger.	
30	The application software should allow online payment	

#	Minimum Requirements	Bidder Compliance (Yes/No)
31	There should be automatic rejection of payment for the settlement of expired notices or challans. Partial payment of an offence shall not be accepted by the system.	
32	The software should update DL/RC smart card with the booked offence.	
<b>C.</b>	<b>E-Challan Application Software</b>	
33	The Application Software should work in a web-based environment.	
34	The application software should be user friendly, easy to operate even by police personnel with minimum qualification of that of a head constable.	
35	The software shall provide comprehensive data back-up and restoration capability.	
36	The system shall function in web-based system where the hand-held device shall work as a node.	
37	The application software should maintain the logs of user activities to facilitate the audit trail.	
38	The system should have sufficient security features such as biometrics, password protection, audit trail, etc.	
39	The system should be able to handle the activities of all the handheld devices at one time simultaneously with huge database size of prosecution, ownerships, driving license etc. without affecting the performance.	
40	The software should be able to generate various periodical reports, summaries, MIS reports, query reply etc. as per the requirements of Guwahati Police.	
41	Administrator should be able to modify the master tables as and when required and should have the capability to push the changes to hand-held devices.	
42	Software up-gradation should be provided by the SI from time to time as per available technology without further cost impact to Guwahati Police.	
43	The Department will provide the entire data of vehicle ownership and driving license for integration with the vendor's application software.	
44	All database tables, records etc. required for various dropdown menus etc. shall also be created by the SI.	
45	The application software shall be provided by the SI to handle various processes of the prosecution required by the office of senior police officers, Courts etc.	
46	The application software should have the capability to export records in CSV, SQL and binary format	

#### 5.4.4.2 E-Challan Hand-Held Device System

#	Parameters	Minimum Specifications	Bidder Compliance (Yes/No)	Product Documentation Reference
1	<b>Make</b>	<to be provided by the bidder>		
2	<b>Model</b>	<to be provided by the bidder>		
3	<b>Core Board</b>			
a	Operating System	Latest Windows, Linux or Android OS		
b	Processor	Min 800 MHz		
c	Memory (Flash ROM)	Minimum 512 MB		
d	RAM	256 MB Min		
e	Extend Slot	Micro SD 32 GB		
4	<b>Motherboard</b>			
a	Display	Minimum 3.5-inch TFT LCD (Trans reflective screen VGA/QVGA)		
b	Touch Screen	Yes		
c	Form Factor	Any		
d	GPS	GPS and A GPS		
e	Bluetooth	Yes		
f	Wi-Fi	Wi-Fi (802.11 b/g/n)		
g	Thermal Printer	Direct thermal line printing 3 inch		
h	Barcode scanner	1D and 2 Scanner		
i	External Interface	USB HOST/RS232(Customized)		
j	Protection class	IP54		
k	Drop resistance level	1.5m		
5	<b>Camera</b>			
a	Camera	3 MP Min		
b	Camera-Video	Support still image and video capture		
6	<b>Keypad</b>			
A	Front	QWERTY 42 Keys function key can be soft key		
7	<b>Interface</b>			

#	Parameters	Minimum Specifications	Bidder Compliance (Yes/No)	Product Documentation Reference
a	Mini-USB Connector	USB2.0 connection		
b	SIM card slot	Yes		
c	TF card slot	Yes		
d	power jack	Yes		
e	Audio Jack	Yes		
<b>8</b>	<b>General</b>			
a	Battery Type	Rechargeable Li- ion battery 3000mAh		
b	Operating temperature	As per Guwahati weather conditions		
c	Storage temperature	As per Guwahati weather conditions		
d	Operating humidity	As per Guwahati weather conditions		
e	Storage humidity	As per Guwahati weather conditions		
f	Payment PINPAD	The device should have IPCI, EMV certified PINPAD as per RBI guideline for accepting payment through Credit / Debit card		
g	Enclosure	Rugged		

## 5.5 COMPONENT 5 – BACKBONE NETWORK & RF CONNECTIVITY

### 5.5.1 Network Backbone Connectivity

For all services outside of the GSCL and parts of the Assam Government systems accessed through the Guwahati Smart City networks shall all be fully compliant to the required security protocols as envisaged by respective systems for data exchange / store / forward from the Guwahati Smart City network. The expected benefits to be derived from city network backbone are:

- a) To provide inexpensive and pervasive connectivity all across the city up to last mile drop. To boost digital inclusion among departments and citizens.
- b) To provide 24\*7 uninterrupted connectivity across the city

- c) To establish a medium for quick data gathering from multiple sources and faster decision making. To act as a channel for integration of all the city services.
- d) To enable the government to have advanced communication products/platforms and better security and surveillance systems seamlessly functioning through this network backbone.
- e) SI is required to undertake estimation of bandwidth & storage requirements considering the benchmark parameters shared below.

S. No.	ICCC System Components	Consideration
1	Integrated Traffic Management System	As per designed solution requirements for real time data transmission
2	Surveillance Cameras (Dome & Bullet)	Resolution: 1920x1080
		Frame Rate: 30 FPS
3	Surveillance Cameras (PTZ)	Resolution: 1920x1080
		Frame Rate: 60 FPS
4	ANPR Cameras	Resolution: 2-MP
		Frame Rate: 50 ~ 60 FPS
5	RLVD	Video footage of incident (t-5 seconds to t+5 seconds, where it is time of incident) at required high resolution
		Minimum 4 Images of violating vehicle along with Number plate
6	SVD	Resolution: 9-MP
		Frame Rate: Frame Rate: 15 ~ 20 FPS

The SI shall be required to prepare detailed network architecture of the overall system, incorporating findings of site survey exercise. Network so designed shall be able to provide real time video stream to the City Operation Centre. The design shall also cover LAN connectivity requirements at locations such as Command and Control center, Data center that shall include setting up of structured cabling, commissioning of active and passive components for operationalization of the Integrated Security and Surveillance system.

SI is expected to provision for necessary bandwidth and connectivity during the contract period. Provisioning for bandwidth shall be done on bandwidth as a service model. City Network backbone shall provision for all the Safe & Smart initiatives for the Guwahati including City Surveillance and ITMS.

S.No.	Parameters	Minimum Specifications	Bidder Compliance (Yes/No)
1	Network Design	The network design shall at least detail out the network connectivity strategy, network scalability, traffic flow management, bandwidth optimization strategy, security strategy, site-wise bill of material, WAN drawings, GSCL Owned Network/Rental MPLS NW/Managed Leased Circuit network configuration plan for seamless integration with other infrastructure, etc. Any additional network design aspects, to meet overall scope of work also need to be documented by the SI.	
		The network solution shall be based on GSCL Owned Network/Rental MPLS NW/Managed Leased Circuit platform to manage the traffic flow including but not limited to various applications & services such as Voice, Video & Data.	
		Further it should provide capability of doing traffic classification and prioritization of applications as per the best practices and requirement of GSCL efficiently.	
		It shall be required to map each location of GSCL's network vis-à-vis the network design and provide technological solution for implementing the network solution at every point of origin of the signal / request into the ICCC and where the device shall be able to support remote commands, the same shall be possible from the ICCC.	
		It shall be ensured that the network deployed should be IPV4 as well as IPv6 compliant, as also supporting unified communications with all departmental handheld walkie-Talkies, mobile systems, RF and mobile phone communication systems, in addition to enabling Audio, Video communications from end point devices as well as from the ICCC.	
2	Operation & Maintenance	Configuration, Operation, Monitoring, Maintenance and Management of CPE Routers and MUX, Modem, OFC Cable installed for the project	
		Reporting to GSCL for all rectification & Maintenance activities in Network & Equipment's as per the SLA.	
		Orderly Start-up and Shutdown of all network infrastructure for city network backbone as per the laid down procedures mutually finalized by the GSCL and SYSTEM INTEGRATOR Incident wise reporting, Link Availability, Loss of Link	



S.No.	Parameters	Minimum Specifications	Bidder Compliance (Yes/No)
		Availability, Historical trends for availability should be reported to the GSCL	
		Daily monitoring of WAN, manual testing, Rectifying and reporting the status to the GSCL.	
		Maintaining an updated inventory / asset list of complete IT Network Infrastructure	
		Configuration / re-configuration / maintenance / monitoring management of Dynamic Host Configuration Protocol (DHCP) servers installed on core routers, routing tables.	
		Maintaining and updating IP address list and optimum management of IP addresses through DHCP/Static entry	
		Maintain and update IP address list and optimum management of IP address	
		Maintain and update LAN and WAN diagrams with relevant details	
		Replacement of supplied equipment in case if the hardware is faulty or any parts is non-functioning	
		Installation, Uninstallation, re-installation of IOS of Routers and Switches due to reasons of bugs, etc.	
		Bandwidth should be managed using tools that ensure availability of bandwidth on a remote basis. The services should ensure that the bandwidth is available to the department as per the requirements	
3	Planned Activities	<p>*For planned activities the bandwidth should be augmented before 15 days of date of actual usage, and for unplanned activities selected SYSTEM INTEGRATOR should augment the bandwidth as per tripartite discussions</p> <p>* Network should also be capable of providing Bandwidth on Demand.</p>	

S.No.	Parameters	Minimum Specifications	Bidder Compliance (Yes/No)
		<p>Communication Management (NMS proposed under this project to be used for this)</p> <ul style="list-style-type: none"> <li>a. Monitoring of quality of various communication links on</li> <li>b. LAN, WAN, leased circuit/ISDN and Liaison with ISPs Link Availability</li> <li>c. Alerts for loss of Availability</li> <li>d. Historical trends for Availability</li> <li>e. Incident-wise Reporting</li> <li>f. All incidents leading to downtimes on a link should be available at least end-of-day online</li> <li>g. Historical trending for today/yesterday/last 7 week/last month should be available</li> </ul>	
		<p>Internet, Intranet and Gateway Access, with internet access being provided to the ICCC, DC and DRC.</p> <ul style="list-style-type: none"> <li>a. Daily monitoring of Internet Leased circuits and All Intranet services.</li> <li>b. Bandwidth Utilization monitoring and reporting the status to GSCL in case if the utilization on the constant basis is exceeding 80%.</li> <li>c. DNS Server and Domain Resolution.</li> <li>d. Lookup for Internet hosts.</li> <li>e. Proxy Server Configuration, URL filtering and URL Access log.</li> <li>f. If any intranet services are not available, the status should be immediately reported to GSCL IT Cell.</li> </ul>	
4	MIS - Daily	<p>SYSTEM INTEGRATOR should also submit certain information as part of periodic review as and when required by the GSCL Daily Reports</p> <ul style="list-style-type: none"> <li>a. Summary of issues / complaints logged at the Help Desk</li> <li>b. Summary of NMS, other performance monitoring tools</li> <li>c. Network Bandwidth utilization.</li> <li>d. Summary of resolved, unresolved and escalated issues / complaints</li> </ul>	
5	MIS - Weekly	<p>Weekly Reports</p> <ul style="list-style-type: none"> <li>a. Issues / Complaints Analysis report for calls, call trend, call history, etc.</li> <li>b. Summary of network equipment rebooted.</li> <li>c. Summary of issues / complaints logged with the</li> </ul>	

S.No.	Parameters	Minimum Specifications	Bidder Compliance (Yes/No)
		OEMs. d. Summary of changes undertaken in the WAN Network including major changes like configuration changes, patch upgrades etc.	
6	MIS - Monthly	Monthly Reports a. Component wise physical as well as Network infrastructure availability and resource utilization. b. Consolidated SLA / (non)-conformance report c. Log of preventive / scheduled maintenance undertaken d. Log of break-fix maintenance undertaken e. Network Traffic Analysis, pattern identification and suggestions for improvement across network backbone Network Utilization f. Network Device Status g. Network Uptime Statistics & Threshold violation. h. Bandwidth utilization as measured at aggregation point as well as on individual links.	
7	MIS - Quarterly	Quarterly Reports a. Uptime, Downtime and performance report b. SLA compliance Report for the Quarter c. Hardware pool Report	
8	MIS - Half Yearly	Half yearly Reports a. Network infrastructure Upgrade / Obsolescence Report.	
9	Incident Reporting	Incident Reporting a. Detection of security vulnerability with the solutions / workarounds for fixing. b. Hacker attacks, Virus attacks, unauthorized access, security threats, etc.	
10	Redundancy	Redundancy in connectivity to all remote locations, connected smart devices, other field devices, the ICC, the SDC sites connected through OFC Network/Leased Circuits is essential. Should have redundancy in place to meet necessary SLA requirements.	
11	Security	Network Security being one of the most important aspects for the GSCL, it would be governed by stringent standards.	

S.No.	Parameters	Minimum Specifications	Bidder Compliance (Yes/No)
		There shall not be any network security breach. A breach is said to have occurred if access is denied, an inappropriate access is provided, data theft, malicious postings in any sites, mis-connection or wrong diversion of lawful data to any unauthorized user / portal / unauthorized external storage Security incidents could consist of any of the following:	
		Denial of Service Attack: - This shall include non-availability of service (Internet bandwidth, messaging service and other web services due attacks that consumes related network resources)	
		Data Theft: - Compromise of any kind of the network.	
		Intrusion: - Successful Unauthorized access to the GSCL	
		information system, resulting in loss of confidentiality/Integrity/availability of data.	
		Malicious Traffic: - The SYSTEM INTEGRATOR shall be responsible for isolation of the node/network in which malicious traffic is generated which may be due to virus, malware etc. on detection.	
		All active components shall have adequate security provisions, to protect itself from any security attack including but not limited to DoS, password break, malicious software, unauthorized access and recording of all access information in the active components.	
		Link Security: SYSTEM INTEGRATOR must ensure that the link provided is a secure VPN from end to end including CPE, last mile and LAN.	
		SYSTEM INTEGRATOR shall be required to bind the MAC address of the computer with IP as and when required by the GSCL.	
		All the network solution offered by the SYSTEM INTEGRATOR shall have the security provisions to prevent any unauthorized access to anybody including SYSTEM INTEGRATOR or its partners. The GSCL may reserve the right to get testing of components/ equipment supplied under this contract by any designated Third-Party Agency.	

S.No.	Parameters	Minimum Specifications	Bidder Compliance (Yes/No)
		During the currency of the project SYSTEM INTEGRATOR shall adhere and conform to the Network Security Policy of the GSCL and guidelines issued by Government of India/Government of Odisha from time to time. For all hosted sites and accesses from remote users and citizens, an OWASP or those prescribed by the STQC and CERT-IN guidelines shall have to be cleared before hosting and after any software or hardware system revision / upgrade.	

## 5.5.2 OFC Deployment Guidelines & Specification

### A) Location & Alignment of Trench

Trench must be aligned according to permission granted by authority/ agency (Road/NH/NHAI/SH/PWD/GMDA/GMC/APDCL or any others). However following guidelines must be adhered to;

- a) Trench must be done strictly within limits of the ROW permission granting authority.
- b) Trench must not be done on the road berms. Where it is not possible to avoid the road berms. GSCL/ROW authorities' concurrence is must before start of execution.
- c) Cross pits must be made manually to check presence of any underground utilities at adequate spacing.
- d) Trench boundaries shall be marked with rope / lime powder prior to digging in order to get trench in straight line.
- e) Trench shall be located at lowest point of lower area if feasible. Trench must not come over field's boundary or any heap of soil/garbage dump.
- f) Trees roots must be by passed to avoid damage while trenching and ensuring safe passage of OFC. Such negotiation should be of smooth curve.
- g) Depth will be measured from lower side (in case of ground with slope) of natural ground level. Where cable is laid through duct, depth of trench shall be measured from top of duct.
- h) Specified trench depth has to be maintained always in all types of Soil.

- i) However in certain exceptional site conditions like hills or hard strata it may not be feasible to dig up to specified depth. In such cases, duct may be laid at lesser depth as per specification with DWC pipe/GI pipe/ PCC concreting individually as per specification.
- j) In all cases of lesser depth, deviation notes will have to be raised and got approved as per table mentioned in Deviation Table. Reason for not achieving the specified depth along with type of deviation should be clearly mentioned along with the details of protection provided.
- k) Bottom of trench shall be uniform and should follow contour of ground. Width of excavated trench sufficient to lay requisite number of HDPE Ducts and GI / DWC pipes and also concreting, wherever required.
- l) To prevent soil erosion due to free rain water flowing along or inside the trench, suitable "Blockades/Stone Pitching" will have to be constructed at every 10 m with height up to ground level.
- m) In city areas trench will normally follow footpath / pedestrian way of road except where it may have to come to edge of carriage way or when cutting across road with specific permissions from road authorities responsible (such permission will be obtained from concerned authorities).
- n) Alignment of trench will be decided in consultation with GSCL site-In charge. Once alignment is marked, no deviation from alignment is permissible except with approval of GSCL site-In charge.
- o) While marking alignment only centreline will be marked and excavated trench is as straight as possible. All necessary assistance and layout shall be kept in record for marking the alignment.
- p) The ROW shall be cleared, prepared and graded to facilitate marking of the alignment of the trench. All bushes, undergrowth, stems, rocks and other obstacles shall be removed to facilitate marking the centreline. It is to be ensured that minimum amount of bushes and shrubs shall be removed to clear way and shall give all consideration to preservation of trees within ROW limits.
- q) HDPE duct(s) shall be laid in straight line, both laterally/ horizontally as well as vertically except at locations where it has to necessarily take a bend because of change in alignment or gradient of trench. Minimum bending radius of two meters shall be maintained throughout.

- r) Mentioned depth will be measured from top of laid duct. In case hard rock of volcanic (Igneous) is encountered from surface then deviation Type 'A', Type 'B', Type 'C' and Type 'D', are allowed and no NC need to be filled. However the protections for other strata are as per table below;

**DEVIATION TABLE**

Deviation Type	Variation of Depth in mm		Type of Protections
Type - A	1200	1000	Backfilling and compaction if found less depth in Acceptance Testing (AT)
Type - B	1000	800	DWC as per IS 14930 "Duraline Make"
Type - C	800	600	DWC with all around covering 1:2:4 PCC size 300 Wx300 H mm. In case of Hard Rock Surface, only DWC will be used. (Or Suggested PCC Pipe)
Type - D	600	300	DWC with all around covering with Chicken Mesh Sieve, 1:2:4 PCC size 300 Wx300 H mm with 80 mm PCC bed. (Or Suggested PCC Pipe)

**B) Precautions to be taken During Trenching**

- a) It is required that trenches are not kept open. Trenching, cable laying/ducting and backfilling activities be done parallel as far as possible to avoid any mishap or accident due to open trenches.
- b) No trench shall be kept open close to carriage way/berms. Caution boards shall be displayed at all such locations, to caution public.
- c) If warning covers of other services or operators are encountered during excavation, earth around these is gently removed to loosen them. The covers are then removed and stacked outside the trench for reuse. When underground plan of other services are exposed during excavation, adequate protection is provided at suitable intervals along the run of these plans/services and concerned authorities shall be informed.
- d) In event of inadvertent damage, location and nature of damage must be intimated to concerned department immediately. In the meantime action is taken for preventing aggravation of damage.
- e) Necessary barricades, night lamps, warning boards and required watch man shall be provided, to prevent any accident to pedestrians or vehicles or animals.

- f) Caution boards are set up at a height of 1.25 Meters above ground level so that they are visible from a distance of 25 Meters. Boards will have yellow and black background with writing in bold letters with red fluorescent paint. Boards shall be displayed at start and finish point of area in which work is under progress. Additional display boards are placed at either side of the trench. During night warning lamps (flicker lamp, lantern with glass painted red) shall be provided.
- g) Adequate precautionary measures shall be provided to prevent caving in of the trenches while excavation, due to soil condition. At such locations, width of the trenches shall be kept adequate and necessary arrangement shall be made for safe working within trenches. Arrangement must also be made for pumping out sub-soil/underground water from trench, if any.
- h) For digging the trench Manual labours shall be used and shall ensure that no damage is caused to any underground or surface installations belonging to other public utility services and/or private parties.
- i) Temporary foot-bridges are provided when trenches are made across entrance of buildings etc.
- j) Special care should be taken in digging footpaths. Proper protection shall be provided to avoid accidents. No inconvenience should be caused to pedestrians.
- k) Underground power cable is not to be moved. Electricity department to be immediately informed. Horizontal and vertical separation of 60 cm shall be maintained from power cable. As far as possible power cable should be crossed at right angle.
- l) Near foundations and boundary walls, excavation must be taken up in consultation of and in presence of owners.
- m) All necessary arrangement is made to maintain stability of trenching.
- n) Any valuable material of cultural/ historical/ archaeological interest, if found while trenching, shall be brought to the notice of GSCL and the authority concerned.

### **C) Duct Laying**

- a) Specified lengths of Ducts shall be laid using dispenser/de-coiler designed for the purpose. It is to be ensured that Duct laid is free from twist and kinks. Any collapsed portion of duct shall be removed before backfilling and duct made continuous by putting couplers.



- b) Place the duct in trench as straight as possible. However at bends horizontal and vertical minimum bending radius as per specification to be maintained.
- c) Ducts shall be laid in flat bottom trench free from stones, sharp edged debris. No water should be present in trench, while laying the duct/DWC pipe.
- d) Ends of ducts shall always be closed with End Plugs to avoid ingress of mud, water or dust.
- e) The ducts shall be joined with couplers using duct cutter and proper tools only. Do not use hacksaw to cut the duct. The duct joint shall be practically airtight to ensure smooth cable blowing using cable blowing machines.
- f) All coupler locations shall be covered with stone as per specification prior to backfilling and position marked on as built drawing (ABDw).
- g) Never place coupler along the bent portion of duct/trench in both horizontal as well as vertical direction.
- h) Wherever GI pipes are used rubber bushes shall be used at the two ends of the GI pipes to protect the damages of HDPE ducts. When GI pipes are to be laid with suitable bends, pipe bender is to be used. The bends may be obtained by making proper 'V' cut on GI pipe at two locations close to the bend and by applying bending force so that proper curvature is achieved without sharp corners. The HDPE duct shall be inserted into the GI pipe before bending. GI pipe shall be welded at 'V' cut edges after bending. None of the portion of duct will be visible at V-Cut location. It should be either closed by welding or fixing "m-seal" on clean surface.

#### **D) Duct Integrity Test (DIT)**

- a) After backfilling ducts shall be tested for integrity (air tightness and kink-free shape). Air tightness test is done by pressurizing 2 km or less duct stretch at a time. One end of duct will be closed and compressed air at 5-6kg/cm<sup>2</sup> is sent from the other end. At about 5kg/cm<sup>2</sup> pressure the inlet of compressed air will be closed. Fall in pressure should not be more than 50% in 1 (one) hour.
- b) To check that duct has not collapsed or kinked a wooden/plastic cylindrical piece (shuttle) of size 150 mm long and 0.75 X D mm in diameter where 'D' is inner diameter of duct, is blown into the duct with far end fitted with flexible wire grip/stocking. The wooden shuttle should pass through duct at far end without any obstruction within approx. 10 minutes or less.

#### **E) Back Filling**

- A. Back Filling in Rocky Terrain - Trench shall be initially filled with Sieved soil for about 50 mm which will act as a Soft cushion/Padding and then duct is placed gently over it. After that another layer of 100 mm of fine sieved soil is poured and then entire trench is backfilled with excavated material.
- B. Back Filling in Normal Soil - Under normal soil conditions duct is directly laid in trench and backfilled in same manner as explained in OFC Ducting Specifications. Adequate dry compaction shall be done before Crowning.
- C. Crowning - When backfilling has been done up to ground level a hump of soil is made to cater for soil settlement. Entire excavated soil shall be used for back filling. Crowning shall be confined over width of trench only. No surplus soil shall be left outside trench.
- D. Duct is laid through DWC/GI pipe, which is then covered with concrete as per specification. After making concrete block the curing should be done at least for 7 days. Back filling in remaining portion is done with crushed stones, which have been removed during excavation of trench. Top 100 mm of trench is to be filled with loose soil and crown of 250 mm made on trench.
- E. In case of trench aligned at slope Blockades after every 10 meter in the form of vertical walls of Flag stones or stone masonry be made to obstruct the flow of water. Rest of backfilling is as per above Para's.
- F. Back filling on public, private roads, railway crossing, and footpaths in city areas shall be performed immediately after laying HDPE ducts. Back filling at such location shall be carried out by dry compaction and thoroughly rammed; so as to ensure that original condition is achieved and made safe to traffic. All excess soil/material left out on road/footpath shall be removed without extra cost. However, along highways and cross-country, dug up material left out shall be kept as heap above trench while refilling.
- G. Back-fill shall be maintained by against wash-out, settlement below original level and rotting, until final completion of work and until first monsoon season and reinstated to keep levelled condition as acceptable to the GSCL Site -In charge and highway/local authorities without any extra payment. To ensure this, Bidder will inspect compacted trench alignment after first rain and re do work as pointed out by engineers-in-charge. Decision of GSCL Site-In charge in this regard is final and binding on Bidder.

## **F) Bridge & Culvert Crossing**

The work involves laying of HDPE ducts through GI/DWC pipes laid on the bridge. DWC pipes are to be used at such locations where sun rays and rain water don't fall on them. Either one of the following methods will be employed or same will be decided during first route survey of site engineer/route in charge/applicable authority and contractor representative.

- A. On Arch type bridges where depth up to 300 mm is not possible to dig, make a trench in bridge tar road of 150-mm width and lay DWC duct as per IS14930. Concreting 1:2:4 will be done over the DWC pipe up to the road level.
- B. In case of dry/seasonal rivers/drains, it is advisable to cross water path from river-bed and protection as per specification - A trench of 1.6 Meter or more is made. DWC ducts 117/100 mm with couplers are laid. Ducts (max 2 or as directed by Authority site in-charge) are laid through the DWC duct. DWC duct are encased/covered in 300 mm x 300 mm beam with Smooth plaster/finish, Steel member 8 mm with stirrup at every 300 mm for reinforcement. Beam should extend up to abutment of bridge. Length of DWC duct should go 5 Meter beyond the abutment of Bridge on either side and ducts should be protected up to 10 Meter all around with 1:2:4 concrete. Backfilling of trenches on slopes (entry and exit of river/drain) to be done as per specifications.
- C. In case of River/Nala with water flow, the water path may be crossed from riverbed by diverting water with temporary bunds.
- D. If points a, b & c of this procedures are not feasible then GI pipe or DWC (DWC pipes laid on the bridge. DWC pipes are to be used at such locations where sun rays and rain water don't fall on them, if direct sun rays cannot be avoided on DWC pipes then GI sheet cladding over DWC pipe can be provided) is to be clamped on the outer side of parapet wall with the help clamps as specified. Clamps and anchor bolts are to be fixed at specified spacing. Two GI pipes shall be joined / tightened properly with pipe wrench. The level of GI pipe shall always be below the road level.
- E. If all options explained in procedure not feasible in case of bridge / culverts with wheel guard, and if the PWD/NH/NHAI/SH authorities approve, the GI/DWC pipe can be placed on the wheel guard and concreted with PCC 1:2:4, with duct inside GI /DWC pipe. Proper slope at either end of culvert/bridge should be maintained and the GI pipe should continue on either side and should extend up to trench bottom 1.65 m, covered with concrete. NOTE: care needs to be taken "NOT TO REDUCE WIDTH OF CARRIAGEWAY".

- F. In case the parapet wall is non-existent or is in dilapidated condition, the clamps should be fixed on slab of bridge if permitted.
- G. Cable loop is to be left at bridge crossings in loop chambers as per specifications.
- H. Before crossing culvert the local PWD engineer/ROW authorities must be consulted in charge for future plan of expansion or re-construction and decide the alignment of trench (distance from road centre line).
- I. Leave the cable loop on each side of the culverts as specified. In case there are more than one culvert over 500 Meter span, 20-30 Meter OFC coils to be kept at 500 Meter or as per authority permission but not more than 2 locations in 1 Km length.
- J. Loop pit marker will be installed at Loop Pit.

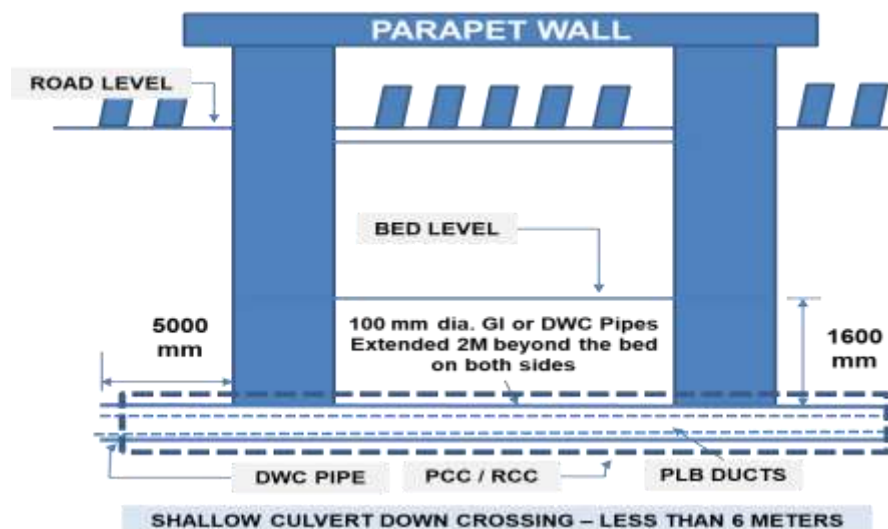


Figure 4: Small Bridge/ Culvert Down Crossing

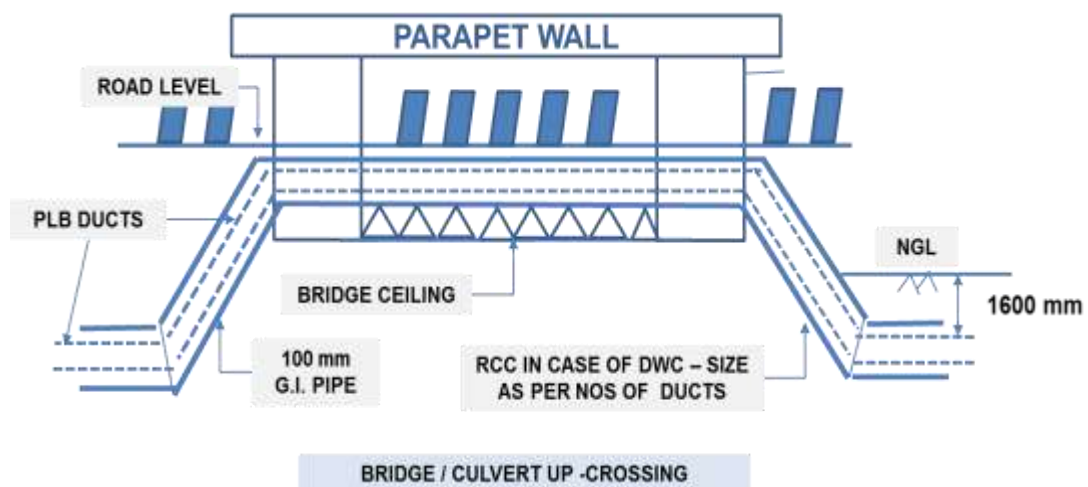


Figure 5: Bridge / Culvert UP-Crossing

## **G) Road & Railway Crossing**

- a) Roads are to be crossed either by horizontal boring or by open cut as the case may be. Suitable permission shall be obtained from Authorities concerned.
- b) In either method of road crossing, DWC duct should be used with three (2) ducts in case of National Highways (NH) or State Highways (SH). DWC duct should project 3 M outside black topping on either side in case of boring, and DWC should be provided for complete length of road crossing and should project 3 Meter outside black topping on either side in case of open trench.
- c) Railway line crossing is to be done by HDD or boring or as per the instructions of Railway authorities. Please ensure that permission to cross railways is obtained before execution.
- d) Only 100 mm dia GI pipe or DWC duct 117/100 mm, or whichever is permitted by Railway Authorities is to be used in case of rail crossing. Length of projection of GI pipe/DWC duct beyond rail lines should be kept as per approval from DRM office. HDPE ducts should be (2 Nos. extra) brought out of railway boundary and properly plugged. Loop pit to be placed one side if single track and both side if track is more than single line with 40 Meter Loop.

## **H) Concrete Methods**

- A. Concreting shall be done as per situation and local authority regulations at site, number and size of pipe to be laid/used, cross section dimension may vary to ensure proper protection to pipes as well as uniformity with any existing structure/base, on which the GI pipes or DWC duct are placed, as demanded by road authorities.
- B. At both ends of Bridges/culverts, where GI pipes slope down and get buried, concreting shall be carried out to ensure that no portion of the GI pipe is exposed and further down as required by the GSCL Site-In charge to protect pipe from any possible damage externally caused.
- C. Any damages caused to the existing structure such as footpath or base of parapet or curb wall on which GI pipes or DWC duct are placed shall be repaired and original condition re-stored to satisfaction of Road Authorities.
- D. Bidder/Contractor shall provide all the materials required for the cement concreting work at the site. Cement concrete mixture used shall be of 1:2:4 compositions i.e. 1 cement: 2 coarse sand 4 concrete aggregate of 20~40 mm nominal size. The aggregates should conformity to IS. Smooth finishing of exposed surface shall be

done with mixture of 1:3 i.e. 1 cement: 3 fine sand.(PCC should be placed in proper shuttering at both side for box PCC)

- E. When concreting is carried out in trenches, a layer of cement concrete mixture of appropriate width 80 mm thickness shall be laid along trench (This will be applicable where trench surface are uneven in Hard Strata due to stones and stones edges are sharp and possibilities of damage of ducts), before laying HDPE ducts. HDPE ducts shall be then laid above this bed of concrete as per construction specifications. After laying HDPE ducts the remaining concreting work shall be carried out to form the cross sectional dimensions 300 X300 mm.
- F. Portions where cement concreting has been done shall be cured for minimum 7 days' time to harden the surface. After curing refilling of balance depth of trench has to be done with excavated soil. In case refilling is to be done immediately like city areas or close to carriage ways, the curing over soil can be continued after refilling. It may be noted that no extra payment is admissible for arranging necessary material, layout tools and machines, or for carrying water for curing while carrying out the work.

#### **I) Stone & RCC Slab Protection**

Wherever cable is laid in cities, where very heavy human habitation exists or where construction activity can happen in near future, stone slabs (Flag stone) of size 25 mm thickness (min) and 300 mm width & 500 lengths shall be put after 30 cms padding with excavated material over duct. In case stone is not available, RCC slab of size 600mm L x 300 mm W x 40 mm T shall be used. Stretches for this protection will be decided during first route survey of Authority or PMC representative.

#### **J) Joint-Pit & Loop Pit Chambers**

The Joint-Pit Chambers are provided at every joint to keep the O.F.C. joint well protected and also to keep extra length of cable, which may be, required to attend the faults at a later date. Jointing chambers are to be prepared normally at a distance of every 2 KMs in City Area. Actual location of jointing chamber depends on length of cable drum and appropriateness of location for carrying out jointing work. The location is finalized by Engineer-in-charge. The jointing chambers are constructed either of brick masonry work at site & pre cast RCC for covers or by way of fixing pre cast RCC chambers and covers as per the instructions from site Engineer-In-charge.

This OFC Ducting for city roads, hence we have planned to keep Loop-Pit Chambers on every 200 Meters of intervals for better connectivity of field devices and sensors. A broad indicating architecture are mentioned below figures.

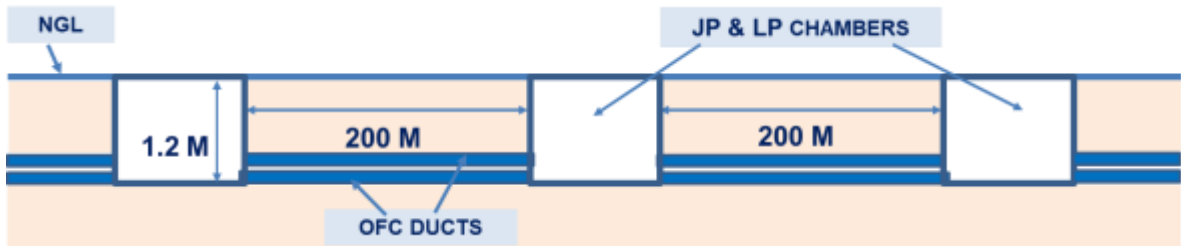


Figure 6: Joint Pit & Loop Pit Chamber (Manhole) Under Road- Elevation View

### K) Constructions of Pre-Cast JP/LP Chambers

- (i) Rectangular base plate of size 1500x1100 mm 150 mm thickness
- (ii) Rectangular middle part of JP & LP Chamber of size 1200x800 mm (internal) and height of 1200 mm and thickness of 150 mm. (Internal size except thickness of chambers)
- (iii) Rectangular top cover/ lid will be in a single or double piece of size of 1500x1100 mm and thickness of 150 mm having two handles for lifting the cover in case of any maintenance activities in centre and word “\*GSCL-OFC” engraved on it. (See the reference figure: 2 & 3). Top cover should be protected with rectangular iron sheet from the edges.

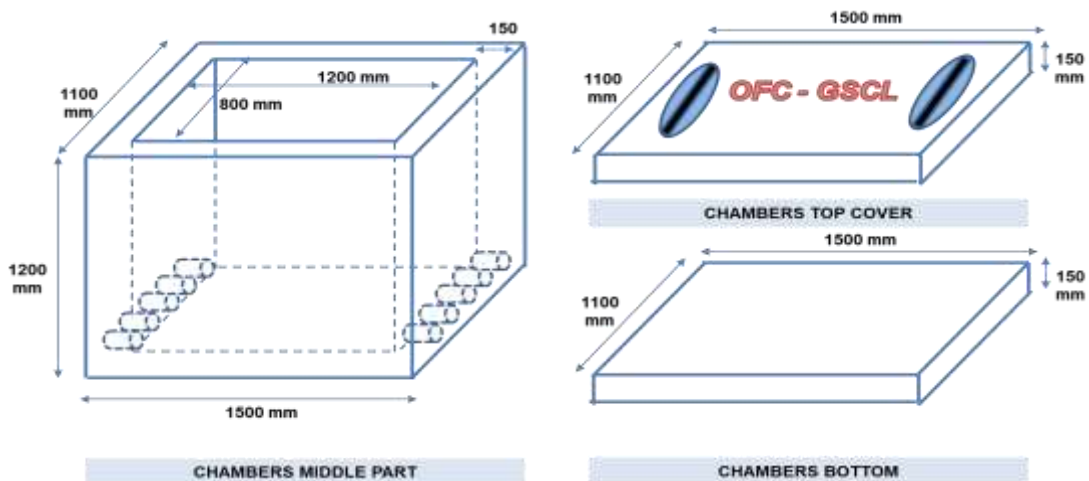


Figure 7: JP & LP Chamber Sections

<b>Pre- Installation Check-List of Joint Pit &amp; Loop Pit</b>		
Material	Reinforcement Details	10 mm Dia MS Steel Rod at 100 mm C/C on both direction
	Concrete Mix	1:2:4
	Size of Metal in RCC	20 mm
Dimension of RCC Chamber (Pre-Cast)	Height of Chamber	1200 mm for all type (internal except wall thickness)
	Inner Size of Chamber	1200*800 mm for all type
	Thickness of Chamber	150 mm (In all directions in case of Pre-Cast except top cover & Bottom)
Dimension of Chamber's LID	Diameter of LID	~1350*950 mm
	Thickness of LID	150 mm for all type
	Lift Handle	Two no. separated from the centre equally on the top of the LID for lifting purpose.
Dimension of Clamp & Accessories for Holding Joint Closure inside the RCC Chamber	Clamp Material	Galvanized Iron Strip
	Design	Refer Drawing
Dimension of Duct Entries	Duct Entry	Full Circle "O" cut in bottom of chamber wall (as per no. of ducts to be connected to that JP/LP Chambers)
	Sealing of Duct Entry	Any open space must be properly sealed with RCC
Physical Check	Curing of JP & LP Chambers	Chambers shall be kept for curing for minimum 14 days before installation & supply to site
	Workmanship	Shall be free from any cracks and damages before installation
	Surfaces	Surface of the chambers shall be smooth and shiny.
	Lift Handle	Check whether the handles are firmly bonded with concrete lid
	Duct Entry Points	Duct entries surface shall be free from sharp edges

### **L) Route Markers (RM)**



Route Indicators are also required to be placed on each JP & LP Locations and where Optical Fibre Cable changes directions like road crossing etc. The indicator shall be secured in upright position by ramming with stone and sand up to a depth of 650 mm under the ground and 550 mm should be on above ground level. and concreting in the ratio of 1:2:4 (1: cement, 2: coarse sand, 4 stone aggregate 20 mm nominal size). Necessary curing shall be carried out for the concreted structure with sufficient amount of water for reasonable time to harden the structure. The route and joint indicator shall be painted with primer before painting with oil paint. The material used should bear ISI mark. The size of each written letter should be at least 50 mm.

- a) Physical Route Markers should be done as per specifications.
- b) Physical RM should be placed at every 100 Meter on route and every corner turning, crossing, culvert, JP, LP locations.

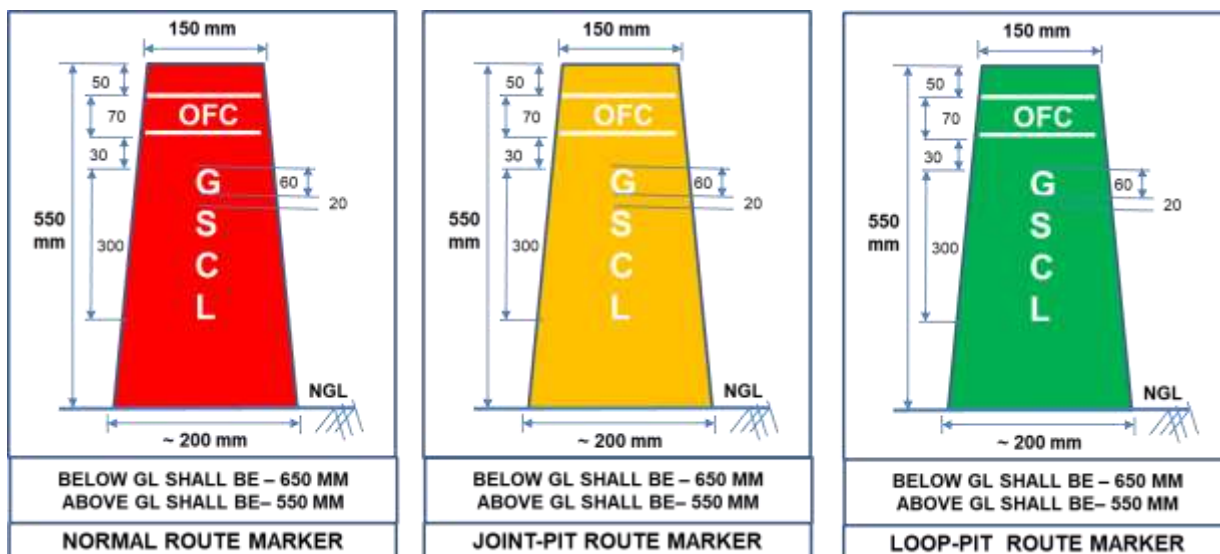
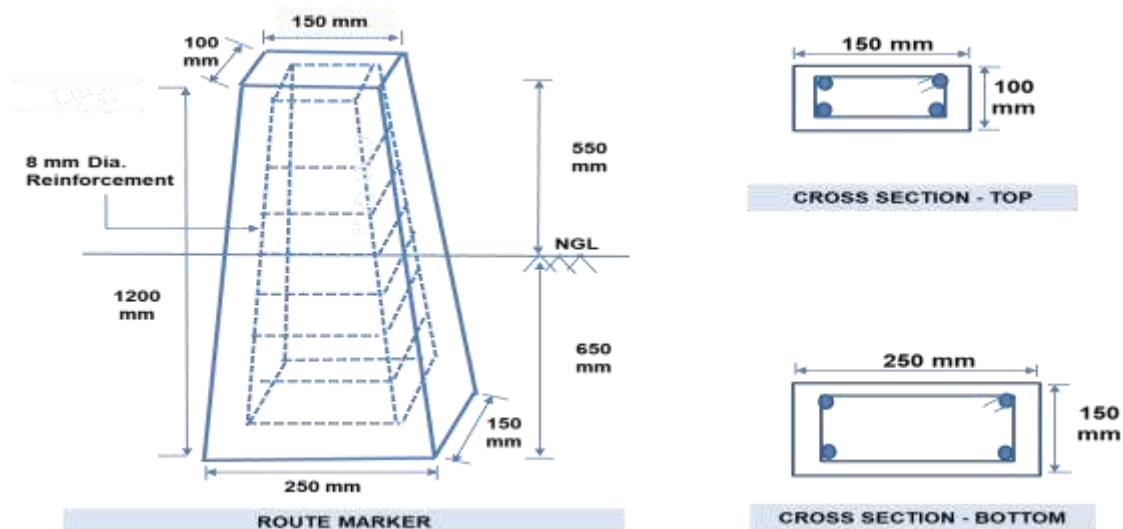


Figure 8: Route Marker Colour Marking








**Figure 9: Cross Sections of Route Markers**

ITEMS	ROUTE MARKER	
	Features	Minimum Configuration Requirements
Material	Reinforcement Details	T10 mm dia. MS Rod (4 No./Marker) stirrups dia. T8 mm at 100 mm C/C. both directions
	Concrete Mix	1:2:4
	Size of metal to be used	10 mm (Min)
Route Marker Dimension	Height	1200 mm (550 above GL, 650 below GL)
	Width x Depth (Top)	150 mm x 100 mm
	Width x Depth (Bottom - end)	250 mm x 150 mm
Labeling	As per attached Route Marker Diagram. All lettering should be embossed in concrete surface and painted with appropriate colors.	
Painting	Paint Quality	Synthetic Enamel
	Paint Approved	Asian or Equivalent
	Color of Normal Route Marker	Orange - British Color Standard (06-E-55 Orange)
	Color of Normal Splice Marker	Yellow -British Color Standard (10-E-51 Yellow)
	Color of Normal Loop Marker	Green - British Color Standard (14-E-56 Green)
Physical Observation	Curing of Route Marker	Shall be kept under curing for minimum 14 days before supply to side.
	Visual Inspection	Shall be free from crack and damages before installation
	Surface	Surface of the marker shall be smooth and shiny

**M) Electronic Route-Marker (RFID) Tagging**

- a) RFID tagging must be on OFC cable on every 100 Meter on entire route. A standard Telecommunication FRID marker shall be used.
- b) The minimum lifetime of data stored in a Smart Route Marker is 30 years
- c) Generation of custom text information for each Smart Route Marker.
- d) Options to edit all data on your underground networks from the comfort of your office or home
- e) Built-in GPS module in each Smart Route Marker Locator
- f) Acoustic GPS navigation.
- g) Display of Smart Markers in the Google Maps environment
- h) RFID Markers shall be buried at depth of 0.9 m from ground in the trench during backfilling the trench
- i) RFID Markers shall be buried at a spacing of 100 m in general to mark trench / route on country side and at approx. 50 m on zig-zag routes. At all major road crossings within the cities & at HDD locations, RFID Markers shall be placed.
- j) Trench shall be completely backfilled immediately after placing Electronic Markers
- k) Electronic Markers shall be located with electronic locator after tuning at specified frequency

Types of underground line structures and the corresponding marker frequencies			
Operating frequency	Type of device	Color of marker	Type of Marker locator
83,0 kHz	Gas pipelines		SML G
101,4 kHz	Telecommunication cables		SML T
121,6 kHz	Sewage pipelines		SML S
134,0 kHz, 169,8 kHz	Energy cables		SML E
145,7 kHz	Water pipelines		SML W

## N) Fiber (OFC) Laying

While implementation; before carrying out the actual Fiber/duct laying process, it is encouraged to carry out a detailed survey based on the outcomes of the preliminary survey carried out earlier. The purpose of the detailed survey is to undertake closer study of various existing telecommunication facilities to work out exact requirement of materials required for different items of work to finalize all the drawings and site plans

required for the execution of work as also to examine the details collected during preliminary survey and to offer necessary changes/modifications, if any.

The following are the main items of work that shall constitute the detailed survey:

- I. Closely examining the proposed cable route and prepared cable route plans
- II. Finalization of the locations for Manholes (JC & LP Chambers) and street cabinets and preparation of site plans.

Appropriate procedure to be selected for installation of termination joint box based on the type of joint enclosure and patch panel LIU in CCC site & Camera Poles. The installation manual shall contain the step by step procedure for installation.

After laying Fibre a Fibre loss report shall be maintained in below given format.

Section Name		Fiber Loss in dB (A->B)				No. Joints		Fiber Loss in dB (B->A)			
Site A		1310 nm		1550 nm		Site B		1310 nm		1550 nm	
Fib. No.	OFC Length (KM)	T. Loss	dB/KM	T. Loss	dB/KM	Fib. No.	OFC Length (KM)	T. Loss	dB/KM	T. Loss	dB/KM
1						1					
2						2					
3						3					
4						4					
5						5					
.						.					
.						.					
48						48					

The end to end loss (link budget) shall not exceed as per given formula below (for both directions A->B & B->A of Fibre).

#### Link Budget (End to End Fibre Loss) Measurement

Wavelength	Link Budget Measurement
1550 nm	<b>Fiber Length*0.21+No. of Joints*0.06+No. of Connector*0.5 dB</b>
1310 nm	<b>Fiber Length*0.31+No. of Joints*0.06+No. of Connector*0.5 dB</b>

List of items to be handed over to Authority / designated authority before handing over the respective section / location for maintenance of optical Fibre communication system

- a. The Cable Route Plan in electronic form (in kml file format on a CD) preferably using AUTOCAD and Google maps. Distances from fixed reference structures like centre of track, OHE mast, bridges, culverts, etc. shall be indicated in the route plan for easy reference in future.
- b. The Fibre Distribution Plan
- c. Measurements of Optical Parameters that includes sectional losses splice wise losses, records of dispersion measurements (in case of long-haul systems) shall be handed over to the maintenance organization.
- d. Schedule for Fibre optic system shall be prepared and maintained for future reference. Reports on adherence to the maintenance schedule shall be submitted as part of SLA compliance along with quarterly invoices. This maintenance which shall include but not be limited to following areas:

#### **O) Cable Blowing**

- a) Drum test will be carried out for every drum as per Drum Test Report format (to ensure that no damage has been caused during transit). Cable drums should be mounted on pay off stand, which is kept on plain ground for stability. Soil under the stand should be firm, not to allow stand to tilt. Process of OFC blowing is explained as under
- b) Cable blowing machine (Cable jet or any other machine) should be deployed along with a good compressor delivering 10 kg/ sq. cm pressure and 700 CFM (cu. Feet /min.) discharge.
- c) Cable drum will be loaded on payoff stand and unwound from topside of the drum. Pay off stand should be placed properly so that it does not get tilted or fall down while dispensing OFC. First half of total length should be blown through duct in one direction from the centre of the span of the duct in which cable is planned to be laid.
- d) In case when complete half of the drum length cannot be blown in a single go, cable is blown up to feasible distance by opening the coupler at that location and then balance length shall be blown and stored in figure of "8" close to trench in obstacle free space. Further blowing shall be done from this location.
- e) After blowing half-length in one direction the cable should be unwounded at the location of pay off stand and stored in a figure of "8". Then inner end of the OFC should be blown in opposite direction.

- f) Kink in OFC during blowing and after blowing must be avoided. At blowing points, the last loop of OFC should be manually pulled after cable blowing, couplers must be tightened.

**P) Earthing**

A copper rod of around 20mm dia and 0.5 m long or 1Foot X 1 Foot Copper plate 3mm thick with Copper Wire/strip brazed to plate shall be buried along with good quality of Charcoal and salt at a min. 2.5 m depth from NGL or as required so that the resistance in normal soil shall not be more than 1 ohm and in rock not be more than 2 ohm. A copper strip/braided flat 32 mm wide and 6 mm thick after bolting and welding with rod shall be brought to the surface for bonding with the optic Fibre armour. Specially made clamp, made of steel, will also be used for bonding the braided copper wire with the copper rod and with cable armour for avoiding corrosion and galvanic currents. Multiple pits may be required in some of the locations where the soil resistivity is high. However, under normal circumstances a single pit would be enough at the locations of good soil conductivity.

**Q) Record Keeping**

All measurements will be recorded in Measurement Sheet / Chainage sheet and reported on a daily basis duly signed jointly GSCL and Contractor representative as per format attached in Annexure- B.

**R) Acceptance Testing**

Acceptance-Testing (AT) of all OFC network & POP sites will be carried out by GSCL or by authorized PMC/person/agency/company. The civil & Optical AT procedure will be carried out as guideline in attached in Annexure - H.

### 5.5.2.1 Under-Ground (UG) – OFC Specifications

SN	Segments	Specification /Target Value	Bidder Compliance (Yes/No)
1	Trench Depth	<b><u>Open Trench</u></b>	-
		<ul style="list-style-type: none"> <li>City Area - Min 1200 mm (millimetre) for all types of Strata.</li> </ul>	
		<ul style="list-style-type: none"> <li>Hilly &amp; Hard Rock Terrain - Min 900 mm for all types of strata</li> </ul>	
		<ul style="list-style-type: none"> <li>Sharp and 90 degrees bend are not acceptable in trenching/ ducting</li> </ul>	
		<b><u>HDD</u></b>	-
		<ul style="list-style-type: none"> <li>Min 1200 mm depth at Entry and Exit Pits or normal soil and depth should be b/w 1200 mm to 2000 mm HDD travelling path.</li> </ul>	
		<ul style="list-style-type: none"> <li>Min Depth to be maintained as per soil Strata.</li> </ul>	
	<ul style="list-style-type: none"> <li>&lt;1200 mm depth not acceptable in HDD except in NH/SH/End to End CC/BT Road where authority not allowed to give open trench permission and it should be in writing.</li> </ul>		
2	Trench width	<ul style="list-style-type: none"> <li>400 mm at top and 300 mm at bottom, width can vary to ensure ease of duct laying.</li> </ul>	
3	Duct laying	<ul style="list-style-type: none"> <li>HDPE Duct 1 Numbers (RED and GREEN) or as approved by authority (GSCL). For Crossings, specifications for the respective crossings to be followed if specified.</li> </ul>	
4	Stone Slab at Built up area / Coupler Location	<ul style="list-style-type: none"> <li>Stone slab (Min 25 mm Thickness X 300 mm width X 500mm lengths at built up/heavy habitat area.</li> </ul>	
		<ul style="list-style-type: none"> <li>Coupler to be Covered with - Red Stone/Farsi stone slab or Cast slab (Min 25 mm Thickness X 300 wide X 1000 mm length) protruding at-least 100 mm outside the Coupler position on all sides. Stone to be laid after 1ft backfilling then do complete backfilling and position marked on As built drawing. Stone slab +/- 25% tolerance acceptable only in width and Length.</li> </ul>	
5	Joint Pit / Loop Pit / Splice Chamber - (Access Ring & Last Mile)	<b><u>City Area</u></b>	-
		<ul style="list-style-type: none"> <li>Dimension of JP &amp; LP Chamber - Internal 1200 x 800 x 1200 mm (Length x Width x Height) with wall size of 150 mm all direction.</li> </ul>	
		<ul style="list-style-type: none"> <li>Joint Pit – At <u>every 2.0 KMs</u> or as per OFC length but not less than 2 KMs</li> </ul>	

SN	Segments	Specification /Target Value	Bidder Compliance (Yes/No)
		<ul style="list-style-type: none"> <li>Loop Pit – At Every 200 Meter depend on feasibility and Authority will decide final distance and single chamber Camera Pole site.</li> </ul>	
		<ul style="list-style-type: none"> <li>Joint Pit Chamber/Loop Pit Chamber to be installed with top Lid at 0.0 mm depth from Natural ground level (NGL) in pre-caste cylinder type chamber for easy operations.</li> </ul>	
		<ul style="list-style-type: none"> <li>If sufficient space is not available due to utilities /congested/Hilly area site engineer will decide dimension with consultation of area manager but not less than 600*600*600 mm (L*W*D)</li> </ul>	
		<ul style="list-style-type: none"> <li>Lid Depth must be measured from natural ground level (NGL) and not the crown level. Crowning is to be done after reaching ground level.</li> </ul>	
		<ul style="list-style-type: none"> <li>Loop of 20-30 Meter to be placed in Loop Chamber</li> </ul>	
		<ul style="list-style-type: none"> <li>Loop of 10-20 Meter in Joint Chamber from both ends</li> </ul>	
		<ul style="list-style-type: none"> <li>RCC Rectangular/Cylinder Chamber can be constructed as per specification at zero lid depth from NGL (Normal Ground Level).</li> </ul>	
6	GI Pipe for protection	<ul style="list-style-type: none"> <li>As per IS-1239, Diameter 50/75/100 mm (Recommended is 100 mm dia) class B</li> </ul>	
7	DWC duct for Protection	<ul style="list-style-type: none"> <li>As per IS-14930, Diameter 117/100 mm for 2 No. of HDPE Duct.</li> </ul>	
8	Clamps to Hold GI/DWC	<ul style="list-style-type: none"> <li>GI Clamps with Fischer Bolts; 6 mm Thick X 30 mm Wide, Max. Spacing 1.5 Meter,</li> </ul>	
9	Duct Lengths	<ul style="list-style-type: none"> <li>Recommended in Multiples of 500 Meter for open trench and Multiples of 100/200 Meter for HDD and Multiples of 100/200 Meter Open trench in Intracity else to be discussed and agreed with applicable authority.</li> </ul>	
		<ul style="list-style-type: none"> <li>All duct must be encapsulated with End Plug &amp; Simple Plug</li> </ul>	
10	Bend Allowed in Duct	<ul style="list-style-type: none"> <li>Minimum bending radius 2 Meter</li> </ul>	
11	DIT	<ul style="list-style-type: none"> <li>100% Length to be tested for sections &gt; 2- 4 KMs; with 5 Kg/cm<sup>2</sup> pressure before blowing by Bidder/Contractor.</li> </ul>	
		<ul style="list-style-type: none"> <li>Pressure fall should not be &gt; 50% in 1 Hour</li> </ul>	



SN	Segments	Specification /Target Value	Bidder Compliance (Yes/No)
		<ul style="list-style-type: none"> <li>DIT test to be carried out during blowing if Deployment team offer for test intimate well before to NQ (3 days before) as agreed otherwise test to be arranged at the time of AT. Min 4kms duct to be tested in every 50Kms route randomly.</li> </ul>	
		<ul style="list-style-type: none"> <li>&lt;2 Kms length coupler integrity to be test during AT by consecutive 3 coupler check or duct rod randomly &amp; &lt; 4 KM in Intercity.</li> </ul>	
12	Concrete for Protection	<ul style="list-style-type: none"> <li>PCC 1:2:4 (1 cement: 2 coarse sand: 4 coarse aggregate of 20mm nominal size; Smooth Finishing with 1:3 i.e. 1 cement: 3 fine sand plaster or Compaction by vibrator ) 300 mm X 300 mm Cross Section ( 80 mm Concrete at base of the trench if surface uneven to rest duct on base)</li> </ul>	
13	OFC Cable	<ul style="list-style-type: none"> <li>Armoured 24 F Cable (G-652D)</li> </ul>	
14	Cable Blowing Pressure	<ul style="list-style-type: none"> <li>10KG/Sq. Centimetres and 700 CFM (Cubic Feet/ Meter) Discharge</li> </ul>	
15	Splicing	<ul style="list-style-type: none"> <li>Avg. Loss per Splice(at joint 0.07 dB Max , Total Average Splice Loss - 0.06 dB(all joints average)</li> </ul>	
16	Fiber Optical Loss	<ul style="list-style-type: none"> <li>Measurement to be taken at 1550 nm (Nanometer)</li> </ul>	
		<ul style="list-style-type: none"> <li>Max loss 0.25 dB/KM of OFC Including Connector loss</li> </ul>	
17	Water Penetration Test	<ul style="list-style-type: none"> <li>1 Hr for Joint Closure at 1m Depth under water (TEC and ITU-T specification)</li> </ul>	
18	Cable Loop at Bridge Crossings	<ul style="list-style-type: none"> <li>Bridge Length Up to 50 Meter – Loop Length, on single side 60 Meter</li> </ul>	
		<ul style="list-style-type: none"> <li>Bridge Length &gt; 50 Meter – Loop on both sides 60 Meter</li> </ul>	
		<ul style="list-style-type: none"> <li>Cable Bend Radius to be min 600 mm</li> </ul>	
19	Culvert/Nala Crossings	<ul style="list-style-type: none"> <li>Preferably crossing should be from culvert/nala bed and if it's not possible then UP crossing with DWC+PCC 300 mm *300 mm and if ROW authority not allowed or narrow culvert/nala and sufficient space not available to do specified PCC then more than 150 mm*150 mm dimension PCC also acceptable but in such case if digging is possible at culvert/nala try to do the digging to avoid any obstacle due to PCC.</li> </ul>	

SN	Segments	Specification /Target Value	Bidder Compliance (Yes/No)
		<ul style="list-style-type: none"> <li>If PCC not possible to cover protection then up-crossing should be with 100 mm GI of class B</li> </ul>	
20	NH/SH Crossing	<b><u>Open Trench in Road cutting</u></b>	-
		<ul style="list-style-type: none"> <li>More than 1.2 Meter depth to be maintained after cutting the Road Surface in open trench and duct to be laid with DWC +CM+ PCC.</li> </ul>	
		<ul style="list-style-type: none"> <li>If depth is &lt;1.2 Meter due to Hard Rock protection should be DWC+CM+PCC up to road level to be done, If this procedure applied then no penalty clause will be applicable with appropriate deviations.</li> </ul>	
		<ul style="list-style-type: none"> <li>DWC pipe to be placed with min 3 Meter length coming outside road shoulder topping if depth achieved as per specification or up to the specified depth on both sides.</li> </ul>	
		<b><u>HDD</u></b>	-
		<ul style="list-style-type: none"> <li>Min Depth to be maintained as per soil Strata,&lt;1.50 Meter depth not acceptable in HDD except in NH/SH/End to End CC/BT Road where authority not allowed to give open trench permission and it should be in writing.</li> </ul>	
		<ul style="list-style-type: none"> <li>Loop Chamber to be provided on single side with 40 Meter loop in SH crossing</li> </ul>	
		<ul style="list-style-type: none"> <li>Loop Chamber to be provided on both side with 40 Meter loop in NH crossing</li> </ul>	
		<b><u>Moulling</u></b>	-
		<ul style="list-style-type: none"> <li>1.20 Meter Depth to be maintained as per Soil Strata(As per inter/ Intra-city specification) and DWC to be placed at both ends protruding out by 3 Meter or up to the specified depth</li> </ul>	
		<ul style="list-style-type: none"> <li>In case of multiple road crossings, Loop Chamber to be placed at every 500 Meter.</li> </ul>	
21	Railway Crossing	<ul style="list-style-type: none"> <li>Crossing to be done by HDD/Moulling only</li> </ul>	
		<ul style="list-style-type: none"> <li>2 Nos. Extra HDPE Ducts more than planned Nos of Duct on that Route to be laid and to be properly plugged.</li> </ul>	
		<ul style="list-style-type: none"> <li>Loop chamber to be provided on one side with 40 Meter Loop in case of Single Track.</li> </ul>	
		<ul style="list-style-type: none"> <li>Loop chamber to be provided on both side with 40 Meter Loop in case of more than 1 Track.</li> </ul>	
22	Seasonal Drains/Rivers	<ul style="list-style-type: none"> <li>Preferably crossing to be done by clamping along with the bridge</li> </ul>	

SN	Segments	Specification /Target Value	Bidder Compliance (Yes/No)
		<ul style="list-style-type: none"> <li>If above option is not feasible then, Trench depth should be &gt;1.60 Meter on river bed for open trench and DWC+PCC protection with U-clamp of 1 Meter length to be placed with covering of DWC for extra grip of DWC duct</li> </ul>	
		<ul style="list-style-type: none"> <li>Additional protection to be provided after jointly discussing with all respective authority</li> </ul>	
		<ul style="list-style-type: none"> <li>HDD can be done for both seasonal and temporary drains but at least 3.0 Meter of depth will be maintained from river bottom soil level.</li> </ul>	
23	Earthing	<ul style="list-style-type: none"> <li>At Joint Pit Closest to 8 KMs, At POP/Equipment's Site , Every Cable Joint in City Area ( at every Splice Chamber for Intracity if feasible)</li> </ul>	
		<ul style="list-style-type: none"> <li>Copper rod 20 mm Diameter and 0.5 Meter long or 300 mm X 300 mm Copper plate 3 mm thick with Copper Wire/strip brazed to plate</li> </ul>	
		<ul style="list-style-type: none"> <li>Good quality of Charcoal and salt at a min. 2500 mm depth and 600 mm Diameter</li> </ul>	
		<ul style="list-style-type: none"> <li>Resistance in normal soil shall not be more than 1 Ohm and in rock not be more than 2 Ohm.</li> </ul>	
24	Route Markers	<ul style="list-style-type: none"> <li>Every 200 Meter and at Major Crossing, Major Trench Deviation or route diversion at both end</li> </ul>	
		<ul style="list-style-type: none"> <li>RCC (1:2:4) of length 1200 mm ± 20 mm with bottom cross-section of 250 mm x150 mm ± 10 mm, Tapering to 100 mm x 200 mm ± 10 mm.</li> </ul>	
		<ul style="list-style-type: none"> <li>Embossed "OFC-GSCL" with Color Codes as per Specifications</li> </ul>	
		<ul style="list-style-type: none"> <li>650 mm length of route marker shall be buried underground, and 550 mm shall be exposed (± 20mm)</li> </ul>	
		<ul style="list-style-type: none"> <li>To be install at 0.5 Meter from back of the trench (away from the road center).</li> </ul>	
		<ul style="list-style-type: none"> <li>Electronic Route Markers shall be buried at depth of 0.9 Meter from ground in the trench during backfilling the trench and at 100 Meter Distance, wherever applicable</li> </ul>	
25	Linear and Ring Path	<ul style="list-style-type: none"> <li>Linear and Ring path will be by separate trenching and minimum gap in both trenches would be &gt;2 Meter in both Open and HDD method</li> </ul>	
		<ul style="list-style-type: none"> <li>If gap &lt;2.0 Meter in both path by any method will be called SPOF (Single Point of Optical Failure) and appropriate approved deviation is must.</li> </ul>	

### 5.5.2.2 Over-Head (OH) - OFC

As a Smart City we discourage to deploy the OFC on overhead due to frequent OFC cut on OH and aesthetic looks. If there are no any options to deploy the UG-OFC then we consider the overhead OFC deployment.

S. No.	Item / Measure	Specification /Target Value	Bidder Compliance (Yes/No)
1	Aerial Cable	<b>Permanent Aerial Cabling</b>	
		<ul style="list-style-type: none"> <li>GI/MS (Silver color painted) pole to be used as per drawing. which approved by GSCL</li> </ul>	
		<ul style="list-style-type: none"> <li>Proper porcelain pulley or metal pulley or supporting clamps to be used for OFC rolling as per provided pics.</li> </ul>	
		<ul style="list-style-type: none"> <li>Pole should be undergrounded at least 1 M and fix with proper 1:2:4 concreting(200mm(dia)*500mm(Height) all-around of pole</li> </ul>	
		<ul style="list-style-type: none"> <li>Approx. 2- 3MM dia GI string wire to be used for support of OFC and OFC not to be tighten directly by wire.</li> </ul>	
		<ul style="list-style-type: none"> <li>OFC loop approx. 10 M to be kept at every 5th pole or every turning point with mounted "O" ring or clamp on pole loop radius should not be less than 0.6M</li> </ul>	
		<ul style="list-style-type: none"> <li>OFC closer should be kept in proper way so that OFC should not be bend.</li> </ul>	
		<ul style="list-style-type: none"> <li>Pole can be placed at every 20-30 Meters intervals.</li> </ul>	
		<ul style="list-style-type: none"> <li>2.0 to 3.0 mm GI wire to be laid with OFC with proper small pipe clamps (adjustable clamps) and proper clamp with poles.</li> </ul>	
		<ul style="list-style-type: none"> <li>OFC not to be tighten directly by string wire</li> </ul>	
3	OFC Cable	<ul style="list-style-type: none"> <li>ADSS 24 F Cable (SM Futureguide SR-15e Bend Insensitive)</li> </ul>	

### 5.5.2.3 Network Rack – 42U

ITEMS	NETWORK RACKS	
	Features	Minimum Configuration Requirements
NW RACKS - 42U	Size	Standard 24" (600mm) width and 42" (1050mm) depth for optimal use of floor space

ITEMS	NETWORK RACKS	
	Features	Minimum Configuration Requirements
	Reverse & Front Doors	Locking, removable, reversible front and rear doors
	Side Panels	Locking, removable side panels keyed alike with doors
	Accessories	Pre-installed casters and leveling feet; Rolls through standard 7-foot doorway
	Standards	Meets all enclosure requirements towards PCI DSS (Payment Card Industry Data Security Standard) Compliance

#### 5.5.2.4 Optical Fiber Cable (OFC)

ITEMS	OFC	
	Features	Minimum Configuration Requirements
OFC	Core	24 F (3 Tube – 8F Core in each Tube)
	ITU-T Standards	OFC Cables must be as per the ITU-T standard G.652D or G.655D Non-Zero Dispersion-Shifted Fiber – <b>Armoured Optical Fibre Cable.</b>
	Attenuations	0.21 dB / Km for each individual Fibre.
	Tensile strength:	The cable shall withstand a load of value $\leq 9.81 \times 2.5 \times W$ Newton, where 'W' is the weight of 1Km of the cable and the strain $\leq 0.25\%$
	Crush load:	The cable shall sustain a compressive load of 4 KN/100x100mm.
	Impact load:	Shall withstand an impact caused by a mass of weight of 50 N.
	Torsion load:	Shall withstand a load of 100 N for 2m cable length.
	Water penetration:	Shall meet or exceed the limit as per latest TEC and ITU-T specification.
	Cable bend:	Minimum-bending radius will be 20D, where 'D' is outer dia of the cable.
	Others:	Shall meet the latest TEC and ITU-T specification.
	PMD & CD	The manufacturing PMD and CD values should be as per the standards.

### 5.5.2.5 ADSS Optical Fiber Cable (OFC)

#	Parameters	Minimum Specifications	Bidder Compliance (Yes/No)
1	Fiber - Type	ADSS - Single Mode (G.652D)	
2	Wavelengths (nm)	1310/1383/1550	
3	Maximum Attenuation (dB/km)	On 1310 nm $\leq 0.35$ dB/km On 1550 nm $\leq 0.25$ dB/km'	
4	Polarization Mode Dispersion(PMD)	Less Than or up to $\leq 0.2$ ps/km <sup>1/2</sup>	
5	Zero Dispersion Slope	Less Than or up to $\leq 0.092$ ps/nm <sup>2</sup> .km	
6	Peak Coating Strip Force	1.0~8.9 N	
7	Temperature Cycling Induced Attenuation @1310 nm,1550 nm,1625nm(-60°Cto+85°C)	Less Than or up to $\leq 0.05$ dB/km	

### 5.5.2.6 HDPE Duct (PLB Type)

ITEMS	HDPE DUCT	
	Features	Minimum Configuration Requirements
HDPE DUCT	ISI Standards	1. IS: 4984 - 1995 - Specification for High Density Polyethylene Pipes for Water Supplies. 2. IS: 7328 - 1992 - High-density polyethylene materials for moulding and extrusion. 3. IS: 2530 - 1963 - Methods for Tests for polyethylene moulding materials and polyethylene compounds. 4. ASTM: D-638, Type-IV Specimens 6993 - Test Method for Environmental Stress-Cracking Ethylene Plastics.
	Size	40 mm outer dia & 32 mm internal dia
	Service Life	50 Years
	Color	Orange & Yellow
	Materials	The material used in the manufacture of ducts shall contain suitable UV-Stabilizers in required proportions such that ultra violet rays do not affect the ducts

### 5.5.2.7 Joint Closure (Splice Closure)

ITEMS	JOINT CLOSURE (JC)	
	Features	Minimum Configuration Requirements
JOINT CLOSURE	Water Penetration	Standard and water tight to avoid any water penetration inside the closure.
	Size	180mm(Diameter with clamp) x 540mm long
	Splice Capacity	Splice capacity of 96F

### 5.5.2.8 Patch Panel (LIU)

ITEMS	PATCH PANNEL (LIU) & CONNECTOR (8 Port & 48 Port)	
	Features	Minimum Configuration Requirements
PATCH PANNEL (LIU)	Mating Cycle	1000
	Ferrule Size	2.5 mm Ceramic
	Typical Insertion Loss	0.25 - 0.30 dB
	IEC Specification	61754-4

## 5.5.3 Transmission Equipment Specifications (POP Sites)

### 5.5.3.1 Core Router

S. No.	Minimum Specification from Day 1	Compliance (Y/N)	Product Doc. Reference
1	Make: <to be provided by the bidder>		
2	Model: <to be provided by the bidder>		
3	Should be 19" Rack Mountable Modular Router		

S. No.	Minimum Specification from Day 1	Compliance (Y/N)	Product Doc. Reference
4	<p>Each Router shall have below routed ports -</p> <ul style="list-style-type: none"> <li>i) 32xSFP+ ports, populated with <ul style="list-style-type: none"> <li>- 16x10Gbps, 10Km SM Transceivers</li> <li>- 4x10Gbps 40Km SM transceivers</li> <li>- remaining 12xSFP+ should support both 1Gbps and 10Gbps transceivers for future scalability.</li> </ul> </li> <li>ii) 12x40Gbps QSFP ports, populated with <ul style="list-style-type: none"> <li>- 8x40Gbps, 10km SM Transceivers to connect to PoPs</li> <li>- 4x40Gbps Cables/Transceivers (Multimode) required to connect Data Center Appliances as per design requirement..</li> </ul> </li> <li>iii) all proposed transceivers should be from same Router OEM</li> <li>iv) All proposed transceivers should be hot swappable.</li> <li>v) Port requirement should not be meet with adapters/breakout cables.</li> <li>vi) All ports should be dedicated/modular on a single router chassis. No adapter, converter or breakout cables to be used to meet port requirement.</li> </ul>		
5	Should have redundant Route Processor/Route Engine		
6	Each Router shall have redundant AC power supply		
7	Should have a minimum capacity of 2Tbps		
8	Should support up to 16K MAC addresses.		
9	<p>Shall support</p> <ul style="list-style-type: none"> <li>- minimum 256K IPv4 and IPv6 routes</li> <li>- minimum 4K multicast routes</li> </ul>		
10	Should have minimum 32GB RAM		
	<b>Redundancy</b>		
11	Hot swappable Redundant AC Power Supply and fans		
	<b>Technology</b>		
12	Support for Ethernet VPN (EVPN)		
13	Virtual Private LAN service (VPLS) /equivalent		
14	MPLS label-switching (LSR) routers		
15	MPLS-PE (Provider Edge) Router		
16	Segment Routing (SR)		
17	Traffic Engineering over MPLS (MPLS-TE)		
18	Layer 2 MPLS		
19	Layer 3 MPLS		
	<b>Routing Protocol</b>		
20	OSPF, OSPFv3		
21	IS-IS, IS-IS for IPv6		
22	BGPv4		



S. No.	Minimum Specification from Day 1	Compliance (Y/N)	Product Doc. Reference
23	Route redistribution among above routing protocols		
24	Route summarization, Route Filtering		
25	Policy Based Routing		
26	Bidirectional Forwarding Detection (BFD)		
	<b>Segment Routing</b>		
27	Segment routing for IPv4 Segment routing for IPv6 Topology-Independent Loop-Free Alternate (TI-LFA) for faster convergence Remote-LFA Segment Routing (SR)-Any cast Segment Identifier (SID) SR and LDP integration support		
	<b>Multicast</b>		
28	IPv4 and IPv6 multicast		
29	Protocol-Independent Multicast (PIM) - i) PIM-SM ii) PIM-SSM		
30	IGMPv3		
31	IGMP snooping		
32	16K IGMP groups		
	<b>Security feature</b>		
33	Should have VRF feature		
34	RADIUS/TACACS+		
35	IPv4 and IPv6 ACL		
36	Should be able to configure IP SLA/equivalent		
37	Advanced Encryption Standard (AES)/3DES		
38	Should support Layer 2 VPN		
39	Should support Layer 3 VPN		
	<b>Layer 2 Feature</b>		
40	802.1q (VLAN) and Inter VLAN Routing		
41	Should support 802.1d (spanning tree protocol), 802.1s (multiple spanning tree protocol),		
42	Should support LACP		
43	VRRP/HSRP		
	<b>QoS</b>		
44	Should have 802.3p (CoS)		
45	Hierarchical QoS		
46	Per port QoS configuration		
47	Differentiated Services Code Point (DSCP) based QoS		
48	IP Precedence Type of Service (ToS) based QoS		

S. No.	Minimum Specification from Day 1	Compliance (Y/N)	Product Doc. Reference
49	DSCP traffic shaping		
50	Ingress and Egress Policing		
	<b>Automation</b>		
51	NETCONG/YANG/equivalent		
	<b>Other Features</b>		
52	Should have NTP feature		
53	ISSU/equivalent		
54	Shall support operating temperature range of 0°C to +40°C		
55	Shall be powered by 220-240VAC, 50Hz input		
	<b>Management</b>		
56	SNMPv3		
57	LLDP		
58	CLI, Telnet, SSH		
59	Should have 1xConsole Port		
60	Should have 1xOut of Band Management Ethernet Interface		
61	Router series should be MEF 3.0/2.0 compliant		
	<b>Security Requirement</b>		
62	FIPS-140-2		
	<b>Other Certifications/Compliance</b>		
63	EN/IEC/IEC/UL/CSA 60950-1		
64	NEBS - GR-1089-Core - GR-63-Core		
65	FCC Part 15 Class A		
66	ROHS		
	<b>OEM Criteria</b>		
67	Warranty: 5 Years 24 X 7 Support with NBD Advance Hardware Replacement comprehensive warranty.		
68	The bidder should propose complete BoM with part codes of sub-components, warranty, license, subscription for 5 years etc.		
69	The OEM should be available in India Market for last 5 years		
70	The OEM should have TAC support in India		
71	Any other components required to fulfil the Network design requirement should be mentioned and included in proposed solution		

### 5.5.3.2 DWDM/OTN Equipments for POP Sites for Backbone Connectivity

S. No.	Parameters	Minimum Specifications	Bidder Compliance (Yes/No)
A	<b>Make</b>	(Bidder to Submit)	
B	<b>Model</b>	(Bidder to Submit)	
1	<b>Architecture</b>	The DWDM/OTN offered equipment shall comply to OTN feature-sets in accordance with ITU-T Standards. The offered equipment shall have 400G OTN cross-connect capacity with licenses included at ODU0/ODUFlex Non-blocking cross-connect level based solution requirements.	
2		The DWDM/OTN equipment shall be compact & modular supporting redundancy of control card or cross-connect fabric, timing/synchronization subsystem, and control processor subsystem.	
3		Current requirement is one 100G lamda each in east and west direction link. But solution should be scalable for the Nx100G by adding MUX/DMUX & line cards as per future requirement.	
4		Equipment must support both 10G and 100G DWDM wavelength (may use difference transponder card)	
5		The system must support 1+1 Line side protection. Both 100G ports shall not be on the same card	
6	<b>Interface Support</b>	The offered system should be equipped with min. 2X 100G Port( Each 100G port should be on different modular card) having following configuration flexibility on each modules for optimal usage: Configurable as 10x10G clients & 1x100G Line. Client Ports should support ODUFlux/ODU0, ODU1, FC,1G/10GE. The ports shall support Short/Long haul applications providing flexibility to configure interfaces."	
7	<b>Wavelength Support</b>	The offered system should be able to support mixed operation of 10G/100G line rates sharing the same mux/de-mux hardware as well as be upgradable in service to carry 100 Gbit/s channels along with 10G channels.	
8		The offered system should be able to support mixed operation of 10G/100G line rates sharing the same mux/de-mux hardware as well as be upgradable in service to carry 100 Gbit/s channels along with 10G channels.	

S. No.	Parameters	Minimum Specifications	Bidder Compliance (Yes/No)
9		The offered equipment shall support OTN mapping and hierarchy offering robust OAM, protection and management features.	
10	<b>Environmental and Power Specifications</b>	The DWDM equipment shall satisfy the following environmental conditions 1) Ambient temperature: 0°C to 45°C for the DWDM. 2) Relative humidity: Up to 90% at non-condensing for the DWDM. 3) 220 to 240VACoperation	
11	<b>Link Budget</b>	The attenuation per Km for fibre shall be taken as 0.25 db per km. The link shall be designed with a fibre and OSNR margin of 3db.	
12	<b>Protection</b>	For the ODUk SNC 1+1 protection, it should be possible to configure a hold-off timer as specified in ITU-T Rec. G.798. The system must support ODUk SNC/N and SNC/I protection, supporting ODUk network restoration and OCh protection switching mechanisms.	
13	<b>Network Management System</b>	The graphical user interfaces (GUI) Management System supporting the Simple Network Management Protocol (SNMP) and its respective hardware having a management capacity of at least 25 elements of the proposed network,	
14		The offered management system should support North Bound Interface - CORBA as per TMF814 V3.0 for integration towards OSS/ umbrella management system.	
15		The management system must provide for mandatory access control through passwords. Such passwords should be checked and recorded when the action in the system. The access should allow the differentiation of the degree of authority in at least 3 different levels. The Management System should have the ability to download software centrally to all units and / or network elements when necessary.	
16		The offered equipment shall complied to applicable generic ITU-T standards & no proprietary solutions are admissible.	
17		The network management will be based on the principles of the Telecommunication Management Network (TMN), according to ITU-T Recommendation M3010.	

S. No.	Parameters	Minimum Specifications	Bidder Compliance (Yes/No)
18		The Management System must support the Simple Network Management Protocol (SNMP) management protocol as well as OA & M (Operations, Administration, and Maintenance) capabilities.	
19		Security management should cover, among other things, security of local access to the Network element and the security in access of functions resident in the system Centralized network management. The management system must have the resources to guarantee security of access to the NE, Such as creation of different types of users, record of actions performed by each user, NE access control, etc.	
20		The management system must have the features and functionalities to perform the Fault isolation with automatic correlation and tools for root failure analysis. The management system must have functions of query, filter, grouping and Recognition of alarms.	
21		Fault management must have Storage of collected information such as notifications, Performance data, user information, Equipment and alarms, among others, in order to maintain a database of for at least 90 days.	
22		The management system must provide for mandatory access control through passwords. Such passwords should be checked and recorded when the action in the system. The access should allow the differentiation of the degree of authority in at least 3 different levels. The Management System should have the ability to download software centrally to all units and / or network elements when necessary.	
23	<b>Generic ITU-T standards which equipment shall comply</b>	G.692 Optical interfaces for multichannel systems with optical amplifiers	
24		G.694.1 Spectral Grids for WDM Applications: DWDM Frequency Grid;	
25		G.697 Optical monitoring for DWDM systems	
26		G.698.1 Multichannel DWDM applications single-channel optical interfaces	
27		G.698.2 Single channel optical channel amplified multichannel DWDM applications Interfaces	

S. No.	Parameters	Minimum Specifications	Bidder Compliance (Yes/No)
28		G.709 / Y.1331 Interfaces for the Optical Transport Network (OTN)	
29		G.798 - Characteristics of the optical transport network hierarchy Functional Blocks	
30		G.870 / Y.1352 Terms and definitions for Optical Transport Networks (OTN)	
31		G.873.1 Optical Transport Network (OTN): Linear Protection	
32		G.957 Optical interfaces for equipment and systems relating to the synchronous Digital hierarchy	
33		G.959.1 Optical transport network physical layer interfaces	
34		M.3010 Principles for a telecommunications management network	
35	<b>OEM Criteria</b>	<ul style="list-style-type: none"> <li>• OEM without any JV/ Distributor Should have their own registered office in India since Last 10 years.</li> <li>• OEM without any JV/ Distributor Should have their own service center in India since Last 10 years.</li> </ul>	

### 5.5.3.3 Technical Specification of L2 Switches at POP Sites for DWDM/OTN

S. No.	Parameters	Minimum Specifications	Bidder Compliance (Yes/No)
A	<b>Make</b>	(Bidder to Submit)	
B	<b>Model</b>	(Bidder to Submit)	
1	<b>Ports</b>	24*10/100/1000 Base-TX/FX ports and 4 nos of 10G uplink ports. All ports can auto-negotiate between 10Mbps/ 100Mbps/ 1000Mbps, half-duplex or full duplex and flow control for half duplex ports.	
2	<b>Switch type</b>	Layer 2	
3	<b>MAC</b>	32k or more	
4	<b>Backplane</b>	Minimum 128Gbps Switching fabric capacity	
5	<b>Power Supply</b>	Should support redundant field replaceable power supplies	
6	<b>FAN</b>	Should have redundant field replaceable FAN unit	
7	<b>IPv4 and IPv6 Hosts Addresses</b>	Switch should support minimum of 8K IPv4 hosts or better and 4K IPv6 hosts or better	

S. No.	Parameters	Minimum Specifications	Bidder Compliance (Yes/No)
8	<b>Operating Temperatures</b>	0 degree to 55 degree, shall support 0% to 95% non-condensing humidity conditions	
9	<b>IP Route Table</b>	Switch should support minimum of 12K IPv4 routes and 6K IPv6 routes	
10	<b>Forwarding rate</b>	Packet Forwarding Rate should be 95.0Mpps or better	
11	<b>Port Features</b>	Must support Port Mirroring, Port Trunking and 802.3ad LACP Link Aggregation port trunks	
12	<b>Flow Control</b>	Support IEEE 802.3x flow control for full-duplex mode ports.	
13	<b>Protocols</b>	IPV4, IPv6	
14		Support 802.1D, 802.1S, 802.1w, Rate limiting	
15		Support 802.1Q VLAN encapsulation, IGMP v1, v2 and v3 snooping	
16		802.1p Priority Queues supporting minimum 8 hardware queues per port, port mirroring, DiffServ	
17		DHCP support with built in DHCP server and relay capabilities	
18		Support upto 4K VLANs with jumbi frame handling capability of 13K packet size	
19		Support IGMP Snooping and IGMP Querying	
20		Support Multicasting	
21		Should support Loop protection and Loop detection,	
22		Should support Ring protection	
23	<b>Access Control</b>	Support port security	
24		Support 802.1x (Port based network access control).	
25		Support for MAC filtering.	
26		Should support TACACS+ and RADIUS authentication	
28	<b>Metro Features</b>	Should support Ethernet Ring Protection offering sub 50-ms protection using ERPS as per ITU-T G.8032	
29		Should have robust OAM capabilities supporting IEEE 802.3ah, Connectivity Fault Management (CFM) IEEE 802.1ag	
30	<b>Metro Features</b>	Should support Ethernet Ring Protection offering sub 50-ms protection using ERPS as per ITU-T G.8032	
31		Should have robust OAM capabilities supporting IEEE 802.3ah, Connectivity Fault Management (CFM) IEEE 802.1ag	
32	<b>VLAN</b>	Support 802.1Q Tagged VLAN and port based VLANs and Private VLAN	

S. No.	Parameters	Minimum Specifications	Bidder Compliance (Yes/No)
33		The switch must support dynamic VLAN Registration or equivalent	
34	Traffic Policing	Network Time Protocol or equivalent Simple Network Time Protocol support	
35		Switch should support traffic segmentation	
36		Traffic classification should be based on user-definable application types: TOS, DSCP, Port based, TCP/UDP port number"	
37	Management	Switch needs to have console port for management via PC	
38		Must have support SNMP v1,v2 and v3	
39		Should support 4 groups of RMON	
40		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"	
41	OEM Criteria	<ul style="list-style-type: none"> <li>• OEM without any JV/ Distributor Should have their own registered office in India since Last 10 years.</li> <li>• OEM without any JV/ Distributor Should have their own service center in India since Last 10 years.</li> </ul>	

#### 5.5.4 Wireless RF Connectivity

- a) Bidder shall propose the best solutions of wireless RF connectivity at all ITMS Crossing (64-Nos.) Locations in Guwahati. Bidder to take care of solutions with future upgradability and inter-portability and cost-effective (Either on Rental Basis or own Deployment Basis) solutions for project life cycle.
- b) The successful bidder shall be responsible for end-to-end implementation of connectivity including the all transmission, transreceiver (BTS), CPE, civil, cabling earthing, electrical & power backup work of all the locations under this tender and shall quote and provide/supply any item of latest make and model not included in the bill of materials but required for successful implementation, commissioning as well as its management of the system.
- c) Items, which are not mentioned in the bill of material, shall be separately quoted.



- d) Any such items, which have not been quoted by successful bidder in the bid but are required for successful completion of the project no extra cost would be paid by the authority.
- e) The scope is deemed to include all components, accessories and equipment required to implement backbone communications backbone for a fully functional Intelligent Traffic Management system, CCTV, RLVD & ANPR system and E-Challan for Guwahati city regardless of whether they are explicitly mentioned or not.
- f) Locations to be identified by Bidder for proposed Towers for RF Base Stations.
- g) Existing/Proposed PoPs are not selected considering RF Tower installation. So, provisioning of RF Tower in all PoPs may not be feasible or allowed by the concerned authority/Department where PoP is located. For erecting RF tower, one may have to follow DoT regulations.
- h) Connectivity between BTS Towers to Data Centre will be fiber optics cables (OFC) and there is no any space available (or permission granted) at State Data centre to erect BTS tower.

#### 5.5.5 Wireless RF for redundant Connectivity – Short Distance

Point to Multi Point (P2MP) Master BTS Radio Specification - Shorter Distance (max. up to 10 KMs) Pole Connectivity

S. No.	Specifications	Compliance (Yes / No)
a.	Make and Model	
1	The BS radio should support 2x2 MIMO OFDM, Supporting up to 500 Mbps	
2	Radio System should operate in India ISM Band as per WPC Regulation GSR 1048(E)	
3	The Radio should support AES-128 / FIPS 197 encryption.	
4	The BS Radio System should support synchronization mechanism of transmission timing of different collocated-Sites in order to eliminate mutual interference between multiple sites through GPS synchronization.	
5	The Link should not be standard 802.11 a/b/g/n/ac-based chipset for preventing security risk over the air.	
6	Radio system should operate on TDMA/TDD mode or in any other parallel technologies. It should not be based on CSMA technology	

<b>S. No.</b>	<b>Specifications</b>	<b>Compliance (Yes / No)</b>
7	Radio System should support Channel Bandwidth of 20, 40, 80 MHz	
8	Radio should support channel incremental step size of 5 MHz	
9	The BS Radio System must deliver actual/net usable aggregate throughput of up to 500 Mbps with Single sector base station radio	
10	Radio system shall support OFDM.	
11	The Radio System should support the Quality of Service based on 4 Queue according to 802.1p/Diffserv	
12	Radio and antenna System should support smart beamforming for reducing the effect of interference	
13	Radio should support isolation between CPEs	
14	Radio should support Symmetric & Asymmetric bandwidth Configuration for Uplink & Downlink	
15	The Radio should support channel accuracy of $\pm 10$ ppm	
16	The BS Radio should support ATPC	
17	The system should have the feature of indications of current modulation available identify interference/performance each chain and both direction	
18	The Base station sector radio should support EIRP as per regulatory	
19	The Radio System must have built-in Spectrum analyser tool to find the best available frequency to be used.	
20	Radio System should support MTU size of 1700 bytes or higher increasing fragmented frame size by limiting overheads and delivering higher data for a given duration of time	
21	Radio System should support Framing/Coding IEEE802.3/U standard on Ethernet Interface to the network	
22	User must be able to define separate VLAN for management and data traffic, to isolate management traffic from user data traffic.	
23	The base station sector radio should support dual stack IPv4 & IPv6 IP Address from day one	
24	The radio should support IPv4 & IPv6 protocol filtering and prioritization	
25	The radio system should have the feature of controlling assured bandwidth management for each connected CPE, any obstruction/interference at one CPE should not have impact on the performance of other CPEs in the same sector.	
26	Latency should not exceed 20 ms with full traffic load condition	
27	The radio System should support secure protocols SNMP v1/v2c, SNMPv3 and HTTPs for management	

S. No.	Specifications	Compliance (Yes / No)
28	The BS radio should have provision to configure destinations for sending SNMP traps to network supervisors and managers	
29	Element Management software should be able to Prevent Unauthorized access to the Radio	
30	The BS radio should support RADIUS authentication to authorize the user.	
31	NTP client should be available for time and Date synchronization with NTP server of operator network and for time stamping of events logs	
32	The radio must have provision of Initiation of software reset command to either side radio from Link management software.	
33	Should have provision of Registration of CPE only from Base Station end for added security. No Registration of CPE to BS should be permitted from CPE end.	
34	Radio system should have additional SFP port for extending data for more than 100 meters	
35	Radio should support 10/100/1000 Mbps Ethernet Port with auto negotiation (IEEE 802.3)	
36	The Base station sector radio should support 90/120-degree coverage Integrated or External sector antenna.	
37	The BS radio system should be IP66, IP67 or higher for dust and water Ingress protection and attach certification by International/Government Accredited Lab	
38	The Outdoor Radio Unit Operating temperature should be -40°to +55° Celsius	
39	Humidity supported for the Base Station should be 5 to 100% condensing.	
40	Radio system should support up to 40 Subscriber per sector.	
41	Radio should support Wind speed (operational) of 170km/h.	
42	The radios should support Regulations - FCC Part 15.407 and Part 90Y; IC RSS210; CE; ETSI 301 893/302 502 WPC - GSR-1048€,EN 62638-1	

### 5.5.6 Wireless RF for Redundant Connectivity – Long Distance

Point to Multi Point (P2MP) Master BTS Radio Specification - Longer Distance (Max. up to 15-20 KMs) Pole Connectivity

S. No	Specifications	Compliance (Yes / No)
-------	----------------	-----------------------

<b>S. No</b>	<b>Specifications</b>	<b>Compliance (Yes / No)</b>
<b>a.</b>	Make and Model	
<b>1</b>	Radio System should operate in India ISM Band as per WPC Regulation GSR 1048(E)	
<b>2</b>	The Radio should support AES-128/FIPS 197 encryption	
<b>3</b>	The BS Radio System should support synchronization mechanism of transmission timing of different collocated-Sites in order to eliminate mutual interference between multiple sites through GPS synchronization.	
<b>4</b>	The Link should not be standard 802.11 a/b/g/n/ac-based chipset for preventing security risk over the air.	
<b>5</b>	Radio system should operate on TDMA/TDD mode or in any other parallel technologies. It should not be based on CSMA technology	
<b>6</b>	Radio System should support Channel Bandwidth of 20, 40, 80 MHz	
<b>7</b>	Radio should support channel incremental step size of 5 MHz	
<b>8</b>	The BS Radio System must deliver actual/net usable aggregate throughput of up to 300 Mbps with Single sector base station radio	
<b>9</b>	Radio System should support OFDM.	
<b>10</b>	The Radio System should support the Quality of Service based on 4 Queue according to 802.1p/Diffserve	
<b>11</b>	Radio should support isolation between CPEs	
<b>12</b>	Radio should support Symmetric & Asymmetric bandwidth Configuration for Uplink & Downlink	
<b>13</b>	The Radio should support channel accuracy of $\pm 10$ ppm	
<b>14</b>	The BS Radio should support ATPC	
<b>15</b>	The system should have the feature of indications of current modulation available identify interference/performance each chain and both direction	
<b>16</b>	The Base station sector radio should support EIRP as per regulatory	
<b>17</b>	The Radio System must have built-in Spectrum analyzer tool to find the best available frequency to be used.	
<b>18</b>	Radio System should support MTU size of 1700 bytes or higher increasing fragmented frame size by limiting overheads and delivering higher data for a given duration of time	
<b>19</b>	Radio System should support Framing/Coding IEEE802.3/U standard on Ethernet Interface to the network	
<b>20</b>	User must be able to define separate VLAN for management and data traffic, to isolate management traffic from user data traffic.	

<b>S. No</b>	<b>Specifications</b>	<b>Compliance (Yes / No)</b>
21	The base station sector radio should support dual stack IPv4 & IPv6 IP Address from day one	
22	The radio should support IPv4 & IPv6 protocol filtering and prioritization	
23	The radio system should have the feature of controlling assured bandwidth management for each connected CPE, any obstruction/interference at one CPE should not have impact on the performance of other CPEs in the same sector.	
24	Latency should not exceed 20 ms with full traffic load condition	
25	The radio System should support secure protocols SNMP v1/v2c, SNMPv3 and HTTPs for management	
26	The BS radio should have provision to configure destinations for sending SNMP traps to network supervisors and managers	
27	Element Management software should be able to Prevent Unauthorized access to the Radio	
28	The BS radio should support RADIUS authentication to authorize the user.	
29	NTP client should be available for time and Date synchronization with NTP server of operator network and for time stamping of events logs	
30	The radio must have provision of Initiation of software reset command to either side radio from Link management software	
31	Should have provision of Registration of CPE only from Base Station end for added security. No Registration of CPE to BS should be permitted from CPE end.	
32	Radio should support 10/100/1000 Mbps Ethernet Port.	
33	The Base station sector radio should support 90/120-degree coverage Integrated or External sector antenna.	
34	The BS radio system should be IP66/IP67 or higher for dust and water Ingress protection and attach certification by International/Government Accredited Lab	
35	The Outdoor Radio Unit Operating temperature should be -40°to +55° Celsius	
36	Humidity supported for the Base Station should be 5 to 100% condensing.	
37	Radio system should support up to 40 Subscriber per sector.	
38	Radio should support Wind speed (operational) of 170km/h.	
39	The radios should support Regulations - FCC Part 15.407 and Part 90Y; IC RSS210; CE; ETSI 301 893/302 502 WPC - GSR-1048€,EN 62638-1	

### 5.5.7 Point-to-Point (P2P) Connectivity – Long Distance

S. No.	Parameters	Specifications	Compliance (Yes / No)
1	Make	<to be provided by the bidder>	
2	Model	<to be provided by the bidder>	
3	Band Support	Radio System should operate in India ISM band as per WPC regulation GSR 1048E	
4	LOS, nLOS Operation	Radio must support LOS, nLOS operation	
5	Channel Bandwidth	Radio must support Channel Bandwidth of - 20,40 & 80 MHz	
6	Channel Spacing	System must be supported the channel step size of 5 MHz or better	
7	Channel Selection	1. Dynamic spectrum, Optimizations or Manual intervention	
		2. Automatic Channel Selection	
		3. Continual self-optimization to avoid interference	
8	Max. Output Power at Antenna Port	Up to 27dBm, can change according to active modulation	
9	Modulation	Radio must Support Modulation from BPSK to 256 QAM	
10	Duplex Scheme	Radio should have the support for Time Division Duplex (TDD) and dynamic or fixed transmit/receive ratio	
11	Architecture	Single cable between IDU & ODU distance supported up to 90 Mtrs	
12	Receiver Sensitivity	up to -93 dBm	
13	Distance Coverage	More than 40 KMs	
14	VLAN Support	VLAN support based on IEEE 802.1Q	
15	Frame Size	System should support the jumbo frame size of up to 3000 Bytes	
16	QoS	Should support as per IEEE 802.1P & DSCP	
17	Queue Support	It is mandatory for the system to support 4 QOS levels	
18	Synchronous Ethernet	System should support GPS synchronization technique to eliminate interference.	
19	Security	128 Bit AES/ FIPS 197 Encryption	

S. No.	Parameters	Specifications	Compliance (Yes / No)
20	Throughput	Actual / usable throughput of 450 Mbps	
21	Packet Per Second	up to 165000 PPS	
22	Spectral Efficiency	Minimum 10b/Hz	
23	Bandwidth	System should be able to configure symmetric & asymmetric bandwidth upload and download percentage should be user configurable.	
24	MIMO-B	System must have the support for 2x2 MIMO-B technology to increase the throughput.	
25	LAN Interface	System must have 1000Base(T) half/full duplex rate auto negotiated (802.3 compliant)	
26	IPv6 Support	System must support IPv6/IPv4 dual stack support	
27	Split Frequency Support	System should support the flexibility to configure different TX & RX frequency for master and slave radio.	
28	Spectrum Analyser Mode	Built in spectrum Analyzer. Running spectrum should not affect the link performance or outage.	
29	Support for Dynamic Spectrum Optimizer	System should support DSO technology to deliver the hitless performance.	
30	NLOS Performance	System must support 1024 subscriber for superior performance in NLOS conditions.	
31	Management	1. System should have support of IPv4/IPv6, UDP, TCP, IP, ICMP, SNMP, HTTP, FTP.	
		2. System should have support of Network Management with HTTP, HTTPs, FTP, SNMP v2, SNMPv3.	
32	Management of VLAN	System should have the support of VLAN 802.1Q	
33	Ethernet Latency	Latency should be below 10 ms with 90% load condition	
34	Antenna Type	23dBi or higher Integrated Antenna or External Antenna based on link budget.	
35	GPS Synchronization	System should support GPS synchronization technique to eliminate interference.	
36	Chipset Radio	Proposed radio should not be Wi-Fi chipset radio based on Wi-Fi Std. IEEE 802.11 n/ac	
37	Power Supply	System should support both AC & DC power supply	

S. No.	Parameters	Specifications	Compliance (Yes / No)
38	Operation Temperature	Radio must operate between -40 to 55 Degree Temperature	
39	Wind Survival	200 km/h	
40	Protection	IP66/IP67	
41	Certifications	1. MEP	
		2. FCC Part 15, RSS 210	
		3. CE,ETSI 301 893/302 502	
		4. Safety UL60950-1, IEC60950-1, EN60950-1, CSA-C22.2	
		5. EMC EN 301 489-1	

#### 5.5.8 Customer Premises Equipment's (CPE) / Client Radio – Subscriber Module

S. No	Specifications	Compliance (Yes / No)
1	Make: <to be provided by the bidder>	
2	Model: <to be provided by the bidder>	
3	Radio System should operate in India ISM Band as per WPC Regulation GSR 1048 €	
4	CPE should support maximum Tx power up to 27 dBm	
5	The Radio should support channel bandwidth of 20, 40 & 80 MHZ	
6	Radio should support channel incremental step size of 5 MHz	
7	Radio system should operate on TDMA/TDD mode or in any other parallel technologies.	
8	Modulation Technology should be OFDM - MIMO 2x2 and diversity.	
9	Radio system should support adaptive modulation from 64QAM to 256QAM.	
10	Radio System should have the features of Indications of current modulation available identify interference/performance	
11	Radio should support AES-128, FIPS 197 encryption certifications.	
12	Radio should cover distance of 10 KMS or better on availability of LoS with minimum throughput of 50 Mbps.	
13	Radio System should support throughput of at least 200 Mbps & support of capacity upgrade license further without changing hardware.	



S. No	Specifications	Compliance (Yes / No)
14	Separate VLAN for management and traffic should be supported.	
15	Radio should support MTU size of 1700 bytes or higher increasing fragmented frame size by limiting overheads and delivering higher data for a given duration of time.	
16	Radio system should have Gigabit Interface with Auto-Negotiations (IEEE802.3)	
17	Radio should support Framing/Coding IEEE802.3/U standard Ethernet Interface to the network	
18	The Radio System should support dual stack IPv4 & IPv6 - IP address from day one.	
19	The Radio System should support dual stack IPv4 & IPv6 - protocol filtering & prioritization	
20	Management VLAN, Data VLAN Transparency should be supported	
21	Latency should support lower than 25ms	
22	The Radio System should support Quality of Service according to IEEE802.1P , TOS/Diffserve	
23	CPE Radio should support smart dynamic assured capacity controlled by Base station	
24	CPE should support Radius Authentication. UL & DL bandwidth should be automatically pushed to CPE after Radius Authentication.	
25	The CPE Radio should have provision to disable temporarily connection to NW behind the CPE for Diagnostic purpose such as broadcast/multicast storm.	
26	CPE radio should have option to rate limit broadcast/multicast traffic.	
27	The CPE radio should have provision of Initiation of Soft Reset command from Link Management software	
28	Radio should support any GUI/LED/RSSI indication or audible buzzer for antenna alignment.	
29	The System should have the feature of RSSI indication to enable final alignment in azimuth and elevation planes on CPE.	
30	The Radio System should support secure protocol SNMPv2c, SNMPv3 and HTTPs for Management.	
31	For ease of field management, should be able to manage Base Station and CPEs using a single computer / Laptop	
32	The Radio System should support the upgradation of firmware/software over the air through EMS software tools.	
33	Offered Radio be either integrated antenna from or connectorized according to the link budget requirement.	
34	Input Voltage 110-240 VAC or -20 to -60 VDC	

<b>S. No</b>	<b>Specifications</b>	<b>Compliance (Yes / No)</b>
<b>35</b>	Power consumptions of Radio should be maximum <20W.	
<b>36</b>	Operating Temperature of Radio should be between -40 to 55 Degree	
<b>37</b>	Humidity supported for the Base Station should be 5 to 100% condensing.	
<b>38</b>	The link should not be standard 802.11 a/b/g/n/ac-based chipset for preventing security risk over the air.	
<b>39</b>	The Radio System should support wind speed (operational) 170 KM/H.	
<b>40</b>	The Radio should support Regulations - FCC Part 15B and FCC RSS, ETSIWPC - GSR-1048 € for wireless.	

## **5.6 COMPONENT 6 – ENABLING WORK AT TEMPORARY ICCC LOCATIONS**

At temporary locations of ICCC the interior work, furniture, desk, chair, cabins and rack server space & video hall etc. will be arrange by SI bidder. The indicative requirements are mentioned below;

### **5.6.1 Functional Requirements – ICCC (Temp. Location)**

Temporary location of ICCC and each section of ICCC shall be furnished with state-of-the-art modular furniture of reputed brand as per the functional requirement.

Workstation shall be made of pre laminated particle board top with powder coated metal support structure. Modesty partition shall be made of powder coated aluminum framing and modular aluminum panels. The hollow space inside modesty partition shall provide suitable wire management provision for both data and power. Privacy panel shall be provided with colored lacquered glass. Pedestal unit with three numbers drawers and cushion on top shall come with each workstation.

For conference room, meeting room etc. modular conference tables shall be provided with provision for adequate number of power and data point for fixing laptops and other related accessories required for modern day conferencing.

All chairs shall be ergonomically designed. Back rest shall be made of mesh type fabric. Seats shall have fabric finish with CM foam and arm rests shall be with polypropylene. Base shall be "5- star" type in black nylon.

All chairs shall have adjustment facilities for height, back rest, lumbar support, tilting, hand rest support etc.

## **5.6.2 Functional Requirements – Non-IT Work at Temp. ICCC Location**

### **5.6.2.1 Video Wall**

A video wall of approx. 6.50 x 2.5 Meter has been proposed and this will have cube with vesseless screen that fits into given wall size. An IT console will be provided below the video wall to suit IT/ Electrical cabling requirements. The Video wall shall have a clearance of 800mm from the wall to create an access alley for maintenance of the screens and equipment's of the video wall. The video wall shall be designed with adequate framing to take the load of the equipment.

### **5.6.2.2 Fire Doors**

These doors as applicable standards will be made of sheet metal with a 2-hour fire rating and will have a vision panel with a wired glass or as per manufacture specifications.

### **5.6.2.3 Acoustic Treatment**

Acoustic treatment and materials with acoustical properties are proposed in the CCC. The material used shall be rockwool insulation, perforated ceiling tiles, nitrile rubber or acoustic tiles on vertical surfaces finished with approved fabric. The doors will be provided with rubber/brush seals to account for acoustics and smooth operations.

### **5.6.2.4 Signage**

General signage (in English and Local language) and fire signage as per standard norms will be provided within the space along with a fire evacuation map at strategic locations.

### **5.6.2.5 Logo**

The logo for GSCL/ICCC shall be mounted on the wall behind the reception desk

### 5.6.2.6 Reception Wall

The wall at the backdrop of the reception table will have a texture finish with niches to house lights for the proposed logo or the feature wall

The situation room and the server room floor levels are raised by 400mm (FFL) to accommodate IT cabling. The floor in the CCC room rises from zero level to 400mm in multiples of 100mm (4 tiers) for the monitoring console system.

### 5.6.3 Technical Specifications – Non-IT Requirements

#### 5.6.3.1 Non-IT Requirements & Specifications

The functional requirements and technical specifications provided in the below sections and at other sections in this RFP are indicative and carry guiding rule. The SYSTEM INTEGRATOR is free to offer products and solutions which meet requirements of the RFP focusing on the outcome, future scalability, security, reliability and adherence to specified SLA under this RFP, in line with applicable standards & best practices adopted in the industry. The SYSTEM INTEGRATOR is encouraged to design an Optimized solution which is technically superior, innovative, proven, better in terms of functionality and is cost effective. Any specified parameters mentioned in the scope/technical requirement in the RFP may be considered if it is required for meeting current & future requirements during the contract period. The SYSTEM INTEGRATOR is fully responsible for the specified outcome to be achieved. It is essential that Fire Proof material be used as far as possible and Certification from Fire Department be taken for Command Centres before Go-Live.

#### 5.6.3.2 Civil and Architectural Work

Sl. No	Description	Bidder Compliance (Yes/No)
<b>A</b>	<b>False Ceiling (at ICCC)</b>	
1	Providing and fixing metal false ceiling with powder coated 0.5mm thick hot dipped galvanized steel tiles 595 x 595 mm with regular edge (10mm) suitable for 25mm grid supported on suitable powder coated galvanized steel grid as per manufacturer specification. The same shall be inclusive of cut outs for lighting, AC grills, Fire detectors, nozzles, etc.	
2	Providing and fixing 12 mm thick fire line Gypsum false ceiling and lighting troughs 300 mm as per design including 100 mm high cornices as lighting pelmets on G.I. frame work, in G.I. vertical supports at every 450mm c/c and horizontal runners at every 900mm c/c self-taping metal screws to proper line and level. The same shall be inclusive of making	

Sl. No	Description	Bidder Compliance (Yes/No)
	holes and required framing for fixing electrical fixtures, A.C. grills etc. GI vertical supports to be anchored to slab by means of anchor fasteners.	
<b>B.</b>	<b>Furniture and Fixture</b>	
1	Workstation size of min. 18" depth made with 1.5mm thick laminate of standard make over 18mm thick commercial board complete with wooden beading including cutting holes & fixing of cable manager etc. complete with French polish. Edges shall be factory post-formed. The desk shall have the necessary drawers, keyboard trays, cabinets etc. along with sliding / opening as per approved design with quality drawer slides, hinges, locks etc.	
2	Providing & making of storage unit with 18 mm thick MDF board along with 1.5 mm approved laminate colour outside and 2 coat of enamel paint inside the storage of size 1'6"x1'6"x2'4". The same should be provided with all the required accessories including the handle, lock, sliding channel and necessary hardware, etc. complete with French polish	
3	Cabin table of min. depth 2' made with 1.5mm thick laminate of standard make over 19mm thick commercial board complete with wooden beading including cutting holes & fixing of cable manager etc. complete with French polish.	
4	Providing, making & fixing 6" high laminated strip using 1.5mm thick laminate over 10mm thick commercial board on all vertical surface in the entire server & ancillary areas including low height partition, brick wall, partition wall, cladding etc. complete with French polish in all respect.	
5	Providing, making & fixing an enclosure for gas cylinder of Shutters and Partitions along with wooden support and 18 mm thick MDF board along with 1.5 mm approved laminate colour outside and 2 coat of enamel paint inside the shutter. The same should be provided with all the required accessories including the handle, lock, loaded hinges, tower bolt and necessary hardware etc. complete with French polish.	
<b>C</b>	<b>Partitions (wherever required as per approved drawing)</b>	
1	Providing and fixing in position full height partition wall of 125 mm thick fire line gyp-board partition using 12.5 mm thick double fire line gyp-board on both sides with GI steel metal vertical stud frame of size 75 mm fixed in the floor and ceiling channels of 75 mm wide to provide a strong partition. Glass wool insulation inside shall be provided as required. Fixing is by self-tapping screw with vertical studs being at 610 mm intervals. The same should be inclusive of making cut-outs for switch board, sockets, grill etc. It shall also include preparing the surface smoothly and all as per manufacture's specification etc. finally finishing with one coat of approved brand of fire-resistant coating.	
2	With glazing including the framework of 4" x 2" powder coated	

Sl. No	Description	Bidder Compliance (Yes/No)
	aluminum section complete (in areas like partition between server room & other auxiliary areas).	
3	Providing & fixing Fire Rated Wire Glass minimum 6 mm thick for all glazing in the partition wall complete. (External windows not included in this).	
4	All doors should be minimum 1200 mm (4 ft.) wide.	
<b>D</b>	<b>Flooring (wherever required as per approved drawing)</b>	
1	The SYSTEM INTEGRATOR shall procure and install a raised floor to match the floor height and room aesthetic in accordance with the approved final layout and design. The SYSTEM INTEGRATOR shall consider standard parameters for developing the final height, width, point of load, and uniform distribution load of the raised floor for the rooms based on type of furniture and overall load.	
2	<p>The SYSTEM INTEGRATOR shall ensure the following features and parameters are considered while designing and commissioning the raised floor:</p> <ol style="list-style-type: none"> <li>1. Point of Load (PoL) shall be considered 20% more than the actual load</li> <li>2. Uniform Distribution Load shall be calculated according to the final Point of Load</li> <li>3. Noise- Proof</li> <li>4. Fireproof</li> <li>5. Maintenance window for easy access to under the raised floor</li> <li>6. Separate electrical and data cable tray under the raised floor</li> <li>7. Face of floor tiles shall conform to the aesthetic part of the approved design</li> </ol>	
3	The SYSTEM INTEGRATOR shall perform load test and noise test of the constructed raised floor.	
4	<p>The SYSTEM INTEGRATOR shall complete the following requirements for the raised flooring panels:</p> <ol style="list-style-type: none"> <li>1. Floor shall be designed for standard load conforming to BIS 875-1987.</li> <li>2. Panels shall be made up of 18-gauge steel of 600 mm x 600 mm size treated for corrosion and coated with epoxy conductive paint (minimum thickness 50 Micron).</li> <li>3. Raised flooring covering shall be antistatic, high-pressure laminate, two (2) mm thick in approved shade and color with PVC trim edge. It shall not make any noise while walking on it or moving equipment. Load and stress tests on floor panels shall be performed as part of acceptance testing.</li> </ol>	

Sl. No	Description	Bidder Compliance (Yes/No)
<b>E</b>	<b>Painting</b>	
1	Providing and applying Fire retardant paint of pre-approved make and shade to give an even shade over a primer coat as per manufacturers' recommendations after applying painting putty to level and plumb and finishing with 2 coats of fire-retardant paint. Base coating shall be as per manufacturer's recommendation for coverage of paint.	
2	For all vertical Plain surface.	
3	For fire line gyp-board ceiling.	
4	Providing and laying POP punning over cement plaster in perfect line and level with thickness of 10 - 12 mm including making good chases, grooves, edge banding, scaffolding pockets etc.	
5	Applying approved fire-retardant coating on all vertical surfaces, furniture etc. as per manufacturer's specification.	

#### 5.6.4 Shifting of ICCC to Permanent Building

Shifting of all IT & Non-IT equipment's, including the DG, UPS/Power Plant equipment's will be under SI scope of work.

SI shall be responsible for the proper handling of all equipment's while shifting, installation & commissioning at new permanent ICCC building. New permanent ICCC building will be having all interior and new furniture works readily available, hence old furniture (which will be not used in permanent ICCC) from temporary ICCC location will be auctioned.

### 6.0 ANNEXURE I: DETAILED WORK PHASES AND CONSIDERATIONS

#### 6.1.1 Requirement Survey Phase

The SI must perform the detailed assessment of the IT Solution requirements as mentioned in this RFP. Based on the understanding and its own individual assessment, SI shall develop & finalize the System Requirement Specifications (SRS) in consultation with GSCL and its representatives. While doing so, SI at least is expected to do following:

- i. SI shall study and revalidate the requirements given in the RFP with GSCL and submit as an exhaustive FRS (functional Requirement Specification) document.
- ii. SI shall develop the FRS and SRS documents.

- iii. SI shall develop and follow standardized template for requirements capturing and system documentation.
- iv. SI must maintain traceability matrix from SRS stage for the entire implementation.
- v. SI must get the sign off from user groups formed by GSCL.
- vi. For all the discussion with GSCL team, SI shall be required to be present at GSCL office with the requisite team members.
- vii. Prior to starting the site clearance, the SI shall carry out survey of field locations as specified in Annexure VIII, for buildings, structures, fences, trees, existing installations, etc.
- viii. The infrastructure of existing traffic signal and other street ICT infrastructure may need to be dismantled and replaced with the new systems which are proposed and required under the scope of the project. The infrastructure like poles, cantilevers, cabling, aspects etc. should be reused to derive economies for the project with prior approval of GSCL. The dismantled infrastructure shall be delivered at the GSCL designated location without damage at no extra cost.
- ix. All existing road signs which are likely to be affected by the works are to be carefully taken down and stored. Signs to be re-commissioned shall be cleaned, provided with new fixings where necessary and the posts re-painted in accordance with GSCL guidelines. Road signs, street name plate, etc. damaged by the SI during their operation shall be repaired or replaced by SI at no additional cost.
- x. The SI shall directly interact with electricity boards for provision of mains power supply at all desired locations for field solution. GSCL shall facilitate the same. The recurring electricity charges will be borne by GSCL as per actual consumption.

### **6.1.2 Design Phase**

The SI shall build the solution as per the Design Considerations detailed in **Section 5**. The solution proposed by SI should comply with the design considerations requirements as mentioned therein.

### **6.1.3 Project Development Phase**

The SI shall carefully consider the scope of work and provide a solution that best meets the project's requirements. Considering the scope set in this RFP, the SI shall carefully consider the solutions it proposes and explicitly mention the same in the technical proposal. The implementation of the application software will follow the procedure mentioned below:

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

- 1) SI will be responsible for supplying the application and licenses of related software products and installing the same so as to meet project requirements.
- 2) SI shall have provision for procurement of licenses in a staggered manner as per the actual requirement of the project.



- 3) The SI shall perform periodic audits to measure license compliance against the number of valid End User software licenses consistent with the terms and conditions of license agreements, volume purchase agreements, and other mutually agreed upon licensed software terms and conditions. The SI shall report any exceptions to license terms and conditions at the right time to GSCL. However, the responsibility of license compliance solely lies with the SI. Any financial penalty imposed on GSCL during the contract period due to license non-compliance shall be borne by SI.
- 4) SI shall also supply any other tools & accessories required to make the integrated solution complete as per requirements. For the integrated solution, the SI shall supply:
  - a) Software & licenses.
  - b) Supply tools, accessories, documentation and provide a list of the same. Tools and accessories shall be part of the solution.
  - c) System Documentation: System Documentation both in hard copy and soft copy to be supplied along with licenses and shall include but not limited to following. Documentation to be maintained, updated and submitted to GSCL regularly:
    - Functional Requirement Specification (FRS)
    - High level design of whole system
    - Low Level design for whole system / Module design level
    - System Requirements Specifications (SRS)
    - Any other explanatory notes about system
    - Traceability matrix
    - Technical and product related manuals
    - Installation guides
    - User manuals
    - System administrator manuals
    - Toolkit guides and troubleshooting guides
    - Other documents as prescribed by GSCL
    - Quality assurance procedures
    - Change management histories
    - Version control data
    - SOPs, procedures, policies, processes, etc. developed for GSCL
    - Programs
    - Entire source codes
    - All programs must have explanatory notes for understanding
    - Version control mechanism
    - All old versions to be maintained

- Test Environment
- Detailed Test methodology document
- Module level testing
- Overall System Testing
- Acceptance test case

These documents need to be updated after each phase of project and to be maintained updated during entire project duration. The entire documentation will be the property of GSCL.

#### 6.1.4 Integration Phase

The Command and control center should be integrated with feeds of all component under the ICCC Project. The SI shall provide the testing strategy including traceability matrix, test cases and shall conduct the testing of various components of the software developed/customized and the solution-as-a-whole. The testing should be comprehensive and should be done at each stage of development and implementation.

The broad scope of work to be covered under Integration Phase will include the following, but is not limited to:

S. No.	Departments /Systems	Minimum Integration Requirements
1	City Surveillance & ITMS	<ul style="list-style-type: none"> <li>• Integrates with existing cameras and new cameras. Should support multiple video sources from multiple locations. Platform should have no limitation in displaying the number of CCTV video sources</li> <li>• Integrate and assess inputs from different sources such as CCTV, ANPR, RLVD, Speed detection systems and other sensors further to assist with actionable intelligence.</li> <li>• CCTV, Video Analytics, and sensors further to assist with actionable intelligence.</li> <li>• Should use dynamic channel coverage specifically for video stream function for efficient bandwidth usage for multiple Remote-Control center</li> <li>• Display module should have capability to control multi-screened display wall in sync with operator console</li> <li>• Should support Fixed type and PTZ camera. Control PTZ function from the screen to control the camera. But with changing tile configuration each camera should be viewed with much lower resolution.</li> </ul>

S. No.	Departments /Systems	Minimum Integration Requirements
		<ul style="list-style-type: none"> <li>The system should dynamically reduce the bit rate and bandwidth for each stream based on the viewing resolution at the remote location.</li> <li>Integration with GIS map</li> </ul>

Following are the minimum use cases identified for integration for above mentioned integrations. The bidder is expected to propose more use cases based on the global leading practices and project experiences:

S. No.	Departments/ Systems	Relevant ICCC Use Cases	Data Feed Frequency	Dataset Required
1	ITMS & City Surveillance	Show location of traffic lights	Batch	Location coordinates of traffic light installations at junctions
2		Show Status of Traffic Lights	Real-time	Real-time/Near real-time status of traffic lights downtime
3		Show location of CCTV Cameras	Batch	Location coordinates of CCTV Cameras installations at junctions
4		Show Status of CCTV Cameras	Real-time	Real-time/Near real-time status of CCTV Cameras downtime

### **6.1.5 Go-Live Preparedness and Go-Live**

- a) SI shall prepare and agree with GSCL, the detailed plan for Go-Live (in-line with GSCL's implementation plan as mentioned in RFP).
- b) The SI shall define and agree with GSCL, the criteria for Go-Live.
- c) The SI shall ensure that all the data migration is done from existing systems (if any).
- d) SI shall submit signed-off UAT report (issue closure report) ensuring all issues raised during UAT are being resolved prior to Go-Live.
- e) SI shall ensure that Go –Live criteria as mentioned in User acceptance testing of Project is met and SI needs to take approval from GSCL team on the same.
- f) Go-live of the application shall be done as per the finalized and agreed upon Go-Live plan.

### **6.1.6 Operations and Maintenance**

Success of the Project would lie on how professionally and methodically the entire Project is managed once the implementation is completed. From the SI perspective too, this is a critical phase since the quarterly payments are linked to the SLA's in the post implementation phases. SI thus is required to depute a dedicated team of professionals to manage the Project and ensure adherence to the required SLAs. SI shall provide operations and maintenance services for the software, hardware and other IT and Non-IT infrastructure installed as part of the project after Go-Live for a period of 5 years. Warranty period of the product supplied under project i.e. hardware, software, IT/Non-IT etc., will be considered after phase wise Go-Live. The scope of work for the Operations & Maintenance Phase can be categorized under 8 service categories.

#### **6.1.6.1 Project Management & Facilities Management Services**

The SI will be required to provide facilities management services to support the GSCL and stakeholder department officials in performing their day-to-day functions related to this system.

SI is required to depute a dedicated, centralized project management and technical team for the overall project management and interaction with GSCL and stakeholder departments.

#### **6.1.6.2 Provision of the Operational Manpower & Contact Center Manpower to view the various data feeds and call centre operations at ICCC**

The SI is required to provide suitable manpower to monitor the data feeds ICCC and support GSCL, Traffic Police and other stakeholder departments for operationalization of smart solutions of the project. The exact role of these personnel and their responsibilities

would be defined and monitored by GSCL and respective departmental personnel. SI shall be required to provide such manpower meeting following requirements:

1. All such manpower shall be minimum graduate pass
2. All such manpower shall be without any criminal background / record.
3. GSCL reserves the right to carry out background check of the personnel proposed on the Project for verification of criminal record, at the beginning of deployment or during deployment.
4. SI shall have to replace any person, if not found suitable for the job.
5. All the manpower shall have to undergo training from the SI for at least 15 working days on the working of project. Training should also cover dos & don'ts and will have few sessions from GSCL and Stakeholders/End User Department officers on right approaches for monitoring the feeds & providing feedback to GSCL, Stakeholders/End User Department officers and other associated government agencies.
6. Each person shall have to undergo compulsory 1 day training every month
7. Operational Manpower shall work in 3 shifts, with no person being made to see the data 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.

The Current estimation of the man-power required from the SI is as follows:

#	Description	Quantity
1.	Contact Centre Manpower for operationalization of the systems (9 resources in normal working in shift & 2 resources each in day shifts for Field O&M)	11

The remaining operational manpower and supervisors required for operationalization of the project will be provided by GSCL, as per requirements.

#### **6.1.6.3 Basic Infrastructure Services**

Following services shall be provided by the SI under the basic infrastructure services:

1. Ensure availability of the infrastructure (both physical and IT) including but not limited to Power, Cooling, Racks, Storage and other peripheral equipment installed at the time of Project commissioning as per the SLAs.
2. Ensure scalability in terms of availability of racks and supporting infrastructure.

3. Proactive and reactive maintenance, repair and replacement of defective components (physical and other peripheral IT infrastructure) installed for the Project through this RFP. The cost for repair and replacement shall be borne by the SI.
4. Any component (Physical & IT installed at the time of Project commissioning) that is reported to be faulty / non-functional on a given date should be either fully repaired or replaced by temporary substitute (of equivalent configuration) within the time frame agreed upon in the Service Level Agreement (SLA).
5. Proactive monitoring of the entire basic infrastructure installed.
6. SI shall maintain records of the maintenance of the basic infrastructure and shall maintain a logbook on-site that may be inspected by the GSCL, Police department and other stakeholder departments/end users at any time.

#### **6.1.6.4 Network Monitoring Services**

The activities shall include:

1. SI shall provide services for management of ICCC Project to maintain performance at optimum levels on a 24 x 7 basis.
2. SI shall monitor and administer the network.
3. SI shall create and modify VLAN, assignment of ports to appropriate applications and segmentation of traffic.
4. SI shall carry out break fix maintenance of the LAN cabling or maintenance work requiring civil work.

#### **6.1.6.5 Integration Testing**

This shall be a black-box testing role primarily to ensure that the application to be deployed does not disrupt the Guwahati operations and affect other Guwahati infrastructure in terms of performance and security. The technical tasks to be carried out shall be as follows:

1. Functional Testing: Ensuring that the application functionality as described by the GSCL, Police department and other stakeholder departments/end users. The functional testing of application will necessarily be minimal as this is a core responsibility of the Supplier.
2. Performance Testing: Ensuring that the application meets expressed performance requirements on the Guwahati servers by using performance test tools and performance monitoring tools.
3. Security Testing: Testing for exploitable application security weaknesses that undermine the application security or the security of the infrastructure.

#### **6.1.6.6 Vendor Management Services**

The activities shall include:

1. Coordination with all the project stakeholders to ensure that all Guwahati activities are carried out in a timely manner.
2. SI shall coordinate and follow-up with all the relevant vendors to ensure that the issues are resolved in accordance with the SLAs agreed upon with them.
3. SI shall also ensure that unresolved issues are escalated to respective departments.
4. SI shall maintain database of the various vendors with details like contact person, telephone nos., escalation matrix, response time and resolution time commitments etc.
5. SI shall draw a consolidated quarterly SLA performance report across vendors for consideration of the GSCL, Police department and other stakeholder departments/end users.

#### **6.1.6.7 Network Management**

The objective of this service is to ensure continuous operation and upkeep of the Network infrastructure of the project including all active and passive components. The selected SI shall be responsible to coordinate with Network Service Provider for network related issues between ICCC, DC and other sub systems. The services to be provided for Network Management include:

- 1 Ensuring that the network is available 24x7x365 as per the prescribed SLAs for the 5 years of operations after final acceptance testing of all equipment's and services.
- 2 Attending to and resolving network failures and snags.
- 3 Support and maintain the overall network infrastructure including but not limited to LAN passive components, routers, switches etc.
- 4 Configuration and backup of network devices including documentation of all configurations.
- 5 24x7x365 monitoring of the network to spot the problems immediately.
- 6 Provide information on performance of Ethernet segments, including capacity utilization and error statistics for the segment and the top-contributing hosts, WAN links and routers.
- 7 Ensuring timely information to the GSCL, Police department and other stakeholder departments/end users pertaining to issues of Network Backbone

#### **6.1.6.8 Physical Infrastructure Management and Maintenance Services**

All the devices that will be installed in the Project as part of the physical infrastructure should be SNMP enabled and shall be centrally and remotely monitored and managed on a 24x7x365 basis. Industry leading infrastructure management solution should be deployed to facilitate monitoring and management of the Infrastructure on one integrated console. The physical infrastructure management and maintenance services shall include:

1. Proactive and reactive maintenance, repair and replacement of defective components (IT and Non-IT/ Hardware and Software). The cost for repair and replacement shall be borne by the SI.
2. The SI shall have to stock and provide adequate onsite and offsite spare parts and spare component to ensure that the uptime commitment as per SLA is met. To provide this service it is important for the SI to have back to back arrangement with the OEMs. The SI needs to provide a copy of the service level agreement signed with the respective OEMs.
3. Component that is reported to be down on a given date should be either fully repaired or replaced by temporary substitute (of equivalent configuration) within the time frame indicated in the Service Level Agreement (SLA). In case the selected SI fails to meet the above standards of maintenance, there will be a penalty as specified in the SLA.
4. The selected SI shall also maintain records of all maintenance of the system and shall maintain a logbook on-site that may be inspected by the GSCL, Police department and other stakeholder departments/end users at any time.

#### **6.1.7 Exit Management**

- a) This sets out the provisions, which will apply on expiry or termination of the Master Service Agreement, the Project Implementation, Operation and Management SLA.
- b) In the case of termination of the Project Implementation and/or Operation and Management, the Parties shall agree at that time whether, and if so during what period, the provisions of this Schedule shall apply.
- c) The Parties shall ensure that their respective associated entities carry out their respective obligations set out in this Exit Management Schedule.

##### **6.1.7.1 Cooperation and Provision of Information**

During the exit management period:

- a) The SI will allow the GSCL or its nominated agency to access information reasonably required to define the current mode of operation associated with the provision of the services to enable the GSCL to assess the existing services being delivered;
- b) Promptly on reasonable request by the GSCL, the SI shall provide access to and copies of all information held or controlled by them which they have prepared or maintained in accordance with this agreement relating to any material aspect of the services (whether provided by the SI or sub-contractors appointed by the SI). The GSCL 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 GSCL 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.



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

- a) On the commencement of the exit management period, the SI will promptly supply the following to the GSCL or its nominated agency:
  - 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 GSCL or its nominated agencies transitioning the services to its Replacement SI in a readily available format nominated by the GSCL, its nominated agency;
  - all other information (including but not limited to documents, records and agreements) relating to the services reasonably necessary to enable GSCL or its nominated agencies, or its Replacement SI to carry out due diligence in order to transition the provision of the Services to GSCL or its nominated agencies, or its Replacement SI (as the case may be).
- b) Before the expiry of the exit management period, the SI shall deliver to the GSCL 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.

#### **6.1.7.3 Transfer of Certain Agreements**

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

#### **6.1.7.4 General Obligations of the SI**

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

#### **6.1.7.5 Exit Management Plan**

The SI shall provide the GSCL 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 GSCL'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 GSCL and identification of specific security tasks necessary at termination;
  - Plans for provision of contingent support to GSCL, 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 GSCL 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 GSCL or its nominated agencies within 90 days from the Effective Date of this Agreement.

#### **6.1.8 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:

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

- 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

- GSCL, 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.

## **6.1.9 Project Management and Governance**

### **6.1.9.1 Project Management Office (PMO)**

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

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

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

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

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

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

### 6.1.9.2 Helpdesk and Facilities Management Services

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

The SI shall setup a central helpdesk dedicated (i.e. on premise) for the Project, which shall be supported by individual smart city command centres, implemented and proposed to be setup under Guwahati Smart City Programme. This helpdesk would be operational upon implementation of the Project. Providing helpdesk/support services from a shared facility of any other party/provider is not permitted.

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

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

S. No.	Type of Resource	Minimum Quantity	Minimum Deployment during Operation and Maintenance phase
1	Project Manager	1	100% (8*5)
2	Integrated Command and Control Centre (ICCC) Expert	1	100% (8*5)
3	Solution Architect	1	Onsite Support to Project team on need basis
4	Network & Security Infrastructure Expert	1	100% (8*5)
5	Security & Surveillance Expert	3	100% (8*5)
6	Integrated Traffic Management Expert	3	100% (24*7)
7	Server & Storage Expert	1	100% (8*5)
8	Command Centre Operators	11	100% (24*7 – 3 resources in each rotational shift & 2 resource in general shift for field maintenance)

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

### **6.1.9.3 Steering Committee**

The Steering Committee will consist of senior stakeholders from GSCL, its nominated agencies and SI. SI will nominate its Smart City vertical head to be a part of the Project Steering Committee

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

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

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

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

### **6.1.9.4 Project Monitoring and Reporting**

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

Other than the planned meetings, in exceptional cases, project status meeting may be called with prior notice to the Bidder. GSCL reserves the right to ask the bidder for the project review reports other than the standard weekly review reports.

### **6.1.9.5 Risk and Issue management**

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

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

The SI shall monitor, report, and update the project risk profile. The risks should be discussed with GSCL and a mitigation plan be identified during the project review/status

meetings. The Risk and Issue management should form an agenda for the Project Steering Committee meetings as and when required.

#### **6.1.9.6 Governance procedures**

SI shall document the agreed structures in a procedure's manual.

#### **6.1.9.7 Planning and Scheduling**

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

The project plan should include the following:

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

#### **6.1.9.8 License Metering / Management**

The SI shall track software usage throughout the IT setup so as to effectively manage the risk of unauthorized usage or under-licensing of software installed at the ICC. This may be carried out through the use of standard license metering tools.

#### **6.1.10 Change Management & Control**

##### **6.1.10.1 Change Orders / Alterations / Variations**

- a. The SI agrees that the requirements given in the Bidding Documents are minimum requirements and are only indicative. The SI would need to fetch out the details at the time of preparing the design document prior to actual implementation. It shall be the responsibility of the SI to meet all the requirements of technical specifications contained

in the RFP and any upward revisions and/or additions of quantities, specifications sizes given in the Bidding Documents required to be made during execution of the works, shall not constitute a change order and shall be carried out without a change order and shall be carried out without any time and cost effect to Purchaser.

- b. Further upward revisions and or additions required to make SI's selected equipment and installation procedures to meet Bidding Documents requirements expressed and to make entire facilities safe, operable and as per specified codes and standards shall not constitute a change order and shall be carried out without any time and cost effect to Purchaser.
- c. Any upward revision and/or additions consequent to errors, omissions, ambiguities, discrepancies in the Bidding Documents which the SI had not brought out to the Purchaser's notice in his bid shall not constitute a change order and such upward revisions and/or addition shall be carried out by SI without any time and cost effect to Purchaser.

#### **6.1.10.2 Change Order**

- a. The Change Order will be initiated only in case (i) the Purchaser directs in writing the SI to include any addition to the scope of work covered under this Contract or delete any part of the scope of the work under the Contract, (ii) SI requests to delete any part of the work which will not adversely affect the operational capabilities of the facilities and if the deletions proposed are agreed to by the Purchaser and for which cost and time benefits shall be passed on to the Purchaser, (iii) the Purchaser directs in writing the SI to incorporate changes or additions to the technical specifications already covered in the Contract.
- b. Any changes required by the Purchaser over and above the minimum requirements given in the specifications and drawings etc. included in the Bidding Documents before giving its approval to detailed design or Engineering requirements for complying with technical specifications and changes required to ensure systems compatibility and reliability for safe operation (As per codes, standards and recommended practices referred in the Bidding Documents) and trouble free operation shall not be construed to be change in the Scope of work under the Contract.
- c. Any change order as stated in this RFP comprising an alteration which involves change in the cost of the works (which sort of alteration is hereinafter called a "Variation") shall be the Subject of an amendment to the Contract by way of an increase or decrease in the schedule of Contract Prices and adjustment of the implementation schedule if any.



- d. If parties agree that the Contract does not contain applicable rates or that the said rates are inappropriate or the said rates are not precisely applicable to the variation in question, then the parties shall negotiate a revision of the Contract Price which shall represent the change in cost of the works caused by the Variations. Any change order shall be duly approved by the Purchaser in writing.
- e. Within ten (10) working days of receiving the comments from the Purchaser or the drawings, specification, purchase requisitions and other documents submitted by the SI for approval, the SI shall respond in writing, which item(s) of the Comments is/are potential changes(s) in the Scope of work of the RFP document covered in the Contract and shall advise a date by which change order (if applicable) will be submitted to the Purchaser.

#### 6.1.11 Testing and Acceptance Criteria

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

Type of Testing	Responsibility	Scope of Work
System Testing	SI	<ol style="list-style-type: none"> <li>1. SI to perform System testing</li> <li>2. SI to prepare test plan and test cases and maintain it. GSCL may request the SI to share the test cases and results</li> <li>3. Should be performed through manual as well as automated methods</li> <li>4. Automation testing tools to be provided by SI. GSCL doesn't intend to own these tools</li> </ol>
Integration Testing	SI	<ol style="list-style-type: none"> <li>1. SI to perform Integration testing</li> <li>2. SI to prepare and share with GSCL the Integration test plans and test cases</li> <li>3. SI to perform Integration testing as per the approved plan</li> </ol>

		<ol style="list-style-type: none"> <li>4. Integration testing to be performed through manual as well as automated methods</li> <li>5. Automation testing tools to be provided by SI. GSCL doesn't intend to own these tools</li> </ol>
Performance and load Testing	SI/ GSCL / Third Party Auditor (to monitor the performance testing)	<ol style="list-style-type: none"> <li>1. SI to do performance and load testing.</li> <li>2. Various performance parameters such as transaction response time, throughput, page loading time should be considered.</li> <li>3. Load and stress testing of the Project to be performed on business transaction volume</li> <li>4. Test cases and test results to be shared with GSCL.</li> <li>5. Performance testing to be carried out in the exact same architecture that would be set up for production.</li> <li>6. SI need to use performance and load testing tool for testing. GSCL doesn't intend to own these tools. GSCL if required, could involve third party auditors to monitor/validate the performance testing. Cost for such audits to be paid by GSCL.</li> </ol>
Security Testing (including Penetration and Vulnerability testing)	SI/ GSCL / Third Party Auditor (to monitor the performance testing)	<ol style="list-style-type: none"> <li>1. The solution should demonstrate the compliance with security requirements as mentioned in the RFP including but not limited to security controls in the application, at the network layer, network, data centre(s), security monitoring system deployed by the SI</li> <li>2. The solution shall pass vulnerability and penetration testing for rollout of each phase. The solution should pass web application security testing for the portal, mobile app and other systems and security configuration review of the infrastructure.</li> <li>3. SI should carry out security and vulnerability testing on the developed solution.</li> <li>4. Security testing to be carried out in the exact same environment/architecture that would be set up for production.</li> <li>5. Security test report and test cases should be shared with GSCL</li> <li>6. Testing tools if required, to be provided by SI. GSCL doesn't intend to own these tools</li> <li>7. During O&amp;M phase, penetration testing to be conducted on yearly basis and vulnerability assessment to be conducted on half-yearly basis.</li> </ol>

		8. GSCL will also involve third party auditors to perform the audit/review/monitor the security testing carried out by SI. Cost for such auditors to be paid by GSCL.
User Acceptance Testing of Project	<ul style="list-style-type: none"> <li>• GSCL or GSCL appointed third party auditor</li> </ul>	<ol style="list-style-type: none"> <li>1. GSCL / GSCL appointed third party auditor to perform User Acceptance Testing</li> <li>2. SI to prepare User Acceptance Testing test cases</li> <li>3. UAT to be carried out in the exact same environment/architecture that would be set up for production</li> <li>4. SI should fix bugs and issues raised during UAT and get approval on the fixes from GSCL / third party auditor before production deployment</li> <li>5. Changes in the application as an outcome of UAT shall not be considered as Change Request. SI has to rectify the observations.</li> </ol>

**Note:**

- a. Bidder needs to provide the details of the testing strategy and approach including details of intended tools/environment to be used by SI for testing in its technical proposal. GSCL does not intend to own the tools.
- b. The SI shall work in a manner to satisfy all the testing requirements and adhere to the testing strategy outlined. The SI must ensure deployment of necessary resources and tools during the testing phases. The SI shall perform the testing of the solution based on the approved test plan, document the results and shall fix the bugs found during the testing. It is the responsibility of SI to ensure that the end product delivered by the SI meets all the requirements specified in the RFP. The SI shall take remedial action based on outcome of the tests.
- c. The SI shall arrange for environments and tools for testing and for training as envisaged. Post Go-Live; the production environment should not be used for testing and training purpose. If any production data is used for testing, it should be masked, and it should be protected. Detailed process in this regard including security requirement should be provided by the SI in its technical proposal. The process will be finalized with the selected bidder.
- d. All the Third-Party Auditors (TPA) as mentioned above will be appointed and paid by GSCL directly. All tools/environment required for testing shall be provided by the SI.

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

#### **6.1.11.1 Factory Testing**

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

1. Cable
2. Pole
3. Signal Aspects

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

#### **6.1.11.2 Final Acceptance Testing**

The final acceptance shall cover 100% of the I Project, after successful testing by the GSCL, Police Department, other stakeholders/end user department or its PMU; a Final Acceptance Test Certificate (FAT) shall be issued by the GSCL to the SI.

Prerequisite for Carrying out FAT activity:

1. Detailed test plan shall be developed by the SI and approved by GSCL. This shall be submitted by SI before FAT activity to be carried out.
2. All documentation related to ICCS Project and relevant acceptance test document (Including IT Components, Non-IT Components etc.) should be completed & submitted before the final acceptance test to the GSCL.
3. The training requirements as mentioned should be completed before the final acceptance test.
4. Successful hosting of Application, NMS and MIS Software.
5. For both IT & Non-IT equipment's / software manuals / brochures / Data Sheets / CD / DVD / media for all the Guwahati Project supplied components.

The FAT shall include the following:

1. All hardware and software items must be installed at respective sites as per the specification.

2. Availability of all the defined services shall be verified.
3. The SI shall be required to demonstrate all the features / facilities / functionalities as mentioned in the RFP.
4. The SI shall arrange the test equipment required for performance verification and will also provide documented test results.
5. The SI shall be responsible for the security audit of the established system to be carried out by a certified third party as agreed by GSCL.

Any delay by the SI in the Final Acceptance Testing shall render him liable to the imposition of appropriate Penalties. However, delays identified beyond the control of SI shall be considered appropriately and as per mutual agreement between GSCL and SI. In the event the SI is not able to complete the installation due to non-availability of bandwidth from the bandwidth service providers, the Supplier and GSCL may mutually agree to redefine the Network so the SI can complete installation and conduct the Final Acceptance Test within the specified time.

## **7.0 ANNEXURE II: PAYMENT SCHEDULE AND MILESTONES**

The system Integrator should submit Project plan and Procurement plan as mentioned in Tender document for approval of GSCL.

As per approved Project plan and procurement plan, subsequent request orders shall be place to the SI.

GSCL shall issue a "Request Order" in writing, indicating the number of units of Hardware and Software to be supplied along with the location (Project Site). Upon getting the Request Order, the SI shall promptly and as soon as possible within the lead time specified in the request order, supply, install and implement specified numbers of hardware and software at stated project site and commissioned the same. GSCL shall specify the Lead Time in Request Order.

## 7.1 Payment Schedules for Implementation Phase

Item No.	Item Description	Payment Breakup	Remarks
<b>Schedule A</b>			
<b>A</b>			
<b>A.1</b>	Site Survey, Design & Drawings- Conducting Detailed Site survey, Submission of Detailed Project report comprising Detailed Design & Drawings of all components listed in Vol-II	Value commensurate to the discovered quote for Site survey, Design & drawings as per commercial format	
<b>Schedule B</b>			
<b>1.1</b>	<b>Traffic Violation Detection System at Traffic Junctions</b>		
<b>1.1.1</b>	ANPR Camera with accessories & required analytics SW	(a) On supply – 60 % of approved rate (b) On Installation – 15 % of approved rate (c) On Commissioning -15 % of Approved Rate (d) On Go-live – 10 %	Payment against Supply will be done only for approved quantity from GSCL
<b>1.1.2</b>	RLVD Camera with accessories & required analytics SW		
<b>1.1.3</b>	Sped Violation Detection System, Including the complete solutions - a) 9MP IP Camera, b) 4D tracking Radar, c) Local Processing Unit, d) LED Flash, e)Software License Lifetime use fee, f) Junction Box with Network, Power Component, Cables, accessories, and installations		
<b>1.1.4</b>	Vehicle Activated Radar Speed Signs - Highway Variable Display Board 1x1meter, 3 color display (red, green, and amber)		
<b>1.1.8</b>	Industrial Grade Outdoor - L2-PoE switches - 8 Port +4 SFP (Only for ITMS)		
<b>1.1.9</b>	Industrial Grade Outdoor - L2-PoE switches - 08 Port +4 SFP (Only for SVD)		
<b>1.1.10</b>	UPS with Battery (appropriate Backup per technical specification and SLA mentioned in volume II of this RFP)		
<b>1.1.11</b>	10 Mtr Gantry System/Cantilever Pole - ANPR & RLVD		

Item No.	Item Description	Payment Breakup	Remarks
1.1.13	ANPR Analytics Software License with No Helmet, Triple Ride of 2-wheeler, No Seatbelt, Driver talking on Phone, Free left Blocking while driving with ANPR.		
1.1.14	RLVD Analytics Software License		
<b>1.2</b>	<b>ATSC - Signalization at Traffic Junctions</b>		
1.2.1	ATCS Traffic Controller	(a) On supply – 60 % of approved rate (b) On Installation – 15 % of approved rate (c) On Commissioning -15 % of Approved Rate (d) On Go-live – 10 %	Payment against Supply will be done only for approved quantity from GSCL
1.2.2	Countdown timer		
1.2.3	Vehicle Detection System		
1.2.4	Galvanized standard Poles for Traffic Aspects and Pedestrian signals		
1.2.5	Galvanized Cantilevers for Traffic Aspects and Pedestrian signals		
1.2.6	Traffic Light Aspects – Red		
1.2.7	Traffic Light Aspects – Amber		
1.2.8	Traffic Light Aspects – Green		
1.2.9	Pedestrian lamp heads – Stop Man		
1.2.10	Pedestrian lamp heads – Walk Man		
1.2.11	Supply & Laying of Cabling , junction box installation , earthing , conduiting , trenching , digging of road , etc		
1.2.12	ATCS Centralize Software		
<b>2.1</b>	<b>CCTV Camera at different location in the city</b>		
2.1.1	Indoor Dome Camera	(a) On supply – 60 % of approved rate (b) On Installation – 15 % of approved rate (c) On Commissioning -15 % of Approved Rate (d) On Go-live – 10 %	Payment against Supply will be done only after getting approval of quantity from GSCL
2.1.2	Outdoor Bullet /Fixed Camera		
2.1.3	Outdoor PTZ Camera		
2.1.4	Poles for CCTV Cameras with Accessories		
2.1.5	Junction Box / Control Unit Cabinet for CCTV: including AC Power supply with all cabling, fittings, earthing, lighting arrester , etc.		
2.1.6	Industrial Grade Outdoor - L2-PoE switches - 4 Port +2 SFP		
2.1.7	UPS with Battery (appropriate Backup per technical specification and SLA mentioned in volume II of this RFP)		
2.1.8	VMS Software with all Camera License		
<b>3.1</b>	<b>Optical Transmission Equipment's for POP Sites</b>		

Item No.	Item Description	Payment Breakup	Remarks
3.1.1	Core Router - with 1Gbps, 10km Transceivers - 16, 10Gbps, 10km Transceivers -16, 10Gbps, 40km Transceivers- 4, 40Gbps, 10km Transceivers -8, 40Gbps, 40km Transceivers -02, 40Gbps Cables/Transceivers (Multimode) -04	(a) On supply – 60 % of approved rate (b) On Installation – 15 % of approved rate (c) On Commissioning -15 % of Approved Rate (d) On Go-live – 10 %	Payment against Supply will be done only after getting approval of quantity from GSCL
3.1.2	DWDM/OTN Base Equipment (Min 2x100G (Line OTU4) + min 20x10G interfaces with Redundant PSU and Redundant Fabric Crossconnect , accessories and Patch cords)without CFP/ XFP/SFP		
3.1.3	Optical, CFP, 100GBase-ER4, OTU4, 100G to support 40 km		
3.1.4	Optical, SFP+, 10GBASE-LR/LW, STM64, 9.95Gbps to 11.3Gbps to support 10Km with required patch cord		
3.1.5	Server Hardware( Include Server/ Switch/Rack or any other hardware to manage the Network)		
3.1.6	NMS Software for DWDM/OTN		
3.1.7	Switch with 24 Port SFP GigE and 4 x 1/10G SFP+ with Redundant AC PSU and Layer2+ Software and Installation Kit/Power cable)		
3.1.8	Optical, SFP, 1000BASE-LX, 1.25Gbps, 1310nm to support 10 km with required patch cord		
3.1.9	Optical, SFP+, 10GBASE-LR/LW, STM64, 9.95Gbps to 11.3Gbps to support 10Km with required patch cord		
3.1.10	Overhead OFC Deployment Cost (Including OFC, Pole, RM, JC Closure & Fixture)		
3.1.11	Underground OFC Deployment Cost (Including OFC, HDPE Ducts, Couplers, RM, Chambers JC Closures)		
3.1.12	36U Racks for Tx Equipment's		
3.1.13	FDMS/LIU Equipment		
3.1.14	Patch Cord - 3 Meters (OFC)		
4.1	<b>Wireless- RF Connectivity</b>		



Item No.	Item Description	Payment Breakup	Remarks
4.1.1	RF connectivity at all ITMS crossing with complete solutions - 50 Mbps- Including Tower, Pole, BTS, CPE, Power Backup -- (64-ITMS Crossing)	"DO" (as mentioned above)	"DO" (as mentioned above)
<b>5.1</b>	<b>Video Wall System</b>		
5.1.1	Video Wall Cubes for - Wall size 6.5 x 2.5 Meter - with complete stand and accessories	"DO" (as mentioned above)	"DO" (as mentioned above)
5.1.2	Video Wall Controller with Wall Management System		
<b>5.3</b>	<b>Network , ICCC Platform and Switching Devices</b>		
5.4.1	DG Set - 75 KVA with AMF Panel with Change-over Switch	"DO" (as mentioned above)	"DO" (as mentioned above)
5.4.2	UPS with battery backup - 50 KVA		
<b>7.1</b>	<b>Servers, Switches &amp; Application SW</b>		
7.1.1	Data Centre Spine Switch (Core)	"DO" (as mentioned above)	"DO" (as mentioned above)
7.1.2	Data Centre Leaf Switch (Aggregate)		
7.1.3	Data Centre Out of Band Switch		
7.1.4	GIS Enterprise Software		
<b>7.2</b>	<b>Storage &amp; Other Components</b>		
7.2.1	Primary Storage (3 PB) - 30 Days	(a) On supply – 60 % of approved rate (b) On Installation – 15 % of approved rate (c) On Commissioning -15 % of Approved Rate (d) On Go-live – 10 %	Payment against Supply will be done only after getting approval of quantity from GSCL
7.2.2	Secondary Storage (5 PB) / Compressed Form - 90 Days		
7.2.3	Hyper Converged Infrastructure (HCI)		
7.2.4	Internet Firewall with IPS		
7.2.5	Nest Generation Firewall (NGFW) with Anti APT		
7.2.6	Server Load Balancer with Web application Firewall		
7.2.7	Security Information & Event Management (SIEM) System		
7.2.8	Authentication, Authorization and Accounting – Network Access Control (AAA – NAC)		
7.2.9	Network Management System (NMS)/ Enterprise Management System - EMS		
7.2.10	End Host Antivirus		

For all remaining Items of Schedule-B & Schedule-A (Survey etc) Payment will be done on Prorate basis only after Installation & Commissioning and Final Acceptance Testing of the

respective items & services – (90 % of approved rate after satisfactorily installation and 10 % of Approved rate after Commissioning on approval from GSCL)

**Note:** Mobilization advance will be deducted from Interim Payment certificate as per Clause – 4.6 of Volume 01.

## 7.2 Milestones and Payment Schedules for Operations and Maintenance Phase

The Operations and maintenance phase will start as soon as Go-Live for each phase occurs. The SI will be required to adhere to the SLA and provide post implementations support of warranty and O&M for the remaining project period after implementation/Go-Live.

Milestones	Payment Milestones for the Implementation % Payment of Time Schedule Phase	Payment Schedule	Time Schedule
M3	Year 1 - Payment for O&M after Go-Live	Equal Quarterly O&M Payments – after every three (3) months	Payment of Year 1
M4	Year 2 - Payment for O&M after Go-Live	Equal Quarterly O&M Payments – after every three (3) months	Payment of Year 2
M5	Year 3 - Payment for O&M after Go-Live	Equal Quarterly O&M Payments – after every three (3) months	Payment of Year 3
M6	Year 4 - Payment for O&M after Go-Live	Equal Quarterly O&M Payments – after every three (3) months	Payment of Year 4
M7	Year 5 - Payment for O&M after Go-Live	Equal Quarterly O&M Payments – after every three (3) months	Payment of Year 5

Payment of Operations and maintenance phase will be made on quarterly basis (at completion of each quarter) based on the adherence to SLA, for the amount quoted for each respective year.

## 8.0 ANNEXURE III - COMMON GUIDELINES REGARDING COMPLIANCE OF SYSTEMS/EQUIPMENT

1. The specifications mentioned for various IT / Non-IT components are indicative requirements and should be treated for benchmarking purpose only. SIs are required to undertake their own requirement analysis and may propose higher specifications that are better suited to the requirements.
2. Any manufacturer and product name mentioned in the Tender should not be treated as a recommendation of the manufacturer / product.
3. All IT Components should support IPv4 and IPv6
4. All IT/Electronics components shall comply to the IEC/ISI/BSI standards as applicable
5. All systems will be designed to ensure accessibility to the disabled hence all the components related to IT, electronics and/or digital technology should be in accordance to the latest version of WCAG and the European Standards - EN 301 549 or an equivalent standard as approved
6. SI should adhere with the open standard oneM2M wherever applicable during solution design and implementation
7. The specifications provided in this RFP are indicative and carry guiding rule. The SI is free to offer products and solutions which meet requirements of the RFP focusing on the outcome, future scalability, security, reliability and adherence to specified SLA under this RFP, in line with applicable standards & best practices adopted in the industry. The SI is encouraged to design an Optimized solution which is technically superior, innovative, proven, better in terms of functionality and is cost effective. Any specified parameters mentioned in the scope/technical requirement in the RFP may be considered if it is required for meeting current & future requirements during the contract period. Necessary justification should be given in Technical solution accordingly. The SI is fully responsible for the specified outcome to be achieved.
8. Technical Bid should be accompanied by OEM's product brochure / datasheet. Bidders should provide complete make, model, for all equipment/software quoted, in the Technical Bid.
9. Bidder should ensure that only one make and model is proposed for one component in Technical Bid for example all PTZ cameras must belong to a single OEM and must be of the same model etc.
10. Bidders should ensure warranty and support for all equipment from OEMs during the contract period. All the back-to-back service agreements should be submitted along with the Technical Bid.
11. All equipment, parts should be original and new.
12. The user interface of the system should be a user-friendly Graphical User Interface (GUI).
13. Critical core components of the system should not have any requirements to have proprietary platforms and should conform to open standards.
14. For custom made modules, industry standards and norms should be adhered to for coding during application development to make debugging and maintenance easier.

Object oriented programming methodology must be followed to facilitate sharing, componentizing and multiple-use of standard code. Before hosting the application, it shall be subjected to application security audit (by any of the CERTIN empaneled vendors) to ensure that the application is free from any vulnerability; and approved by the GSCL.

15. All the Clients Machines / Servers shall support static assigned IP addresses or shall obtain IP addresses from a DNS/DHCP server.
16. The indicative architecture of the system is given in this volume. The Successful Bidder must provide the architecture of the solution it is proposing.
17. The system servers and software applications will be hosted in Data Centers as specified in the Bid. It is important that the entire set of Data Center equipment are in safe custody and have access from only the authorized personnel and should be in line with the requirements & SLAs defined in the RFP.
18. The Servers provided should meet industry standard performance parameters (such as CPU Utilization of 60 percent or less, disk utilization of 75 percent or less). In case any non- standard computing environment is proposed (such as cloud), detail clarification needs to be provided in form of supporting documents, to confirm (a) how the sizing has been arrived at and (b) how SLAs would be met.
19. SI is required to ensure that there is no choking point / bottleneck anywhere in the system (end-to-end) and enforce performance and adherence to SLAs. SLA reports must be submitted as specified in the Bid without fail.
20. All the hardware and software supplied should be from the reputed Original Equipment Manufacturers (OEMs). GSCL/or any other authorized agency as nominated by the Authority reserves the right to ask replacement of any hardware / software if it is not from a reputed brand and conforms to all the requirements specified in the RFP documents.
21. Cameras and the Video Management / Video Analytics Software should be ONVIF Core Specification or 'S', compliant and provide support for ONVIF profiles such as Streaming, Storage, Recording, Playback, retrieval of local stored video and Access Control.
22. System Integrator shall place orders on various OEMs directly and not through any sub-contractor / partner.
23. All licenses should be in the name of the Guwahati Smart City Limited (GSCL).

**NOTE:** For all supply equipment's, registered service/support center of the respective OEM should be existing or established in India within 30 days of award of contract. The Bidder should submit an undertaking from the OEM to that effect.

**9.0 ANNEXURE IV - STATUS OF THE SYSTEMS TO BE INTEGRATED IN ICCC IN GUWAHATI CITY**

S.No.	ICT Systems	Status of current Automation	Future Roadmap
1	Integrated Traffic Management System (ITMS)	No	Yes
2	City Surveillance – CCTV	No	Yes
3	GIS	No	Yes

**10.0 ANNEXURE V – SMART CITY GUIDELINES FOR ENSURING UNIVERSAL ACCESS IT SYSTEMS TO EMPOWER CITIZENS WITH DISABILITY TO ACCESS ICT SYSTEMS WITH EASE**

SI. No.	Parameters	Minimum Requirements
1	Text Alternatives	Provide text alternatives for any non-text content so that it can be changed into other forms people need, such as large print, braille, speech, symbols or simpler language.
2	Non-text Content	All images, form image buttons, and image map hot spots have appropriate, equivalent alternative text. Images that do not convey content, are decorative, or contain content that is already conveyed in text are given null alt text (alt="") or implemented as CSS backgrounds. All linked images have descriptive alternative text. Equivalent alternatives to complex images are provided in context or on a separate (linked and/or referenced via longdesc) page.
3	Time-based Media	Provide alternatives for time-based media.
4	Audio Description or Media Alternative (Prerecorded)	A descriptive text transcript OR audio description audio track is provided for non-live, web-based video
5	Adaptable	Create content that can be presented in different ways (for example simpler layout) without losing information or

SI. No.	Parameters	Minimum Requirements
		structure.
6	Info and Relationships	Semantic markup is used to designate headings (<h1>), lists (<ul>, <ol>, and <dl>), emphasized or special text (<strong>, <code>, <abbr>, <blockquote>, for example), etc. Semantic markup is used appropriately. Tables are used for tabular data. Where necessary, data cells are associated with their headers. Data table captions and summaries are used where appropriate. Text labels are associated with form input elements. Related form elements are grouped with fieldset/legend.
7	Meaningful Sequence	The reading and navigation order (determined by code order) is logical and intuitive.
8	Use of Color	Color is not used as the sole method of conveying content or distinguishing visual elements. Color alone is not used to distinguish links from surrounding text unless the luminance contrast between the link and the surrounding text is at least 3:1 and an additional differentiation (e.g., it becomes underlined) is provided when the link is hovered over or receives focus.
9	Audio Control	A mechanism is provided to stop, pause, mute, or adjust volume for audio that automatically plays on a page for more than 3 seconds.
10	Resize text	The page is readable and functional when the text size is doubled.
11	Images of Text	If the same visual presentation can be made using text alone, an image is not used to present that text.
12	Keyboard Accessible	Make all functionality available from a keyboard.
13	Keyboard	All page functionality is available using the keyboard, unless the functionality cannot be accomplished in any known way using a keyboard (e.g., free hand drawing). Page-specified shortcut keys and access keys (access key should typically be avoided) do not conflict with existing browser and screen reader shortcuts.
14	No Keyboard Trap	Keyboard focus is never locked or trapped at one particular page element. The user can navigate to and from all navigable page elements using only a keyboard.

SI. No.	Parameters	Minimum Requirements
15	Pause, Stop, Hide	<p>Automatically moving, blinking, or scrolling content that lasts longer than 5 seconds can be paused, stopped, or hidden by the user. Moving, blinking, or scrolling can be used to draw attention to or highlight content as long as it lasts less than 5 seconds.</p> <p>Automatically updating content (e.g., automatically redirecting or refreshing a page, a news ticker, AJAX updated field, a notification alert, etc.) can be paused, stopped, or hidden by the user or the user can manually control the timing of the updates.</p>
16	Seizures	Do not design content in a way that is known to cause seizures.
17	Three Flashes or Below Threshold	No page content flashes more than 3 times per second.
18	Navigable	Provide ways to help users navigate, find content, and determine where they are
19	Bypass Blocks	<p>A link is provided to skip navigation and other page elements that are repeated across web pages.</p> <p>If a page has a proper heading structure, this may be considered a sufficient technique instead of a "Skip to main content" link.</p> <p>Note that navigating by headings is not yet supported in all browsers.</p> <p>If a page uses frames and the frames are appropriately titled, this is a sufficient technique for bypassing individual frames.</p>
20	Page Titled	The web page has a descriptive and informative page title.
21	Focus Order	The navigation order of links, form elements, etc. is logical and intuitive.
22	Headings and Labels	Page headings and labels for form and interactive controls are informative. Avoid duplicating heading (e.g., "More Details") or label text (e.g., "First Name") unless the structure provides adequate differentiation between them.
23	Focus Visible	It is visually apparent which page element has the current keyboard focus (i.e., as you tab through the page, you can see where you are).
24	Readable	Make text content readable and understandable

SI. No.	Parameters	Minimum Requirements
25	Language of Page	The language of the page is identified using the HTML Lang attribute
26	Language of Parts	The language of page content that is in a different language is identified using the Lang attribute.
27	Predictable	Make Web pages appear and operate in predictable ways.
28	On Input	When a user inputs information or interacts with a control, it does not result in a substantial change to the page, the spawning of a pop-up window, an additional change of keyboard focus, or any other change that could confuse or disorient the user unless the user is informed of the change ahead of time.
29	Compatible	Maximize compatibility with current and future user agents, including assistive technologies.
30	Parsing	Significant HTML/XHTML validation/parsing errors are avoided. In content implemented using markup languages, elements have complete start and end tags, elements are nested according to their specifications, elements do not contain duplicate attributes, and any IDs are unique, except where the specifications allow these features.
31	Name, Role, Value	Markup is used in a way that facilitates accessibility. This includes following the HTML/XHTML specifications and using forms, form labels, frame titles, etc. appropriately. For all user interface components, the name and role can be programmatically determined; states, properties, and values that can be set by the user can be programmatically set; and notification of changes to these items is available to user agents, including assistive technologies.
32	Audio-only and Video-only (Prerecorded)	A descriptive text transcript (including all relevant visual and auditory clues and indicators) is provided for non-live, web-based audio (audio podcasts, MP3 files, etc.). A text or audio description is provided for non-live, web-based video-only (e.g., video that has no audio track).
33	Captions (Prerecorded)	Synchronized captions are provided for non-live, web-based video (YouTube videos, etc.)
34	Captions (Live)	Synchronized captions are provided for all live multimedia that contains audio (audio-only broadcasts, web casts, video conferences, Flash animations, etc.)



SI. No.	Parameters	Minimum Requirements
35	Audio Description (Prerecorded)	Audio descriptions are provided for all video content NOTE: Only required if the video conveys content visually that is not available in the default audio track.
36	Sensory Characteristics	Instructions do not rely upon shape, size, or visual location (e.g., "Click the square icon to continue" or "Instructions are in the right-hand column"). Instructions do not rely upon sound (e.g., "A beeping sound indicates you may continue.").
37	Distinguishable	Make it easier for users to see and hear content including separating foreground from background.
38	Contrast (Minimum)	Text and images of text have a contrast ratio of at least 4.5:1. Large text - at least 18 point (typically 24px) or 14 point (typically 18.66px) bold has a contrast ratio of at least 3:1.
39	Enough Time	Provide users enough time to read and use content.
40	Timing Adjustable	If a page or application has a time limit, the user is given options to turn off, adjust, or extend that time limit. This is not a requirement for real-time events (e.g., an auction), where the time limit is absolutely required, or if the time limit is longer than 20 hours.
41	Link Purpose (In Context)	The purpose of each link (or form image button or image map hotspot) can be determined from the link text alone, or from the link text and its context (e.g., surrounding paragraph, list item, table cell, or table headers). Links (or form image buttons) with the same text that go to different locations are readily distinguishable.
42	Multiple Ways	Multiple ways are available to find other web pages on the site - at least two of: a list of related pages, table of contents, site map, site search, or list of all available web pages.
43	On Focus	When a page element receives focus, it does not result in a substantial change to the page, the spawning of a pop-up window, an additional change of keyboard focus, or any other change that could confuse or disorient the user.
44	Consistent Navigation	Navigation links that are repeated on web pages do not change order when navigating through the site.
45	Consistent Identification	Elements that have the same functionality across multiple web pages are consistently identified. For example, a search box at the top of the site should always be labeled the same way.
46	Input Assistance	Help users avoid and correct mistakes.

SI. No.	Parameters	Minimum Requirements
47	Error Identification	Required form elements or form elements that require a specific format, value, or length provide this information within the element's label. If utilized, form validation errors are presented in an efficient, intuitive, and accessible manner. The error is clearly identified, quick access to the problematic element is provided, and user is allowed to easily fix the error and resubmit the form.
48	Labels or Instructions	Sufficient labels, cues, and instructions for required interactive elements are provided via instructions, examples, properly positioned form labels, and/or field sets/legends.
49	Error Suggestion	If an input error is detected (via client-side or server-side validation), provide suggestions for fixing the input in a timely and accessible manner.
50	Error Prevention (Legal, Financial, Data)	If the user can change or delete legal, financial, or test data, the changes/deletions can be reversed, verified, or confirmed.
51	Visual Captcha	Alternative mode of authentication should be offered to in order to be authenticated.
52	Mandatory use of Unicode for regional language	Unicode facilitates assistive technology to access content.

## 11.0 ANNEXURE VII – CYBER SECURITY REQUIREMENTS FOR GUWAHATI SMART CITY PROJECT

### 11.1 Cyber Security Framework

The Bidder shall develop Cyber Security Framework aimed at building a secure and resilient cyberspace for citizens and stakeholders of Smart City. The Framework shall be designed to protect cyberspace information and infrastructure; build capabilities to prevent and respond to cyber- attacks; and minimize damages through coordinated efforts of institutional structures, people, processes, and technology. Framework shall cover smart city cyber security architecture with reference to the cyber security framework suggested by National Institute of Standards and Technology (NIST), CSA (Cloud Security Alliance) and ISO27001. Framework shall also comply with MoUD/MOHUA guidelines vide circular K-1s016/6U2016-SC-1.

## **11.2 Cyber Security Policy**

The Bidder shall ensure creation and implementation of Smart City Cyber Security Policy and related procedures in line with relevant international standards. The policy shall address security of hardware and software, along with the connectivity between the field device and the respective application software. The bidder shall ensure to develop and implement Standard Operating Procedures for smooth Operations and Maintenance of IT infrastructure.

## **11.3 Cyber Security Governance**

1. The Bidder shall conduct Risk Assessment and prepare Risk Treatment Plan for the IT applications and infrastructure deployed in smart city ecosystem.
2. The Bidder shall facilitate management reporting in form of dashboard covering Risk Assessment results along with risk treatment plan and timeline to the smart city management.
3. The Bidder shall implement all the controls as identified during the Risk assessment and treatment plan as per the agreed timelines.

## **11.4 Cyber Security Organization Structure**

1. The Bidder shall clearly define Organization structure for Smart City Cyber Security with skilled personnel and adequate representation from Senior Management. The organization structure shall also include the roles and responsibilities of personnel deployed for cyber security of smart city.
2. The smart city cyber security resources shall be deployed as part of the team during the complete contract period i.e. implementation and operation stage.

## **11.5 Smart City IT Asset Management**

1. The Bidder shall utilize automated asset management tools to prepare the information asset register (IAR) for all IT assets deployed in the Smart city. The IAR shall capture criticality, rating, classification, owner and custodian of the Asset.
2. The Bidder shall develop and implement an appropriate set of procedures for information labeling and handling in accordance with the classification scheme proposed in the cyber security policy of smart city.

## **11.6 Physical & Environmental Security**

1. The bidder shall implement and manage physical security of IT assets of smart city, which shall include, as a minimum: locks, alarms, surveillance equipment, sensors,

access control systems (biometrics), etc. The bidder shall also design processes and procedures for same.

2. The Bidder shall ensure that all the equipment, information or software shall not be taken off-site without appropriate authorization.

### **11.7 Access Control**

1. The Bidder shall ensure that users shall be provided single sign on functionality if required for the applications and solutions deployed in Smart City.
2. The smart city solution should support multiple authentication methods such as Username password, two factor authentication, digital certificate and biometric based authentication.
3. 2FA solution should be capable of being deployed on mobile devices deployed for smart city
4. Solution should have the capability to define access based on time of day, day of week or by group or user defined access.
5. The smart city solution should have the functionality to provide authentication based on the role.
6. Remote access to all smart city IT users shall be securely managed.
7. The smart city solution should be able to deploy and configure the approved password policy and should provide the feature to configure the logs.
8. The smart city solution should have the option of blocking multiple sessions for the user.
9. All smart city applications should support role-based access control to enforce separation of duties.
10. The application deployed in smart city should display the last login status (successful/unsuccessful, time) to the user and should not store authentication credentials on client computers after a session terminates
11. All smart city solution should be compliant with Indian IT Act, 2000 and Amended IT Act, 2008

### **11.8 Communications and Operations Management**

1. Bidders must ensure that the IT systems in the smart city infrastructure are open, scalable and interoperable. The deployed systems must operate within 4 layers – Sensory layer, communication layer, data layer and application layer adhering to relevant security controls as mandated by the MoUD guidelines.
2. Bidders shall ensure that all the interfaces between IoT devices, field sensors, device applications and storage deployed in smart city are encrypted using appropriate protocols, algorithm and key pairs.
3. All transport link communication must be encrypted and sensitive data both in rest and transit is to be secured using encryption.
4. Bidders must ensure that all the changes made to the smart city infrastructure incl. of IoT field devices, sensors and related applications should be tracked and recorded in order

to enable security monitoring of the infrastructure. The maintained logs should be systematically collated, enabling the access of critical information as per date, fortnight, month, quarter, year etc.

5. Bidders should ensure that separate environments are maintained for production, test and development for smart city infrastructure and solutions to reduce the risks of unauthorized access or changes.
6. Bidders must ensure that smart city IT systems are designed in such a way that only authenticated users have access to the smart city database. Also, the provision of access has to be routed only through designated applications.
7. Bidders must ensure that sensitive data is stored in the smart city database in an encrypted format thereby curtailing the database administrator from reading or modifying the stored sensitive data.
8. Bidders must ensure that the smart city architecture should include a VPN solution enabling designated users to access necessary applications and functions from remote applications.
9. Bidders must enable for the maintenance of an audit trail to record all the administrator, user level activities including the failed attempts thereby enabling a robust high-level security monitoring of the smart city security infrastructure.
10. Bidders must ensure that the smart city components – Network elements, Operating system, Applications etc. are in sync and adhere to a singular master clock. Thereby ensuring an appropriate logging/ time stamping of incidents and bolstering smooth operation of the smart city.
11. Bidders must ensure that adequate security controls are deployed against the tampering of log information and unauthorized access to the smart city infrastructure such as the data center, IoT device control room etc.
12. Bidders must ensure that platforms hosted in the central data center support multi-tenancy with adequate authentication and role-based access. This can be achieved by utilizing Authentication and privilege management technology thereby controlling the access of data as per user privileges.
13. Bidders must ensure that the smart city architecture accounts for latency issues for the flow of data between devices. Suitable protocols should be utilized to minimize data flow latency upon management of heterogeneous data.
14. Bidders must strictly make sure that the communication between IoT field devices and their respective management applications happens only over a data layer (digital platform). Thereby enabling this designated layer to be the one true source of data abstraction, normalization and correlation.
15. Bidders must ensure that the smart city IT infrastructure including the Wi-Fi network adheres to relevant and applicable security standards and protocols. Also, bidders must make sure that the Application Program Interfaces (APIs) are published and the IT systems run on standard protocols.
16. Bidders must ensure that the smart city architecture end-to-end has adequate security controls to enforce safety, privacy and integrity of confidential data. Necessary controls must be deployed to protect the integrity of data flowing into the control systems and other critical infrastructure.

17. Bidders must enable for wireless/ broadband architecture used in the smart city infrastructure to interface with other/citywide wireless networks thereby enabling interoperability.
18. Bidders must ensure that IoT field devices and sensory equipment operating within the smart city periphery connect only to authorize wireless networks. Secure Wi-Fi guidelines as prescribed by the Department of Telecom must be followed.
19. Bidders must make sure that the wireless layer of the smart city network is appropriately segmented, bifurcating the network into various trusted zones. Thereby segregating public and utility networks via VPN (Virtual private networks), ensuring that the traffic from internet users is not routed into sensor networks and vice versa.
20. Bidders must enable for the authentication of the sensory equipment during the provisioning of the sensors and connection into the smart city infrastructure.
21. Bidders must ensure that the data aggregators used for enabling the interoperability between field IoT devices and sensors functioning on different protocols incorporate appropriate authentication and encryption at the aggregator gateway when field devices are not capable of authenticating /encrypting critical information.
22. Bidders must ensure that the IoT field devices and sensory equipment deployed in smart city periphery must not have a physical interface for administration. System and Network monitoring should be only performed remotely thereby ensuring local cyber-attacks/ tampering of field devices is curtailed.
23. Bidders must ensure appropriate network segregation. The smart city data center must be systematically segmented into multiple zones. Each zone must have a dedicated functionality. IoT field devices and sensory equipment must be connected to a completely separate network isolated from public networks and other private networks.
24. Bidders must make sure that the internet facing segment of the data center must incorporate a DMZ (Demilitarized zone), where customer application servers would be located. Predefined ports must be assigned for enabling the communication between the customer application servers and utility application servers to facilitate the access/transfer of data.
25. Bidders must ensure that Smart city data centers are well equipped with adequate security controls to protect the confidentiality, integrity and accessibility of critical data. The center should consider including cyber security systems such as firewalls, Intrusion detection & Intrusion prevention systems, Web Application Firewalls, Behavioral analysis systems for anomaly detection, Correlation engine, Denial of Service prevention device, Advanced Persistent Threat notification mechanism, Federated identity, access management system etc.
26. Bidders must ensure that the Smart city cyber security infrastructure incorporates high level security and monitoring controls such as SIEM (Security Information and Event Management) tools on all networks, field devices and sensors to identify malicious traffic.
27. Bidders must ensure all smart city applications must be hosted within India and must undergo static and dynamic security testing before deployment. Also, the applications must be periodically (at least once a year) tested for adequate security control.
28. Bidders must ensure that the proposed smart city architecture provides for:
  - a. Automatic and secure firmware updates

- b. Device logging and auditing capabilities
  - c. Vendor self-certification for non-existence of backdoors, undocumented and hard coded accounts.
29. Bidders must ensure that all the information on security incidents is regularly shared with Indian Computer Emergency Response Team (CERT-In) and NCIIPC (National Critical Information Infrastructure Protection Centre) and their help is sought for appropriate mitigation and recovery from the security incidents.
30. Bidders shall ensure that Data encryption at rest shall be implemented using departments managed keys, which are not stored in the cloud.
31. The bidder shall setup Cyber Security Continuous Monitoring process to monitor - physical environment, External service provider activity etc. to detect potential cyber security incidents.

### **11.9 Information Systems Acquisition, Development and Maintenance**

1. The Bidder shall prepare the detailed technical security requirement as part of the 'Software Requirement Specification' document with secure coding guidelines for development of applications for smart city.
2. The Bidder shall incorporate validation checks into smart city applications to detect any corruption of information through processing errors or deliberate acts.
3. The Bidder shall obtain information about technical vulnerabilities of information systems being used in smart city, evaluate the exposure to such vulnerabilities, and take appropriate measures to address the associated risk.
4. The bidder shall implement maintenance and repair process of smart city IT assets in timely manner, with approved and controlled tools.

### **11.10 Business Continuity Planning and Disaster Recovery**

1. The Bidder shall implement and operate Disaster Recovery site for the Smart city infrastructure and related IT & OT applications. IT & OT applications and processes should be supported from the disaster recovery site.
2. The Bidder shall define Business Continuity and Disaster Recovery plan and will perform the testing on a half yearly basis

### **11.11 Information Security Audits**

The bidder shall ensure Information security audits of the smart city infrastructure and related applications by a CERT-In empaneled vendor. VA/PT (Vulnerability assessment and Penetration Testing) activities, audits and application security testing must be carried out on twice-a-year basis ensuring optimal operation and security of the smart city infrastructure and applications. Teams carrying out the audit exercise must be different

from the implementation teams. Systematic actionable need to be derived post audits and necessary changes need to be made periodically.

#### **11.12 Security Operations Center**

The bidder shall set up Security Operations Centre to ensure continuous monitoring and manage all kinds of cyber security operations related to smart city such as Incident Management, Logging and Monitoring, Anti-virus Management, Threat Intelligence Support, Secure Technology Disposal and other cyber security support activities to ensure secured smart city ecosystem.

#### **11.13 Awareness Training**

The bidder shall deploy appropriate resources to support periodic awareness training based on latest standards of ISMS. The trainings must focus on educating relevant employees (including privileged users, third party, senior management etc.) on necessary security practices and processes to be followed in order to maintain the Confidentiality, Integrity and Availability of critical data.

#### **11.14 Security Controls for Cloud Services**

The security controls for creating and managing cloud services shall comply with the following guidelines.

Empanelment of Cloud Service Offerings CSPs (Cloud Service Provider) facilities/services shall be compliant with regulative directives and industry best practices. The SLA shall be based on the guidelines issued by Government Departments on contractual terms related to Cloud Services (MeitY guideline dated 31/03/17). The security controls should include the following:

- a) The CSP should be empaneled by MeitY for providing cloud services. The CSPs facilities/services shall be certified to be compliant to the following standards: ISO 27001, ISO 27017, ISO 27018, ISO 20000-9, ISO/IEC 20000-1 & PCI DSS
- b) The CSP/Service Provider shall comply or meet any security requirements applicable to CSPs/Service Providers published (or to be published) by MeitY or any standards body setup / recognized by Government of India from time to time and notified to the CSP/Service Providers by MeitY as a mandatory standard.
- c) The CSP/Service Provider shall meet all the security requirements indicated in the IT Act 2000, the terms and conditions of the Provisional Empanelment of the Cloud Service Providers and shall comply with the audit criteria defined by STQC.
- d) Incident Management shall be managed by CSP / third party.
- e) Periodic secure code review shall be performed for cloud applications.
- f) Data encryption at rest / transit depending on sensitivity of data shall be implemented using departments managed keys, which are not stored on the cloud.



- g) The CSP will undertake to treat information passed on to them as classified. Such Information will not be communicated / published / advertised by the CSP to any person/organization without the express permission of the Department.
- h) CSP shall inform all security breach incidents to Smart City management on real time.
- i) CSP shall ensure data confidentiality and mention Sub-contractual risk shall be covered by CSP.
- j) E-Discovery shall be included as clause in SLA with CSP. It is the process of locating, preserving, collecting, processing, reviewing, and producing Electronically Stored Information (ESI) in the context of or criminal cases/proceedings or investigation. Logging and reporting (e.g., audit trails of all access and the ability to report on key requirements/indicators) must be ensured.
- k) The Law Enforcement Agency as mandated under any law for the time being in force may seek access to information stored on cloud as provided by the Service Provider. The onus shall be on the CSP to perform all due diligence before releasing any such information to any such law enforcement agency.
- l) CSP must ensure location of all data related to smart cities in India only.
- m) The Cloud Service Provider's services offerings shall comply with the audit requirements defined under the terms and conditions of the Provisional Empanelment of the Cloud Service Providers (or STQC /MEITY guidelines. The Audit, Access and Reporting Requirements should be as per the terms and conditions of the Provisional Empanelment of the Cloud Service.
- n) CSP's exit Management Plan shall include - Transition of Managed Services & Migration from the incumbent cloud service provider's environment to the new environment and shall follow all security clauses for smooth transition.
- o) SLA with CSP shall cover performance management & dispute resolution escalation. Guidelines on Service Level Agreement issued by MeitY lists out the critical SLAs for cloud services.
- p) Identification and problem resolution (e.g., helpline, call center, or ticketing system) mechanism must be defined.
- q) Change-management process (e.g., changes such as updates or new services) must be defined.
- r) Appropriate segregation of Virtual Private Cloud (VPC) security rules defined as part of firewall to restrict access, Role based access management, Logging and monitoring shall be ensured.
- s) VPN gateway must be setup to ensure controlled access, appropriate security rules must be employed to encrypt outward data flow, IDS, IPS, API Gateways to be setup and ELB logs to be maintained for any activities and access and exceptions to carried out in the cloud setup, Database logs to be routed as part of the Logging VPC setup.
- t) Digital Certificate shall be implemented for secure access.

- u) Web Application Firewall must be provided, Host IPS must be setup on all the Web servers, Web servers must be configured as per the CIS hardening guidelines and baseline security requirements, logging and monitoring should be enabled.
- v) Application access between hosted smart city applications shall be segregated, internal infrastructure and external traffic, Role based access must be defined, hardening of database instances as per the CIS baselines configuration guidelines in the cloud setup must be ensured, Logging and monitoring must be enabled.
- w) For SLAs to be used to steer the behavior of a cloud services provider, imposition of financial penalties is to be incorporated.
- x) Monitor Vendor Service level agreement for annual end-to-end service availability of 99.999 percent. The end to end service agreement should be in place for minimum period of six years form the date of operations of the systems.

## 12.0 ANNEXURE VIII- LIST OF LOCATIONS

### 12.1 Locations for City Surveillance System

#### A. EAST - DCP

S. No	Locations	Latitude	Longitude	Fixed	PTZ	Total
1	Six Mile VIP Road Junction	N26.07.57	E91.48'307476	6	1	7
2	Six Mile Jayanagar NRL Tinali	N26.7'43.2984	E91.48'21.2868	3	1	4
3	BagharbariTinali	N26.8'1.6944	E91.49'28.542	3	0	3
4	Basistha Charali/Junction	26.6'44.0352" N	91.47'51.6228" E	6	2	8
5	BeltolaTinali/Junction	26.7'43.0464"N	91.48'4.5612"E	3	1	4
6	Bhangagarh Bus Stop	N 26.10'1.3548	E 91.45'59.2524	2	0	2
7	Bhetapara Chariali/ Junction	N26.7'13.314	E91.47'13.7328	4	1	5
8	Ghoramora Chariali	N26.7'14.304	E91.46'44.6592	4	1	5
9	Bhetapara Road2	N26.7.21.94	E91.47.13.29	2	1	3

S. No	Locations	Latitude	Longitude	Fixed	PTZ	Total
10	Bhetapara Road4 (HockyStadium)	26.6'57.4848" N	91.47'13.542" E	2	0	2
11	Bhetapara Road5 (KaliMandir road crossing)	26.7'3.2592" N	91.47'3.534"E	2	0	2
12	Bhetapara Road6 (KaliMandirRoad)	26.7'9.5592" N	91.47'13.8984" E	1	0	1
13	Borbari Near Pratiksha Hospital	26.9'30.6792	91.48'44.1252	2	0	2
14	Borbari Junction	26.9'6.1272	91.48'41.0796	4	0	4
15	CID Bus Stop (BeltolaBasisthaRoad)	N 26.9'22.5936	E 91.46'42.2436	2	0	2
16	Cinemax Dona Planet	N 26.9'39.78	E 91.46'19.8372	2	0	2
17	DownTown/ TrafficJunction	N 26.8'20.9905	E91.46'59.0.664	2	1	3
18	Ganeshguri Bus Stop	N 26.8'48.12	E91.47'21.12	2	0	2
19	Guwahati Medical Collage Hospital Gate	N26.9'38.0556	91.46'4.1664	3	1	4
20	Hatigaon Chariali	N26.7'44.1875	E91.47'11.0256	4	1	5
21	Hatigaon High School,Lakxim Nath Bezbaruah path Crossing	N26.07'58.53	E91.47'08.52	3	0	3
22	Hiteshwar Saikia Collage Panjabari Road	N26.7'57.7668	91.48'46.8144	3	0	3
23	Housefed Bus Stop	N26.8'12.0048	E91.47'29.2848	2	0	2
24	Housing Complex1, Old Passport Office	N26.7'56.0928	E91.47'37.6728	3	0	3
25	Housing Complex2, Sijubari Mazar Road	N26.7'48'5364	E91.46'26.0328	3	0	3
26	Juripar bus stop, Panjabari road	N26.7'59.214	E91.49'3.7704	3	0	3
27	Shankardev Kalakshetra	N26.8'0.078	E91.49'17.6592	3	1	4
28	Khanapara junction 2	N26.7'11.2944	E91.49'20.1576	3	0	3
29	Khanaparafield, APSC point	26.7'17.5692" N	91.49'2.4888" E	4	1	5
30	Khanaparafield2, Koinadhora	26.5'40.1352"N	91.47'4.182" E	3	1	4
31	Lakshimi Mandir bus stop	N 26.8'22.4736	E 91.47'24.9216	3	1	4
32	Jayanagar chariali traffic point	26.7'20.2296" N	91.48'21.9168" E	4	0	4
33	NERIM road, NH37 crossing	26.6'49.0896" N	91.48'20.4768" E	3	0	3
34	Sankaradev Nethralaya	26.7'16.356" N	91.47'56.76" E	2	1	3

S. No	Locations	Latitude	Longitude	Fixed	PTZ	Total
35	Puranbasti Panjabari road	N26.7'58.3752	E91.48'54.8679	3	0	3
36	Rahman Hospital, VIP road	N26.8'5.5932	E91.48'34.1784	1	0	1
37	Rajdhani Masjid Circle	N26.8'30.6888	E91.47'11.1768	4	1	5
38	Rukmini gaon bus stop	N26.8'7.7712	E91.48'9.8424	2	0	2
39	IAS Colony	26.7'16.9176" N	91.48'52.308" E	2	0	2
40	Sewali path, Hatigaon road	N26.8'12.0552	E91.47'8.7828	2	0	2
41	Sijubari junction	N26.7'44.8068	E91.46'45.9228	4	1	5
42	Sijubari Mazar	N26.7'53.83	E91.46'26.74	3	1	4
43	Supermarket	26°08'29.0"N	91°47'43.9"E	3	1	4
44	Survey bus stop	N26.7'47.6976	E91.47'42.63	2	1	3
45	Walford bus stop	N 26.9'19.6196	E 91.46'49.6416	2	0	2
46	Wireless	N26.08'04.34	E91.47'33.82	2	0	2
47	Agriculture University, Khanapara	26.7'14.502" N	91.49'18.12"E	3	0	3
48	Dakhingaon	26.7.51.384" N	91.45'36.5112" E	3	0	3
49	Dakhingaon Road 3	26.7'50.9448" N	91.45'39.4344" E	2	0	2
50	Dakshingaon Burha Masjid	26.7'50.4336" N	91.45'40.2912" E	2	0	2
51	Dakshingaon Road1	26.7'50.9448"N	91.45'39.4344" E	2	0	2
52	Dakshingaon Road2	26.7'50.9448" N	91.45'39.4344" E	2	0	2
53	DPI	N 26.8'39.1848	E 91.46'27.4908	2	0	2
54	Jatiya	N 26.8'25.44	E 91.44'46.08	3	0	3
55	Kahilipararoad1(Lalganesh-Lokhraroad)	N 26.8'13.8228	E 91.44'43.3104	2	0	2
56	Kahilipararoad2(Lalganesh-mandirroad)	N 26.8'13.0228	E 91.45'46.08	2	0	2
57	Kahilipara road3 (Nr. Bishnu Rabha path)	N 26.8'13.934	E 91.46'25.9968	2	0	2
58	LakhmiNagar	26.8'20.288" N	91.46'56.9388" E	3	0	3
59	Lakhra Road2 (Dakhin goan junction)	26.8'33.9576" N	91.44'2.3532" E	3	0	3
60	Lalmati	26.6'39.42" N	91.46'35.0184" E	2	0	2
61	Lakhra junction highway	26.6'28.6164" N	91.45'21.6396" E	6	1	7
62	Lakhra road–Hocky Stadium road	26.7'2.5104" N	91.46'1.2504" E	2	1	3
63	Lakhra Road3	26.8'27.4272" N	91.44'29.5512" E	3	0	3

S. No	Locations	Latitude	Longitude	Fixed	PTZ	Total
64	Lakhra Road4	26.9'20.034" N	91.44'22.9236" E	3	0	3
65	Hatigaon Road–highway crossing near Lalmati junction	26.7'13.60728" N	91.47'16.1376" E	4	1	5
66	Post Office bus stop, GS road	N 26.9'32.706	E 91.46'29.8846	2	0	2
67	Powerhouse	N.26.8'29.4756	E 91.45'25.9056	3	0	3
68	Sarusajai gate junction	26.7'3.1116" N	91.45'30.9852" E	6	2	8
69	Sarusajai 2(kalimandir road crossing)	26.6'51.9984" N	91.45'54.576" E	2	0	2
70	Sarusajai Stadium	26.6'56.682" N	91.45'36.9036E	3	1	4
71	SB, Kahilipara main road	N 26.8'39.7392	E 91.46'17.7744	2	0	2
72	Training centre/ Shiv mandir road crossing, Sixmile	N.26.7'45.228	E91.48'37.9836	4	0	4
73	10AP	N26.8'40.3584	E91.45'59.8968	4	0	4
74	Beharbari chariali	26.6'42.5304" N	91.46'99.7004" E	4	0	4
75	Ganeshguri flyover (Starting of the Bridge six mile side)	26°08'54.6"N	91°47'12.7"E	2	1	3
76	Ganeshguri flyover (Starting of the Bridge Bhangagarh side)	26°09'07.7"N	91°46'57.6"E	2	0	2
77	Ganeshguri (Below the bridge zoo road side)	26°09'00.9"N	91°47'06.2"E	2	0	2
78	Ganeshguri (Below the bridge Last Gate side)	26°08'57.7"N	91°47'07.6"E	2	1	3
79	Hengerbari PHE chariali	N26.9'6.6816	E91.47'32.5716	4	0	4
80	Dispur PS	N26.8'35.95	E91.47'34.09	2	0	2
81	Hatigaon PS	26°07'36.1"N	91°47'12.4"E	2	1	3
82	Bhangagarh PS	26°09'37.7"N	91°46'03.9"E	2	1	3
83	Basistha PS	26°06'43.3"N	91°47'42.0"E	2	0	2
84	Hengerbari LP School Nr. BJP Party Office bylane	N26.9'3.3804	E91.48'52.5012	4	1	5
85	Ginger Hotel bylane, VIP road	N26.8'51.936	E91.48'43.2864	1	0	1
86	Hanuman mandir, Ganeshguri	N 26.8'47.04	E 91.47'22.3296	2	0	2
87	Sixmile flyover-Jaya nagar road junction	N26.7'51.4132	E91.48'30.2436	4	0	4

S. No	Locations	Latitude	Longitude	Fixed	PTZ	Total
88	Hengerabari road tinali	N26.8'55.3488	E91.47'12.318	3	0	3
89	Hengerbari- Borbari road	N 26.9'2.0232	E 91.48'15.5124	3	0	3
90	ABC traffic point	N 26.9'42.5376	E 91.48'15.5124	4	0	4
91	Bhangagarh traffic point near bigbazaar	N 26.9'55.5372	E 91.46'18.7392	4	0	4
92	Sreenagar traffic point	N 26.9'30.0636	E 91.47'33.0529	2	0	2
93	Silpagram, panjabari	N 26.7'50.9124	E 91.49'15.8124	3	0	3
94	Japorigogroad-Nayanpur road junction	N 26.9'20.2284	E 91.49'15.8124	4	0	4
95	Japorigog- Anandapur tinali	N 26.9'22.1976	E 91.47'27.7944	3	0	3
96	Pilingkata road	26.6'29.5956" N	91.48'1.6092" E	4	0	4
97	Natun bazaar tinali, Patharkuchi	26.6'29.0628" N	91.47'10.6368" E	3	0	3
98	Basistha mandir bus stop	26.5'42.3564" N	91.47'9.5316" E	8	1	9
99	Sachal road	N 26.8'35.1168	E 91.48'43.7388	2	2	4
100	VIP road7, Chandan nagar	N 26.8'20.3856	E 91.48'40.4028	4	0	4
101	Hengerbari road, Housing Colony bus stop	N 26.9'1.2132	E 91.47'24.0216	3	0	3
102	Lakhimi Path Beltola	N26.7'29.60	E91.47'53.09	2	0	2
103	AG Office bus stop	26.7'2.2692" N	91.47'54.2652" E	4	0	4
104	Sankar path, Hatigaon	N26.8'10.56	E91.47'8.54	2	0	2
105	Arunudoi path, Hatigaon	N26.8'6.5148	E91.47'8.2536	3	0	3
106	RN Choudhuri path	N26.8'3.26	E91.47'8.95	3	0	3
107	Natun path, Hatigaon	N26.8'1.39	E91.47'8.67	2	0	2
108	Bishnujyoti path, Hatigaon	N26.8'1.95	E91.47'8.61	3	0	3
109	Flowerlane, Hatigaon road	N26.7'49.64	E91.47'10.44	2	0	2
110	Hatigaon road1	N26.7'36.786	E91.47'11.598	1	0	1
111	Hatigaon road2	N26.7'35.2812	E91.47'11.0652	2	0	2
112	Reliance market jayanagar	26.74'.8072" N	91.48'22.3992" E	2	0	2
113	NERIM Institute	26.8'20.2884" N	91.46'56.9388" E	1	0	1
114	Near Govindam, Downtown	N 26.8'15.63	E 91.48'0.648	3	0	3
115	Goal Chakkar, GMCH	N 26.9'32.5908	E 91.45'57.5604	4	1	5
116	GMCH Hostel road	N 26.9'36.2112	E 91.46'0.246	2	1	3
117	Veterinary Collage crossing	26.7'16.4856" N	91.49'17.472" E	2	1	3
118	Chaolung Sukaphaa path, Hatigaon	N26.7'44.54	E91.47'02.08	1	0	1

S. No	Locations	Latitude	Longitude	Fixed	PTZ	Total
119	Khanka Road, Sijubari, Hatigaon	N26.7'30.0792	E91.46'45.012	2	0	2
120	Kanaklata Path, Sijubari, Hatigaon	N26.7'29.306	E91.46'44.724	2	0	2
121	Chamata	N26.7'11.9892	E92.0'4.8708	3	0	3
122	Digaru Point	N26.7'19.7652	E91.58'23.3544	4	0	4
123	Nazirakhat	N26.7'18.8328	E91.55'39.5472	3	0	3
124	Medhikuchi	N26.7'14.3364	E91.54'36.2664	3	0	3
125	Patorkuchi	N26.7'6.0168	E91.53'42.2736	3	0	3
126	Khanapara fly over (Shillong Side)	26°07'10.8"N	91°49'32.5"E	2	1	3
127	Khanapara fly over (Basistha Side)	26°07'08.3"N	91°49'09.9"E	2	1	3
128	Khanapara fly over (Under the bridge- Veterenary College side)	26°07'13.1"N	91°49'19.4"E	2	1	3
129	Beltola SBI	26.7'27.0552" N	91.47'58.0884" E	3	0	3
130	Killing 9th mile	26.4'38.3196N	91.49'19.1964"E	3	1	4
131	Jorabat fly over	26.5'55.9284" N	91.51'44.3556" E	6	2	8
132	Ganesh Mandir, Khanapara	26.6'48.5064" N	91.50'8.3652" E	3	1	4
133	Topatoli	N 26.6'18.5296	E 92.9'44.83138	3	0	3
134	Dhopguri	N 26.6'31.85788	E 92.9'44.83138	2	0	2
135	Dimoria College Gate	N 26.6'51.73931	E 92.4'55.33194	2	0	2
136	Tetelia	N 26.7'23.32661	E 92.2'22.87921	3	1	4
137	Lalmati 22 mile	N 26.7'21.16596	E 92.0'49.7614	2	0	2
138	PCC Main Gate	26°08'38.2"N	91°47'31.1"E	4	2	6
139	PCC Employee Gate	26°08'24.9"N	91°47'30.4"E	2	1	3
140	Last Gate	26°08'22.7"N	91°47'23.3"E	2	1	3
141	Gate No. 14 MLA Hostel (Near DCP East Office)	26°08'41.4"N	91°47'13.0"E	2	1	3
142	Minister Colony (From PCC Employee Gate Side)	26°08'28.0"N	91°47'29.7"E	2	1	3
143	Minister Colony (From Dispur PS Side)	26°08'31.7"N	91°47'36.4"E	2	1	3
	<b>Total</b>			<b>399</b>	<b>53</b>	<b>452</b>

**B. WEST – DCP**

S. No.	Police Station	Location	Latitude	Longitude	Fixed	PTZ	Total
1	Azara PS	Under VIP Bridge	26° 06.036'N	91° 35.972'E	2	1	3
2	Azara PS	Dharapur Chariali	26°08.240'N	91° 37.673'E	3	1	4
3	Azara PS	Airport SOS Point	26° 06.195'N	91°35.609"E	2	1	3
4	Azara PS	Airport Parking	26° 06.305'N	91° 35.342'E	2	2	4
5	Azara PS	Bongara Petrol Pump	26° 05.226'N	91° 34.966'E	1	0	1
6	Azara PS	Azara PS	26° 06.987'N	91° 36.869'E	0	1	1
7	Azara PS	Khanamukh	26° 08.325'N	91° 33.116'E	1	1	2
8	Azara PS	e-Com Tower	26° 09.929'N	91° 36.270'E	1	1	2
9	Azara PS	Airforce Gate	26° 05.509'N	91° 35.152'E	0	1	1
10	Azara PS	Borjhar OP	26° 06.441'N	91° 36.303'E	0	1	1
11	Azara PS	Kahikuchi Bazar	26° 06.382'N	91° 36.250'E	1	1	2
12	Azara PS	Rani Gate	26° 05.979'N	91° 36.710'E	1	1	2
13	Azara PS	Airport Exit Point	26° 06.204'N	91° 35.568'E	1	1	2
14	Azara PS	Airport Last Point	26° 06.222'N	91° 35.497'E	1	1	2
15	Azara PS	SOS Road in front of Kiranshriee Hotel	26° 06.195'N	91° 35.809'E	0	1	1
16	Azara PS	VIP in front of Central bank	26° 06.102'N	91° 35.966'E	2	0	2
17	Azara PS	Dharapur In front of Canara Bank/UBI	26° 08.271'N	91° 37.663'E	2	0	2
18	Azara PS	Azara Godhuli Bazar	26° 06.977'N	91° 36.844'E	3	0	3
19	Azara PS	Garal Tiniali	26° 08.309'N	91° 36.396'E	3	1	4
20	Azara PS	Hatkhowapara, nearby Pepsi Gate	26° 07.764'N	91° 37.251'E	2	1	3
21	Azara PS	Patgaon Chowk nearby Pepsi Gate	26° 05.455'N	91° 36.721'E	2	1	3
22	Azara PS	Mountain Shadow Chowk In front of HDFC ATM	26° 06.633'N	91° 36.812'E	2	1	3



S. No.	Police Station	Location	Latitude	Longitude	Fixed	PTZ	Total
23	Azara PS	Matia Tiniali nearby Railway Station Parking	26° 06.304'N	91° 37.284'E	2	1	3
24	Azara PS	Jobe Gaon Chowk Patgaon- Rani Road	26° 04.762'N	91° 36.476'E	3	1	4
25	Azara PS	Rani Gate- Patgaon Road nearby Railway	26° 05.889 'N	91° 36.742'E	2	1	3
26	Gorchuk PS	Gorchuk Police Point	N 26° 6''56.893''	E91°42'30.945''	2	1	3
27	Gorchuk PS	Lokhra Police Point	N 26° 6''41.881''	E91°44'58.495''	2	1	3
28	Gorchuk PS	Boragaon Police Point	N 26° 7''21.851''	E91°41'8.471''	2	1	3
29	Gorchuk PS	Pamohi Tiniali	N 26° 6''15.785''	E91°42'24.162''	2	1	3
30	Gorchuk PS	ISBT Point	N 26° 6''55.575''	E91°43'17.817''	4	3	7
31	Gorchuk PS	Trade Centre	N 26° 6''52.826''	E91°43'33.946''	1	1	2
32	Gorchuk PS	Katahbari 1 No. Majid	N 26° 7''14.057''	E91°43'3.867''	2	0	2
33	Gorchuk PS	In front of DTO office, Betkushi	N 26° 6''47.65''	E91°43'52.12''	2	0	2
34	Gorchuk PS	Pamohi Vegetable Meket	N 26° 6''37.16''	E91°42'29.403''	3	1	4
35	Gorchuk PS	DPS Cutting, Gorchuk	N 26° 6''55.354''	E91°43'3.179''	2	1	3
36	Fatasil Ambari PS	Cycle Factory Chariali	26' 15937	E91°43'52.12''	2	1	3
37	Fatasil Ambari PS	Birubari Tiniali	26' 157400	91'74132	2	1	3
38	Fatasil Ambari PS	Colony Bazar (Shivam Apartment)	26' 1431	91'752670	1	1	2
39	Fatasil Ambari PS	Bataliyan Gate	26' 1477	91'74020	1	1	2
40	Fatasil Ambari PS	Lal Ganesh Tiniali	26' 14175	91'74091	2	1	3
41	Fatasil Ambari PS	Shankar Hotel Chowk	26' 12961	91'87420	1	1	2
42	Fatasil Ambari PS	Ganeshpara	26' 13761	91'7374	1	1	2

S. No.	Police Station	Location	Latitude	Longitude	Fixed	PTZ	Total
43	Fatasil Ambari PS	Dhiyenpara Kali Mandir (Nr. SBI Bank)	26' 14954	91'72481	1	1	2
44	Fatasil Ambari PS	Stadium Back Gate	26' 1446	91'72883	1	1	2
45	Fatasil Ambari PS	Stadium Front Gate	26' 14794	91'73696	1	1	2
46	Fatasil Ambari PS	Ambari Tiniali	26' 15846	91'73709	2	1	3
47	Fatasil Ambari PS	Itavhata Tiniali	26' 14907	91'73166	3	0	3
48	Fatasil Ambari PS	Direnpara Tilla near Masjid	26' 15099	91'72966	2	0	2
49	Fatasil Ambari PS	Datalpara near Petrol Pump	26' 12903	91'72062	2	1	3
50	Fatasil Ambari PS	Manpara near Bar	26' 13481	91'72338	2	0	2
51	Fatasil Ambari PS	Dhirenpara near Hospital	26' 14576	91'72792	3	1	4
52	Fatasil Ambari PS	Barsapara Bridge	26' 14817	91'73607	2	0	2
53	Fatasil Ambari PS	Colony Bazar near VIP Hotel	26' 15391	91'73987	3	1	4
54	Fatasil Ambari PS	Sonai Goli Road	26' 12497	91'74842	2	0	2
55	Fatasil Ambari PS	Ambari Kali Mandir	26' 1612	91'73429	2	1	3
56	Fatasil Ambari PS	Foot Bridge (Below), Maligaon	N26°9'33.38333"	91'73342	2	1	3
57	Jalukbari PS	Mahakal Ganesh Entry-to Kamakhya	N26°9'53.53423"	E91°41'46.40629"	0	1	1
58	Jalukbari PS	No. Gate (NF Rly. HQ.)	N26°9'35.82126"	E91°41'58.92281"	1	1	2
59	Jalukbari PS	Kamakhya Entry Point (Nursery)	N26°9'45.0437"	E91°42'17.57009"	1	1	2
60	Jalukbari PS	Adabari Tiniali	N26°9'30.43649"	E91°42'47.25828"	3	2	5
61	Jalukbari PS	In front of Raddison Blu	N26°8'29.81987"	E91°41'7.21961"	0	1	1
62	Jalukbari PS	Saraighat Entry Point	N26°10'54.62414"	E91°40'31.95617"	2	1	3

S. No.	Police Station	Location	Latitude	Longitude	Fixed	PTZ	Total
63	Jalukbari PS	Saraighat Exit Point	N26°10'3.41072"	E91°40'17.913"	2	1	3
64	Jalukbari PS	Satmile Point (Tiniali)	N26°9'5.76277"	E91°40'19.545"	2	1	3
65	Jalukbari PS	Sundarbari Point	N26°9'0.7173"	E91°31'15.51776"	2	1	3
66	Jalukbari PS	Pandu Cabin	N26°9'58.5765"	E91°40'17.46242"	1	1	2
67	Jalukbari PS	Kamakhya VIP Parking	N28°9'57.10039"	E91°41'14.62592"	1	1	2
68	Jalukbari PS	Bhupen Hazarika Samadhi Khetra	N26°9'27.60019"	E91°42'25.10474"	2	1	3
69	Jalukbari PS	Below the Jalukbari Fly Over	N26°9'27.84787"	E91°40'18.148245"	2	2	4
70	Jalukbari PS	Katiya Dalang	N26.158032"	E91°40'25.14025"	3	1	4
71	Jalukbari PS	Maligaon OP (Gosala)	N 26°9'0.40234"	E 91°41'46.7088"	3	1	4
72	Jalukbari PS	Over Jalukbari Fly Over (Ghty entry side-1)	N 26°9'39.70127	E 91°40'17.68022"	2	1	3
73	Jalukbari PS	Over Jalukbari Fly Over (Sadilapur Point)	N 26°9'54.43183"	E 91°40'15.21149"	2	1	3
74	Jalukbari PS	Forest School Point	N 26°9'1.52834"	E 91°39'7.46093"	2	0	2
75	Jalukbari PS	Tetelia Point	N 26°8'10.26409"	E 91°40'25.97783"	2	0	2
76	Jalukbari PS	PNGB Road (Rail Gate)	N 26°9'26.28644"	E 91°41'47.23195"	2	1	3
77	Jalukbari PS	Kamakhya (Bon Durga Point)	N 26°9'45.43877"	E 91°42'18.63148"	2	0	2
78	Jalukbari PS	Maligaon Chariali	N 26°9'32.44432	E 91°41'46.54122"	3	1	4
79	Jalukbari PS	Gauhati University Back side	N 26°9'7.938"	E 91°39'19.87924"	2	0	2
80	Jalukbari PS	Adabari & Pandu Road SBI Point	N 26°9'37.22998"	E 91°41'6.54997"	2	0	2

S. No.	Police Station	Location	Latitude	Longitude	Fixed	PTZ	Total
81	Jalukbari PS	Engineering College point	N 26°8'39.6888"	E 91°38'31.4412"	2	0	2
82	Bharalumukh PS	Bharalumukh PS	N 26.10'23.814	E 91.43'46.932	1	1	2
83	Bharalumukh PS	Machkhowa Chariali	N 26.10'38.178	E 91.44'4.944	2	1	3
84	Bharalumukh PS	Kumarpara Panchali	N 26.10'11.916	E 91.44'8.022	2	1	3
85	Bharalumukh PS	Athgaon below the fly over	N 26.10'34.11	E 91.44'24.114	2	1	3
86	Bharalumukh PS	Above the fly over	N 26.10'30.55	E 91.44'18.426	1	3	4
87	Bharalumukh PS	Athgaon Goshala Turning point	N 26.10'21.744	E 91.44'25.074	1	0	1
88	Bharalumukh PS	GMC Bhootnath	N 26.10'9.756	E 91.43'20.112	1	1	2
89	Bharalumukh PS	Chabipul chariali	N 26.10'11.244	E 91.44'33.342	2	2	4
90	Bharalumukh PS	Sarabhhati Chariali	N 26.10'7.8	E 91.44'47.31	2	2	4
91	Bharalumukh PS	ITA Machkhowa	N 26.10'43.116	E 91.44'5.634	2	1	3
92	Bharalumukh PS	Apollo Point	N 26.10'27.564	E 91.43'50.64	1	1	2
93	Bharalumukh PS	Fatashil Chariali	N 26.10'5.676	E 91.44'12.258	1	1	2
94	Bharalumukh PS	MG road Gate No. 9	26.17335 N	91.73068 E	2	1	3
95	Bharalumukh PS	Alfresco Point	N 26°10'41.31948	E 91°44'2.55091°	2	0	2
96	Bharalumukh PS	Sankardev Udyan Site	N 26°10'30.414"	E 91°43'53.844"	2	0	2
97	Bharalumukh PS	Near SBI A.T Road (Rly Gate No. 08)	N 26°10'24.99"	E 91°43'54.312"	2	0	2
98	Bharalumukh PS	Kumarpara Near Kumar Nursing Home	N 26°10'16.52603"	E 91°44'0.77356"	2	1	3
99	Bharalumukh PS	Bishnupur Near Kalimandir Tiniali	N 26°10'3.63"	E 91°44'31.14"	2	0	2
100	Bharalumukh PS	Hariyana Bhawan	N 26°10'5.856"	E 91°44'3.702"	2	1	3

S. No.	Police Station	Location	Latitude	Longitude	Fixed	PTZ	Total
101	Bharalumukh PS	Sluice Gate Bharalumukh	N 26°10'8.286"	E 91°43'52.794"	2	0	2
102	Bharalumukh PS	Santipur	N 26°10'2.886"	E 91°43'40.008"	2	0	2
103	Bharalumukh PS	City Bus Stop Near Rly Gate No. 10	N 26°10'18.63"	E 91°43'30.936"	2	0	2
104	Bharalumukh PS	KRC Road near Amarawati	N 26°10'14.526"	E 91°44'0.504"	2	0	2
<b>Total</b>					<b>185</b>	<b>87</b>	<b>272</b>

### C. CENTRAL – DCP

S. No	PS/District	Locations	Latitude	Longitude	Fixed	PTZ	Total
1	Chandmari PS	Chandmari PS tinali (nr. Durga mandir/nr. Old university)	26.184,614	91.770,888	3	0	3
2	Chandmari PS	Maharshi vidya mandir, silpukhuri	26.113,322	91779520	0	1	1
3	Chandmari PS	Infront of/start of gandhi basti path, Silpukhuri	26.181,369	91.762,045	1	0	1
4	Chandmari PS	Railway gate no. 02 gandhi basti/ST - 13	26.181,823	91.763,793	2	0	2
5	Chandmari PS	Mamoni Roysem Goswami path gandhi basti nr. H/No. 1 bylane 06	26.183,468	91.768,965	3	0	3
6	Chandmari PS	Pubsarania/south sarania tinali (border area)	26, 176,091	91.763,685	3	0	3
7	Chandmari PS	Rajgarh Bihu toli turning (nr. School)	26.172,424	91.771,269	2	0	2
8	Chandmari PS	Rajgarh link rd. (nr. Guwahati commerce)	26.180, 125	91.775,235	6	0	6

S. No	PS/District	Locations	Latitude	Longitude	Fixed	PTZ	Total
		college)					
9	Chandmari PS	Chandmari Flyover	26.191, 273	91.772,876	4	0	4
10	Chandmari PS	Chandmari under flyover	26.191,273	91.772,876	7	0	7
11	Chandmari PS	New Guwahati SBI Branch	26.183, 573	91.781, 137	1	0	1
12	Chandmari PS	Bamunimaidan hanuman temple (border area)	26.183, 220	91.798, 150	1	0	1
13	Chandmari PS	Pratidin gali, Chandmari	26.183, 933	91.774, 497	1	0	1
14	Chandmari PS	Silpukhuri petrol pump (nr PB Chaliha path)	26.186, 138	91.763, 439	1	0	1
15	Chandmari PS	Rajgarh zoo road tinali traffic point	27, 182, 482	95.104.699	3	0	3
16	Chandmari PS	Chandmari Traffic junction point	26.183, 922	91.774, 497	3	0	3
17	Geetanagar PS	Aunti Gali	26.178,8759	91.775,8574	2	0	2
18	Geetanagar PS	Durga Mandir, Bye Lane point	26.172, 495	91.796,439	1	0	1
19	Geetanagar PS	Geetanagar High School (Field)	26.173.968	91.789, 480	3	1	4
20	Geetanagar PS	Narikalbari	26.170,434	91.788, 758	3	0	3
21	Geetanagar PS	Ambikagiri Nagar, Chariali	26.169, 006	91.781, 788	4	0	4
22	Geetanagar PS	Bhashkar Nagar bye Lane 02	26.175, 673	91.778,813	1	0	1
23	Geetanagar PS	Ambikagiri Nagar, Bye Lane, Zoo Road	26.168, 798	91.778, 751	1	0	1
24	Geetanagar PS	Akashi Path Tinali, Ambikagiri Nagar	26.167, 355	91.781, 149	3	0	3
25	Geetanagar PS	Central Mall point, Zoo Road	26.168, 611	91.779, 716	1	0	1
26	Geetanagar PS	LKRB Path	26.170, 145	91.775, 762	1	0	1

S. No	PS/District	Locations	Latitude	Longitude	Fixed	PTZ	Total
27	Geetanagar PS	Nabin Nagar near Sankardev Namghar Tiniali	26.170,834	91.773, 865	2	0	2
28	Geetanagar PS	Nabin Nagar near, H/No. 34	26.168, 532	91.774, 607	1	0	1
29	Geetanagar PS	Navin Nagar Tiniali, near H/No. 33, Bye Lane 03, Link Road	26.117, 696	91.738, 521	3	0	3
30	Geetanagar PS	Anil Nagar Rajgarh Link Road near pump station	26.169, 061	91.770, 978	4	0	4
31	Geetanagar PS	Hatigarh Traffic point Chariali	26.172, 927	91.784.805	2	0	2
32	Geetanagar PS	Zoo Tiniali Traffic Point	26.174, 678	91.777, 050	5	0	5
33	Geetanagar PS	RGB Road, State Zoo point	26.163, 812	91.780, 729	2	1	3
34	Geetanagar PS	Jonali taffic point	26.168,097	91.778,812	4	0	4
35	Geetanagar PS	In front of Shradhanjali kanan	26164440	91780028	2	0	2
36	Geetanagar PS	Lakhimi bye lane	26.166,078	91.779,456	1	0	1
37	Geetanagar PS	Doordarshan centre	26.170,595	91.779,255	2	0	2
38	Geetanagar PS	Rupalim path	26169168	91779018	1	0	1
39	Geetanagar PS	Entry point to Rajat kamal path	26171055	91777873	1	0	1
40	Geetanagar PS	Entry point to Uday path	26171188	91777301	2	0	2
41	Geetanagar PS	Entry point to Santi path	26172639	91777321	1	0	1
42	Geetanagar PS	Bye lane no 9	26173908	91776615	2	0	2
43	Geetanagar PS	Padma path	26174350	91776651	1	0	1
44	Geetanagar PS	Apurba sinha path	26.175,978	91.776,083	2	0	2

S. No	PS/District	Locations	Latitude	Longitude	Fixed	PTZ	Total
45	Geetanagar PS	Arunachal path	26176469	91776225	2	0	2
46	Latasil PS	Latasil PS	26.18999	91.75222	2	1	3
47	Latasil PS	Latasil Field (in all four corner)	1. 26.19024 2. 26.19099 3. 26.19073 4. 26.18993	1. 91.75273 2. 91.75236 3. 91.75137 4. 91.75161	4	0	4
48	Latasil PS	Ujan Bazar Fish Market	26.19521	91.75601	2	1	3
49	Latasil PS	Infront of DC Bungalow, Panikol	26.19793	91.76121	1	1	2
50	Latasil PS	Ujan Bazar View Point (Covering till Raj Bhawan Strech)	26.19888	91.76275	4	1	5
51	Latasil PS	Assam State Muslem Tuming Point	26.1857	91.75216	3	0	3
52	Latasil PS	Rabindra Bhawan (covering press club)	26.18544	91.75263	2	0	2
53	Latasil PS	Guwahati Club T C Point	26.18519	91.75823	4	0	4
54	Latasil PS	Lamb RD, S K Bhuyan Point	26.18724	91.75471	2	0	2
55	Latasil PS	Jorpukhuri Point	26.18866	91.75394	3	0	3
56	Latasil PS	Ujan Bazar, F C RD Nr. Goswami Clinic Chariali	26.19102	91.75554	4	0	4
57	Latasil PS	Judges Guest House	26.19695	91.76202	2	0	2
58	Latasil PS	Navagrah Temple M.C. Road	26.19111	91.76539	3	0	3
59	Latasil PS	Guwahati Club Traffic Point (Lakhinath Bejbaruah Chowk)	26.18505	91.75688	4	0	4
60	Latasil PS	Kamrup Natya Samiti M.C. School	26.19066	91.75439	4	0	4
61	Panbazar PS	Panbazar PS	26°11'01"	091°44'24"	1	1	2
62	Panbazar PS	MMCH Point Tiniali	26°11'04"	091°44'24"	3	0	3



S. No	PS/District	Locations	Latitude	Longitude	Fixed	PTZ	Total
63	Panbazar PS	Surkeshwar Temple	26°11'14"	091°44'28"	3	0	3
64	Panbazar PS	Panbazar Pani Tanki Tinali	26°11'14"	091°44'28"	2	0	2
65	Panbazar PS	Commissioner of Police	26°11'15"	091°44'29"	0	1	1
66	Panbazar PS	DC Office/Meghdoot Bhawan	26°11'15"	091°44'29"	2	1	3
67	Panbazar PS	Judges Field Point	26°11'18"	091°44'32"	1	0	1
68	Panbazar PS	High Court Point Tinali	26°11'20"	091°44'34"	3	0	3
69	Panbazar PS	High Court Digholi Point	26°11'12"	091°44'39"	0	1	1
70	Panbazar PS	District Library point Tinali	26°11'05"	091°44'53"	3	0	3
71	Panbazar PS	RBI Panchali	26°11'07"	091°44'57"	5	0	5
72	Panbazar PS	Food Villa Chariali	26°11'12"	091°44'39"	4	0	4
73	Panbazar PS	Panbazar Lakhtokia Bridge	26°11'01"	091°44'42"	3	1	4
74	Panbazar PS	Hari Sabha Tinali	26°11'08"	091°44'29"	3	0	3
75	Panbazar PS	Railway gate no. 2 tinali	26°10'59"	091°44'43"	3	0	3
76	Panbazar PS	Farukdin Ali path Tinali	26°10'54"	091°44'30"	3	0	3
77	Panbazar PS	Sikh Temple Chariali	26°10'57"	091°44'18"	4	0	4
78	Panbazar PS	Viswaratna Hotel AT Road, Chariali	26°11'41"	091°44'33"	4	0	4
79	Panbazar PS	Lakhtokia Bridge	26°11'01"	091°44'42"	2	0	2
80	Panbazar PS	Phool Gali Tanali, Panbazar	26°11'14"	091°44'28"	3	0	3
81	Panbazar PS	Kamarpati Masjid Gali side tinali	26°11'12"	091°44'37"	3	0	3
82	Fancybazar OP	SRCB Road / MG Road	26°10'54"	091°44'31"	3	0	3
83	Fancybazar OP	MS Road / MG Road	26°10'49"	091°44'09"	3	0	3
84	Fancybazar OP	Chamber Road/ MG Road	26°10'48"	091°44'06"	1	0	1
85	Fancybazar OP	Kedar Road / M G Road	26°10'48"	091°44'07"	3	0	3

S. No	PS/District	Locations	Latitude	Longitude	Fixed	PTZ	Total
86	Fancybazar OP	T R P Road/Chamber Road Chariali	26°10'51"	091°44'15"	4	0	4
87	Fancybazar OP	T R P Road/Lakhi Goli	26°10'50"	091°44'12"	3	0	3
88	Fancybazar OP	Taxi Stand, Nr Old Jail Panchaili	26°10'49"	091°44'14"	5	0	5
89	Fancybazar OP	F Masjid Cariali	26°10'47"	091°44'10"	4	0	4
90	Fancybazar OP	M G Road - S Road	26°10'59"	091°10'58"	2	0	2
91	Fancybazar OP	In front of LIC office	26°10'58"	091°44'18"	1	0	1
92	Fancybazar OP	Axis Bank ATM	26°10'58"	091°44'20"	1	0	1
93	Fancybazar OP	Akshay Tower	26°10'57"	091°44'21"	2	0	2
94	Fancybazar OP	Ashok Garment Shop	26°10'57"	091°44'21"	2	0	2
95	Fancybazar OP	Bata	26°10'56"	091°44'22"	2	0	2
96	Fancybazar OP	Opposite Sikh Temple	26°10'55"	091°44'26"	2	0	2
97	Fancybazar OP	City Center	26°10'55"	091°44'27"	2	0	2
98	Fancybazar OP	M Road, infront of GMC Market	26°10'58"	091°44'39"	2	0	2
99	Fancybazar OP	Lakhi Gali/MG Road Tinali	26°10'49"	091°44'09"	3	0	3
100	Paltanbazar PS	Paltanbazar PS	26.18098	91.75107	2	1	3
101	Paltanbazar PS	Paltanbazar Janta Point Chariali	26.18005	91.75143	4	0	4
102	Paltanbazar PS	Solapara path	26.1782	91.75291	1	0	1
103	Paltanbazar PS	Apsara Cinema Hall including covering central bank infront	26.17732	91.75422	2	0	2
104	Paltanbazar PS	Infront of Dakhin sararnia point at starting point	26.17488	91.74963	1	0	1

S. No	PS/District	Locations	Latitude	Longitude	Fixed	PTZ	Total
105	Paltanbazar PS	Iskon Mandir, south sarania	26.17688	91.7593	1	0	1
106	Paltanbazar PS	Gandhi Mandap Covering road	1. 26.1775 2. 26.17749 3. 26.17739	1. 91.76781 2. 91.76785 3. 91.76767	3	0	3
107	Paltanbazar PS	Gandhi mandap approach road chariali	26.17436	91.76768	4	0	4
108	Paltanbazar PS	NRC office backside HUB	26.16565	91.76768	2	0	2
109	Paltanbazar PS	Bhangagarh under flyover nr. Big bazar	26.16565	91.76798	5	0	5
110	Paltanbazar PS	Ulubari ACB Rd Tinali	26.16828	91.75395	3	0	3
111	Paltanbazar PS	Ulubari DGP office	26.17	91.75494	2	1	3
112	Paltanbazar PS	Birubari Bazar Chowk Tnali	26.16017	91.74958	3	0	3
113	Paltanbazar PS	Ulubari K F C point	26.16555	91.76772	4	0	4
114	Paltanbazar PS	Nepali mandir chowk	26.17867	91.75048	3	0	3
115	Paltanbazar PS	Meen bhawan ulubari	26.16726	91.74964	2	0	2
116	Paltanbazar PS	Police Housing Board (backside of DGP Office)	26.17055	91.75116	2	0	2
117	Paltanbazar PS	A K Azad rd nr. SBI + UCO bank tinali	26.17478	91.74953	3	0	3
118	Paltanbazar PS	Rehabari bilpar (inside gali)	26.17506	91.74778	1	0	1
119	Paltanbazar PS	Himatsinka petrol pump tinali A T Road	26.17919	91.74384	3	0	3
120	Paltanbazar PS	ASTC main gate paltan bazar	26.18093	91.74967	3	1	4
121	Paltanbazar PS	Islampur Tinali nr. Yubak sangh	26.18145	91.75884	3	0	3
122	Paltanbazar PS	Gandhi Basti Tinali	26.18153	91.76188	5	1	6
123	Paltanbazar PS	B. Boruah Rd	26.17852	91.75679	1	0	1

S. No	PS/District	Locations	Latitude	Longitude	Fixed	PTZ	Total
124	Paltanbazar PS	Nehru Stadium	26.1796	91.75677	1	1	2
125	Noonmati PS	Noonmati PS	26.18257	91.80292	2	0	2
126	Noonmati PS	IOCL Untake Point Tinali	26.20342	91.790251	3	0	3
127	Noonmati PS	IOCL gate No. 2 nr. Play ground	26.18725	91.80198	1	0	1
128	Noonmati PS	Sunsali Ferri Ghat	26.20392	91.79376	1	1	2
129	Noonmati PS	Sector No. 1 (nr. IOCL Playground)	26.20303	91.79522	3	0	3
130	Noonmati PS	Shristi nagar Tinali	26.20635	91.80641	3	0	3
131	Noonmati PS	Gopal Nagar Location 2 Tinlai nr. SBI ATM (inside Rd)	26.19828	91.79958	2	0	2
132	Noonmati PS	State bank / ATM noonmati (market)	26.18228	91.80237	1	0	1
133	Noonmati PS	Noonmati High School Tinali	26.18228	91.79958	2	0	2
134	Noonmati PS	Sankar nagar path tinali	26.18274	91.79764	2	0	2
135	Noonmati PS	Ganesh mandir/ new guwahati	26.18372	91.7999	1	0	1
136	Noonmati PS	Jayanata Nagar Pump Tinali	26.18233	91.80042	3	0	3
137	Noonmati PS	Refinery petrol pump tinali	26.18152	91.80299	3	0	3
138	Noonmati PS	Oil trunk (IOCL) Kalbat Nr. Petrol Pump	26.18111	91.80443	1	0	1
139	Noonmati PS	2 No. Modhghoria Tinali	26.17844	91.81708	3	0	3
140	Noonmati PS	SBI ATM Madhghoria Petrol Pump	26.17905	91.81992	1	0	1
141	Noonmati PS	Forest gate Tinlai	26.17833	91.82385	3	0	3
142	Noonmati PS	Narengi Railway station kolang park end	26.18069	91.83317	1	0	1

S. No	PS/District	Locations	Latitude	Longitude	Fixed	PTZ	Total
143	Noonmati PS	Regunath High School Tinali	26.18081	91.84093	3	0	3
144	Noonmati PS	Birkuchi Binogi Tinali	26.17493	91.84447	3	0	3
145	Noonmati PS	Magazine point (nr. Shiv mandir)	26.1678	91.8271	1	0	1
146	Noonmati PS	Hanuman Mandir	26.183044	91.793085	2	0	2
147	Noonmati PS	Lakheswar baruah Road Point	26.83031	91.793871	2	0	2
148	Noonmati PS	Ntr. Kanandra Ply Wood	26.1829	91.794386	2	0	2
149	Noonmati PS	Nr. Brahma Kumari Rajyoga Education Center	26.182922	91.795163	2	0	2
150	Noonmati PS	Ganesh Mandir Road Tinali	26.182847	91.79597	3	0	3
151	Noonmati PS	Anil Ply & Glass House	26.182816	91.796888	2	0	2
152	Noonmati PS	Sankar Nagar Road-II	26.18271	91.797491	3	0	3
153	Noonmati PS	Shiva Nagar (Jupuri Basti)	26.182469	91.798534	3	0	3
154	Noonmati PS	Noonmati Sani Mandir Opp Noonmati High School	26.18259	91.79931	3	0	3
155	Noonmati PS	Nr. NICAB Coaching Institute	26.182297	91.800221	2	0	2
156	Noonmati PS	Noonmati Jmae Masjid Lane	26.182249	91.80063	3	0	3
157	Noonmati PS	Guwahati Refinery Link road	26.182203	91.80149	2	0	2
158	Noonmati PS	Nr. Shyam Gas Agency	26.182007	91.802048	2	0	2
159	Noonmati PS	Noonmati Point	26.18204	91.803153	3	0	3
160	Noonmati PS	Noonmati Hindi School, opp IOCL petrol pump	26.181334	91.803066	2	0	2
161	Noonmati PS	Amayapu path	26.173081	91.801765	2	0	2
162	Noonmati PS	Pub-Geetanagar road	26.173701	91.802288	2	0	2

S. No	PS/District	Locations	Latitude	Longitude	Fixed	PTZ	Total
163	Noonmati PS	Panipath	26.174831	91.802546	2	0	2
164	Noonmati PS	Haripar path	26.175377	91.802967	2	0	2
165	Noonmati PS	Gharmara satra path	26.176204	91.803305	1	0	1
166	Noonmati PS	Geetali path	26.176763	91.803394	2	0	2
167	Noonmati PS	Adarani path	26.177639	91.804008	2	0	2
168	Noonmati PS	B G point	26.178523	91.804246	3	0	3
169	Noonmati PS	Boro Chowk Mathgharia	26.179238	91.806192	3	0	3
170	Noonmati PS	Nr. Padma Residency	26.179082	91.807563	2	0	2
171	Noonmati PS	2 No. Mathgharia Durga puja field	26.178942	91.81114	3	0	3
172	Noonmati PS	Vidyalay path	26.178846	91.81321	1	0	1
173	Noonmati PS	Sugam Path Mathgharia	26.178656	91.815433	3	0	3
174	Noonmati PS	Lakhi Mandir Path	26.178948	91.8177597	3	0	3
175	Noonmati PS	Yahoo Motors, Mathgharia	26.178884	91.81802	2	0	2
176	Noonmati PS	Bapuji nagar road, mathgharia	26.178837	91.819116	2	0	2
177	Noonmati PS	Forest gate near thakuria's novelty	26.17839	91.823909	3	0	3
178	Noonmati PS	ASEB colony rd. forest gate	26.178442	91.824256	2	0	2
179	Noonmati PS	Yuba nagar path, forest gate	26.178312	91.824848	2	0	2
180	Noonmati PS	EG Nursing home nr. SBI	26.178641	91.827837	2	0	2
181	Noonmati PS	Narengi Tinali	26.178508	91.829236	6	0	6
182	Noonmati PS	Narengi Bazar Between narengi Tinali, L G tower	26.178932	91.830086	3	0	3
183	Noonmati PS	L G Tower	26.179352	91.830174	4	0	4
184	Noonmati PS	Narengi House Colony Gate	26.179562	91.830924	3	0	3
185	Noonmati PS	Mississippi Enterprise	26.180144	91.831445	3	0	3
186	Noonmati PS	SBI ATM Kalangpur Bazar	26.180795	91.833169	3	0	3
187	Noonmati PS	Kalangpar Bazar entyr to narengi station	26.181195	91.833572	3	0	3

S. No	PS/District	Locations	Latitude	Longitude	Fixed	PTZ	Total
188	Noonmati PS	Urmi Nagar path	26.181466	91.834568	3	0	3
189	Noonmati PS	Nr. Leela Automobiles bajaj service dealer	26.181707	91.834954	3	0	3
190	Noonmati PS	Brahmaputra Traders	26.181706	91.836024	3	0	3
191	Noonmati PS	Maria Public School narengi	26.182004	91.836639	3	0	3
192	Noonmati PS	Birkuchi Tinali	26.182877	91.838324	5	0	5
193	Pragjyotishpur PS	Pragjyotishpur (Chandrapur) PS	26.23321	91.83843	2	1	3
194	Pragjyotishpur PS	Bonda Anchalik School	26.18675	91.84357	2	0	2
195	Pragjyotishpur PS	Amchang Wild Life Tinali	26.18757	91.84432	1	0	1
196	Pragjyotishpur PS	PEWS Nursing Institute	26.19404	91.84807	1	0	1
197	Pragjyotishpur PS	Wedding Resort Boda Tinali	26.19963	91.85252	1	0	1
198	Pragjyotishpur PS	DIG Bunglow, Panikhaiti	26.2021	91.8554	1	0	1
199	Pragjyotishpur PS	Panikhaiti Out Post	26.20361	91.85831	4	1	5
200	Pragjyotishpur PS	Panikhaiti Rail Gate Bazar	26.20533	91.8599	2	0	2
201	Pragjyotishpur PS	Kali Mandir, Panikhaiti	26.2076	91.86214	1	0	1
202	Pragjyotishpur PS	Central Training Institute, Panikhaiti Tinali	26.20899	91.86517	3	0	3
203	Pragjyotishpur PS	Circle Officer Chariali Chandrapur	26.21387	91.87368	2	0	2
204	Pragjyotishpur PS	Nr. Hatisila Gate Tinali	26.21731	91.88585	1	0	1
205	Pragjyotishpur PS	Bharat Petrolim Fuel Station, Hajongbari (Nr. Exit Gate to cover	26.22653	91.9074	1	0	1
206	Pragjyotishpur PS	Tatimara, Chandrapur Tinali	26.23615	91.91626	1	0	1

S. No	PS/District	Locations	Latitude	Longitude	Fixed	PTZ	Total
207	Pragjyotishpur PS	Tatimara Tiniali Nr. Railway Turning	26.23572	91.92512	2	0	2
208	Pragjyotishpur PS	Chandra Bank Tiniali	26.23766	91.92868	2	0	2
209	Pragjyotishpur PS	Chandra B.D.O Office Tinialiank Tiniali	26.23938	91.93678	4	0	4
210	Pragjyotishpur PS	NTC Namghar, Chandrapur	26.2333	91.94117	1	0	1
211	Pragjyotishpur PS	ASEB Tiniali Chandrapur	26.23526	91.94383	1	0	1
212	Pragjyotishpur PS	Govardhan Market Chariali	26.2438	91.95934	2	0	2
213	Satgaon PS	Satgaon PS	N26°9'57.582"	E91°49'52.5576"	3	0	3
214	Satgaon PS	Panjabari tiniali traffic point	N26°7'57.504"	E91°50'2.5576"	4	0	4
215	Satgaon PS	GPS School tiniali Batahghuli	N26°7'56.91"	E91°50'44.2428"	1	0	1
216	Satgaon PS	Batahghuli Bogorital Tiniali	N26°7'58.5912"	E91°50'36.8124"	1	0	1
217	Satgaon PS	Batahghuli LP School at turning point	N26°8'0.5748"	E91°50'36.7224"	2	0	2
218	Satgaon PS	Nabajyoti Nagar tiniali	N26°7'52.4604"	E91°49'40.0944"	1	0	1
219	Satgaon PS	Bagharbari Tiniali	N26°8'1.392"	E91°49'28.1712"	1	0	1
220	Satgaon PS	Infront of Bagharbari Masjid	N26°8'41.028"	E91°49'40.062"	1	0	1
221	Satgaon PS	Satgaon Tiniali Chowk	N26°9'31.644"	E91°50'19.2876"	1	0	1
222	Satgaon PS	Panjabari bus stand	N26°8'1.77"	E91°50'1.1832"	1	0	1
223	Satgaon PS	Manisha pharmacy	N26°8'1.3632"	E91°50'0.114"	1	0	1
224	Satgaon PS	SBI ATM panjabari	N26°7'54.466"	E91°49'56.7228"	1	0	1
225	Satgaon PS	Kailash nagar road	N26°7'58.1584"	E91°44'44.2132"	1	0	1
226	Satgaon PS	SBI /wine shop	N26°7'58.8396"	E91°49'46.3584"	1	0	1
227	Satgaon PS	Abhinandan vivah bhawan	N26°7'58.6992"	E91°44'41.0736"	1	0	1



S. No	PS/District	Locations	Latitude	Longitude	Fixed	PTZ	Total
228	Satgaon PS	DM Enterprise	N26°7'58.1376"	E91°44'37.2108"	1	0	1
229	Satgaon PS	Naba jyoti nagar	N26°7'5781"	E91°49'35.8212"	1	0	1
230	Satgaon PS	Yuba sangha	N26°7'57.9648"	E91°44'35.6664"	1	0	1
231	Satgaon PS	Electricity power house (side)	N26°7'59.6748"	E91°49'31.6416"	1	0	1
232	Satgaon PS	Baghorbori	N26°8'1.0032"	E91°49'29.4564"	1	0	1
233	Satgaon PS	Baghorbori near bus stop	N26°8'0.7152"	E91°49'30.6876"	1	0	1
234	Satgaon PS	Golden Tower (Complex)	N26°7'59.7036"	E91°49'32.358"	1	0	1
235	Satgaon PS	HDFC Atm	N26°7'59.1708"	E91°49'33.4308"	1	0	1
236	Satgaon PS	Mango line	N26°8'0.654"	E91°44'58.5984"	1	0	1
237	Satgaon PS	Panjabari bus stop (Left side)	N26°8'0.744"	E91°49'58.7244"	1	0	1
238	Satgaon PS	Baily trailor	N26°7'59.6568"	E91°49'52.9212"	1	0	1
239	Satgaon PS	Hill top road	N26°7'59.6748"	E91°49'52.6656"	1	0	1
240	Satgaon PS	Kalita enterprise	N26°7'59.6784"	E91°49'49.9728"	1	0	1
241	Satgaon PS	Binita jewelry	N26°7'59.772"	E91°49'48.9792"	1	0	1
242	Satgaon PS	Namghor path	N26°8'20.7456"	E91°46'47.1072"	1	0	1
243	Satgaon PS	Opp. Wine shop	N26°7'59.286"	E91°49'39.4608"	1	0	1
244	Satgaon PS	Psychotic hospital	N26°7'59.1708"	E91°49'33.438"	1	0	1
245	Satgaon PS	Opp. Kailash nagar	N26°7'58.9584"	E91°49'49.2132"	1	0	1
246	Satgaon PS	Opp. Abhinandan vivah bhawan	N26°7'58.6992"	E91°49'41.0736"	1	0	1

		<b>Total</b>			<b>549</b>	<b>20</b>	<b>569</b>
--	--	--------------	--	--	------------	-----------	------------

#### D. BUS STOPS

S No.	Route	Location	Camera QTY
1	Adabari-Khanapara	ABC Opp Dona Planet	2
2	Adabari-Khanapara	Apsara	2
3	Adabari-Khanapara	Bharalumukh (near Police Stn)	2
4	Adabari-Khanapara	Bhoot Nath - Near GMC Office	2
5	Adabari-Khanapara	Christianbasti	2
6	Adabari-Khanapara	Dairy Gate	2
7	Adabari-Khanapara	Dighalipukhari - Near Kubersthan	2
8	Adabari-Khanapara	Fancy Bazar - Mahabir Uddayn (RCC & Steel)	2
9	Adabari-Khanapara	Hub (to be shifted a bit)	2
10	Adabari-Khanapara	In front of Pantaloons	2
11	Adabari-Khanapara	Kamakhya Gate (nursery)	2
12	Adabari-Khanapara	Kar Bhawan	2
13	Adabari-Khanapara	Khanapara Bus Stop	2
14	Adabari-Khanapara	Lachit Nagar	2
15	Adabari-Khanapara	Machhkhowa (RCC)	2
16	Adabari-Khanapara	Maligaon Chariali	2
17	Adabari-Khanapara	Opp. Vishal (50 Mtrs shed towards paltan Bazar)	2
18	Adabari-Khanapara	Paltanbazar - Near Krishnashree Point	2
19	Adabari-Khanapara	Panbazar - Neharu Park Kachhari	2
20	Adabari-Khanapara	Railay Gate no3	2
21	Adabari-Khanapara	Railway St. Near Scout & Guide Off	2
22	Adabari-Khanapara	Rukminigaon	2
23	Adabari-Khanapara	Six Mile Flyover (near Directorate of Agriculture)	2
24	Adabari-Khanapara	Super Market	2
25	Adabari-Khanapara	Wallford	2
26	Khanapara-Adabari	ABC Opp Dona Planet	2
27	Khanapara-Adabari	Apsara	2
28	Khanapara-Adabari	Bharalumukh State Bank	2
29	Khanapara-Adabari	Bhoot Nath - Near GMC Office	2
30	Khanapara-Adabari	Christianbasti	2
31	Khanapara-Adabari	Dairy Gate	2
32	Khanapara-Adabari	Himatsingka etrol Pump	2
33	Khanapara-Adabari	Hub (to be shifted a bit)	2
34	Khanapara-Adabari	Infront of Pantaloons	2
35	Khanapara-Adabari	Kamakhya Gate (nursery)	2
36	Khanapara-Adabari	Khanapara Bus Stop	2
37	Khanapara-Adabari	Lachit Nagar	2
38	Khanapara-Adabari	Maligaon Chariali	2
39	Khanapara-Adabari	Opp. Kar Bhawan Ganeshguri	2
40	Khanapara-Adabari	Paltanbazar Nepali mandir (near meghdoot Cinema)	2
41	Khanapara-Adabari	Railay Gate no3	2
42	Khanapara-Adabari	Rukminigaon	2

S No.	Route	Location	Camera QTY
43	Khanapara-Adabari	Six Mile Flyover (near Directorate of Agriculture)	2
44	Khanapara-Adabari	Super Market	2
45	Khanapara-Adabari	Wallford	2
46	Bashistha-Adabari	Basistha Chariali	2
47	Bashistha-Adabari	Basistha Temple	2
48	Bashistha-Adabari	Beltola Tinali	2
49	Bashistha-Adabari	Bharalumukh State Bank	2
50	Bashistha-Adabari	Himatsingka etrol Pump	2
51	Bashistha-Adabari	Lakhi Mandir	2
52	Bashistha-Adabari	Last Gate	2
53	Bashistha-Adabari	Paltanbazar Nepali mandir (near meghdoot Cinema)	2
54	Bashistha-Adabari	Survey	2
55	Bashistha-Adabari	Wholesale Market Ganeshguri	2
56	Bashistha-Adabari	Wireless BSNL	2
57	Adabari-Bashistha	Basistha Chariali	2
58	Adabari-Bashistha	Basistha Temple	2
59	Adabari-Bashistha	Beltola Tinali	2
60	Adabari-Bashistha	Bharalumukh (near Police Stn)	2
61	Adabari-Bashistha	Dighalipukhari - Near Kubersthan	2
62	Adabari-Bashistha	Fancy Bazar - Mahabir Uddayn (RCC & Steel)	2
63	Adabari-Bashistha	Lakhi mandir	2
64	Adabari-Bashistha	Last Gate	2
65	Adabari-Bashistha	Machhkhowa (RCC)	2
66	Adabari-Bashistha	Opp. Vishal (50 Mtrs shed towards paltan Bazar)	2
67	Adabari-Bashistha	Paltanbazar - Near Krishnashree Point	2
68	Adabari-Bashistha	Panbazar - Neharu Park Kachhari	2
69	Adabari-Bashistha	Railway St. Near Scout & Guide Off	2
70	Adabari-Bashistha	Survey	2
71	Adabari-Bashistha	Wireless BSNL	2
72	Gorchuk -Fatasil	Janki Sweets	2
73	Gorchuk -Fatasil	Katahbari Tinali Near Kk Fashion	2
74	Gorchuk -Fatasil	Milan Nager Path In Front Of Royal Timber	2
75	Gorchuk -Fatasil	Adjacent to Shyam Traders Manpara Near Godown	2
76	Gorchuk -Fatasil	Opp. Ashoka Trade Centre	2
77	Gorchuk -Fatasil	Maternity & Child Welfare, Infront Of Nabajagaram Medicos	2
78	Gorchuk -Fatasil	Dhirenpara Tila Towards Barsapara Stadium	2
79	Gorchuk -Fatasil	Ambari Tinali Durga Mandir	2
80	Gorchuk -Fatasil	Infront Of Soap Factory	2

S No.	Route	Location	Camera QTY
81	Gorchuk -Fatasil	Rgb College	2
82	Gorchuk -Fatasil	Gmc Colony Fatashil	2
83	Fatashil -Gorchuk	Gmc Colony Fatashil	2
84	Fatashil -Gorchuk	Phoolbagan, Rgb College	2
85	Fatashil -Gorchuk	Amabari Tiniali, In Fornt Of Ambari Nabajyog Edding Wall	2
86	Fatashil -Gorchuk	Santu Store, Shirenpara	2
87	Fatashil -Gorchuk	Shoe Staore	2
88	Fatashil -Gorchuk	In Fornt Bhogali Resturants	2
89	Fatashil -Gorchuk	Ganeshpara Shiv Mandir	2
90	Fatashil -Gorchuk	Fatashil Ganeshpara Milan Jyoti Sangha Field	2
91	Fatashil -Gorchuk	Opp. Indian Oil Petrol Pump [	2
92	Fatashil -Gorchuk	Maa Kali Sweets In Fornt Of Afreen Store	2
93	Panjabari-Left	National Seed Corporation	2
94	Panjabari-Left	Near Jilika Path, Near Kalakshetra	2
95	Panjabari-Left	Near /s BD Enterprise	2
96	Panjabari-Right	Opposite ango Lane (R)	2
97	Panjabari-Right	Lions Club (R), RCC	2
98	Panjabari-Right	In front of BSNL (BDO) (R)	2
99	athgharia-Zoo Road Tinali	Before Gurukul Graar School	2
100	athgharia-Zoo Road Tinali	Hatgarh Chariali	2
101	Zoo Road Tinali - athgaria	Hatgarh Chariali	2
102	Zoo Road Tinali - athgaria	athgharia Flyover Turning	2
103	VIP Road - Sixile - Satgaon	Sixile	2
104	VIP Road - Sixile - Satgaon	Chandannagar	2
105	VIP Road - Sixile - Satgaon	Near Barbari Chariali	2
106	VIP Road - Sixile - Satgaon	In front of Pratiksha	2
107	VIP Road - Sixile - Satgaon	Near KR Apartent	2
108	VIP Road - Sixile - Satgaon	Near Sagarika Bibah Bhawan	2
109	Satgaon-Sixile	Satgaon	2
110	Satgaon-Sixile	Near Kaakhya car shop	2
111	Satgaon-Sixile	Barbari Chariali	2
112	Satgaon-Sixile	Chandan Nagar	2
113	Satgaon-Sixile	Sixile	2
114	Ganesh andir-Lalganesh	Opposite Guest House	2

S No.	Route	Location	Camera QTY
115	Ganesh andir-Lalganesh	In front of DPI (Tea Stall)	2
116	Ganesh andir-Lalganesh	Forensic Lab	2
117	Ganesh andir-Lalganesh	Near Narakasur L.P. School	2
118	Ganesh andir-Lalganesh	Bhagaduttapur	2
119	Ganesh andir-Lalganesh	Opposite Office of anager APDCL	2
120	Ganesh andir-Lalganesh	Near Vivekananda	2
121	Lalganesh-Ganesh andir	Lalganesh andir (R)	2
122	Lalganesh-Ganesh andir	Opp. Divine Enterprise, near 4th APBN (R)	2
123	Lalganesh-Ganesh andir	100 ahead of SS (R)	2
124	Lalganesh-Ganesh andir	Opp. Haiku (R)	2
125	Lokhara - Lalganesh	Near BOI Lokhra infront of Saloon	2
126	Lokhara - Lalganesh	Saukuchi Tinali Opp. Hocky Stadiu	2
127	Lokhara - Lalganesh	Opp. Shiv andir	2
128	Lokhara - Lalganesh	Hill View Road after Crossing	2
129	Lokhara - Lalganesh	Lalganesh Point, Central Bank	2
130	Lokhara - Lalganesh	eena Buad, Infront of Battalion Gate	2
131	Lokhara - Lalganesh	Borthakur Sevashra, Colony Bazar	2
132	Lokhara - Lalganesh	Infront if Forest Office	2
133	Lokhara - Lalganesh	Near U turn Birubari Tinali	2
134	Lokhara - Lalganesh	Tiber Shop	2
135	Lalganesh-Lokhara	Infront of Affinity near Nepali andir	2
136	Lalganesh-Lokhara	Purbachal Udyog Bikash	2
137	Lalganesh-Lokhara	Existing Ghuti Opp. Arya Boys Hostel	2
138	Lalganesh-Lokhara	Near B. Baruah Cancer Hospital Opp. ITI Entrance under tree	2
139	Lalganesh-Lokhara	Opp. D.P. Hardware	2
140	Lalganesh-Lokhara	Lalganesh Point, Alcare	2
141	Lalganesh-Lokhara	Hill View Road after Crossing Near asjid	2
142	Lalganesh-Lokhara	Next to Bharat Petroliu Pup	2
143	Lalganesh-Lokhara	Saukuchi Tinali	2
144	Lalganesh-Lokhara	J. Barua edicos Opp.	2
145	Lalganesh-Lokhara	Total BQS	2

S No.	Route	Location	Camera QTY
		<b>TOTAL</b>	<b>290</b>

## 12.2 Locations for Traffic Junctions & ITMS

S.No.	Junction Names	RLVD Camera QTY	ANPR cameras QTY	Total Camera
1	ABC Point, GS Road	3	6	9
2	Srinagar Point	3	6	9
3	Ganeshguri Fly Over	4	8	12
4	Downtown Point	3	6	9
5	VIP Road Point	3	6	9
6	Six-mile underbridge	4	8	12
7	Prison Gate	3	6	9
8	Khanapara Flyover	5	10	15
9	Koinadhora Point	3	6	9
10	Basistha Chariali	4	8	12
11	Beharbari	4	8	12
12	Rangmon Point	3	6	9
13	Science Museum Point	4	8	12
14	Jaya Nagar Point	4	8	12
15	Beltola Point	4	8	12
16	Survey Point	3	6	9
17	Lakhimi Nagar	4	8	12
18	Hatigaon Chariali	4	8	12
19	Bhetapara Chariali	4	8	12
20	Ghoramara Chariali	4	8	12
21	Zoo Point	3	6	9
22	Barbabri Point	3	6	9
23	Bhangagarh Bridge	4	8	12
24	In front of Birubari Cancer Hospital	3	6	9
25	High Court Point	3	6	9
26	Panbazar PAPA Point	4	8	12
27	Planetarium Point	4	8	12
28	Rabindra Bhawan	3	6	9
29	Rail Gate No. 3 (AT Road)	3	6	9
30	Sarabbhati Point	4	8	12
31	Ulubari Flyover	5	10	15
32	Water Supply Point	3	6	9

S.No.	Junction Names	RLVD Camera QTY	ANPR cameras QTY	Total Camera
33	GCC Point	3	6	9
34	Noonmati Point	3	6	9
35	Patharquarry Point	3	6	9
36	Narengi Point	3	6	9
37	Hatigarh Chariali	4	8	12
38	Zoo Road Tinali Point	3	6	9
39	Chandmari Point	3	6	9
40	Silpukhuri	4	8	12
41	Guwahtai College Point	3	6	9
42	BG Tinali, Mathgharia	3	6	9
43	SOS Point	3	6	9
44	VIP Main Chowk	4	8	12
45	Rani Chowk	3	6	9
46	Dharapur	3	6	9
47	Satmile (University bypass)	3	6	9
48	Garchuk Chariali	4	8	12
49	Lokhara Chariali	4	8	12
50	BhupenHazarika Samadhi Kshetra	4	8	12
51	Adabari Bus Stand	3	6	9
52	Maligaon Chariali	4	8	12
53	Maligaon Gate No. 3	3	6	9
54	Bharalumukh Railgate side	4	8	12
55	Machkhowa Point	3	6	9
56	6 No. Gate, AT Road	4	8	12
57	Fatasil Point	4	8	12
58	Chabipool Point	4	8	12
59	Kumarpara Pachali	5	10	15
60	Lalganesh Point	3	6	9
61	Barsapara Point	3	6	9
62	Cycle Factory	4	8	12
63	Boragaon Chariali	4	8	12
64	Guwahati Club Point	3	6	9
<b>Total</b>		<b>226</b>	<b>452</b>	<b>678</b>

### 12.3 Locations for SVD

S. No.	Locations Details	Camera QTY
1	Airport Road – (One Location)	4
2	Bypass Road - Between Khanapara – Jalukbari (Two Locations)	8
		<b>12</b>

### 12.4 Locations for Police Stations – Under the Police Commissionerate Guwahati

S. No	Name of District	PS Name	Latitude	Longitude
1	Guwahati Central	ALL WOMEN	26.1586944	91.7635072
2	Guwahati Central	CHANDMARI	26.185.187	91.770.979
3	Guwahati Central	GEETA NAGAR	26.172.698	91.786.968.
4	Guwahati Central	LATASIL	26°11'23"N	91°45'8"E
5	Guwahati Central	NOONMATI	26.1838250	91.8031030
6	Guwahati Central	PALTAN BAZAR	25°10'52"N	91°45'4"E
7	Guwahati Central	PANBAZAR	26°11'7"N	91°44'28"E
8	Guwahati Central	PRAGJYOTI SHPUR	26.2331291	91.9378579
9	Guwahati Central	SACHAL/ SATGAON	26.16624	91.8310411
10	Guwahati East	BASISTHA	26°6'44"N	91°47'42"E
11	Guwahati East	BHANGAGARH	26.9'37	91.46'4'
12	Guwahati East	DISPUR	26.14347	91.79208
13	Guwahati East	HATIGAON	26°7'36"N	91°47'13"E
14	Guwahati East	KHETRI	26.11425	92.08222
15	Guwahati East	SONAPUR	26.117006	91.970110
16	Guwahati West	AZARA	26°06.987'N	91°36.869' E
17	Guwahati West	BHARALUMUKH	26.17297	91.72982
18	Guwahati West	FATASIL AMBARI	26.15966	91.73915
19	Guwahati West	GORCHUK	26°6'58.698" N	91°42'35.958"E
20	Guwahati West	JALUKBARI	26.1595	91.69607

### 12.5 Locations for Integrated Command & Control Center (ICCC)

#### A. Temporary Locations of ICCC



BSNL Bhawan  
 5<sup>th</sup> Floor, Administrative Building  
 Cotton Road, Pan Bazar,  
 Guwahati - 781001

## B. Permananet Locations of ICCC

A piece of land has been identified near Panjabari, Guwahati & GSCL will construct the G+4 building within 24 Months. SYSTEM INTEGRATOR shall be required to shift all installation from the temporary space to the Permanent space and resume ICCC services as per agreed timeline.

### 12.6 Tentative POP Site Locations

(This is indicative only – Bidder may select POP Locations and QTY as per NW design)

S. No.	PoP Locations (Smart City)	Dark Fibre / Green OFC
		(Primary)
1	Bamunimaidan, AMTRON	Available
2	Narangi, APGCL Office	Available
3	Sachal	Available
4	Zoo Road, Assam State Zoo	Available
5	Bhangagarh, GMCH	Available
6	Barshapara, Cricket Stadium	Available
7	Guwahati Club, TC Girls School	Available
8	Fancy Bazar, PWD	Available
9	Rehabari, Directorate of Employment	Available
10	Lokhra, Sarusajai Sports Complex	Available
11	Baisistha Chariali, Game Village	Available
12	Khanapara, IAS Colony	Available
13	Panjabari, Aranya Bhaban	Available
14	Kahilipara	Available
15	Maligaon Chariali	Available
16	Jalukbari, Assam Forest School	Available
17	Amingaon, ASWAN PoP	Available
18	North Guwahati PoP	Available
19	Azara, ASWAN PoP	Available
20	Bongora, Tech City	Available
21	Bethkuchi, ISBT	Available

S. No.	PoP Locations (Smart City)	Dark Fibre / Green OFC
		(Primary)
22	Panikhati, ASWAN PoP	Available
23	Sonapur, ASWAN PoP	Available

## 12.7 Bill of Material (BOM) Summary

(To be submitted with bid offer)

S. No.	Description of Item	UOM	Tender QTY	Make	Model
A	B	C	D		
	<b>Price shall be included the Supply, Storage, Installation Testing &amp; Commissioning &amp; final user acceptance testing</b>				
<b>1.0</b>	<b>Integrated Traffic Control System</b>				
<b>1.1</b>	<b>Traffic Violation Detection System at Traffic Junctions</b>				
<b>1.1.1</b>	ANPR Camera with accessories & required analytics SW	Nos	452		
<b>1.1.2</b>	RLVD Camera with accessories & required analytics SW	Nos	226		
<b>1.1.3</b>	Sped Violation Detection System, Including the complete solutions - a) 9MP IP Camera, b) 4D tracking Radar, c) Local Processing Unit, d) LED Flash, e)Software License Lifetime use fee, f) Junction Box with Network, Power Component, Cables, accessories, and installations	Nos	6		
<b>1.1.4</b>	Vehicle Activated Radar Speed Signs - Highway Variable Display Board 1x1meter, 3 color display (red, green, and amber)	Nos	12		
<b>1.1.5</b>	Gantry 10-meter width & 6-meter Hight For Highway SVD System	Nos	6		
<b>1.1.6</b>	Junction Box / Control Unit Cabinet for ANPR & RLVD: including AC Power supply and UPS, CPU Sub Module, with all cabling, fittings, earthing , lighting arrester etc.	Nos	131		

S. No.	Description of Item	UOM	Tender QTY	Make	Model
1.1.7	Junction Box / Control Unit Cabinet for SVD Camera: including AC Power supply and CPU Sub Module, with all cabling, fittings, earthing , lighting arrester etc.	Nos	6		
1.1.8	Industrial Grade Outdoor - L2-PoE switches - 8 Port +4 SFP (Only for ITMS)	Nos	131		
1.1.9	Industrial Grade Outdoor - L2-PoE switches - 08 Port +4 SFP (Only for SVD)	Nos	6		
1.1.10	UPS with Battery (appropriate Backup per technical specification and SLA mentioned in volume II of this RFP)	Nos	137		
1.1.11	10 Mtrs Gantry System/Cantilever Pole - ANPR & RLVD	Nos	226		
1.1.13	ANPR Analytics Software License with No Helmet, Triple Ride of 2-wheeler, No Seatbelt, Driver talking on Phone, Free left Blocking while driving with ANPR.	Nos	452		
1.1.14	RLVD Analytics Software License	Nos	226		
1.1.15	Complete cabling and civil works as required - No of Pole (ANPR, RLVD)	Nos	131		
1.2.	<b>Adaptive Traffic Signal Control System (Signalization)</b>				
1.2.1	ATCS Traffic Controller	Nos	64		
1.2.2	Countdown timer	Nos	226		
1.2.3	Vehicle Detection System	Nos	226		
1.2.4	Galvanized standard Poles for Traffic Aspects and Pedestrian signals	Nos	452		
1.2.5	Galvanized Cantilevers for Traffic Aspects and Pedestrian signals	Nos	226		
1.2.6	Traffic Light Aspects – Red	Nos	452		
1.2.7	Traffic Light Aspects – Amber	Nos	452		
1.2.8	Traffic Light Aspects – Green	Nos	1356		
1.2.9	Pedestrian lamp heads – Stop Man	Nos	226		
1.2.10	Pedestrian lamp heads – Walk Man	Nos	226		
1.2.11	Supply & Laying of Cabling , junction box installation , earthing , conduiting , trenching , digging of road , etc	Nos	64		
1.2.12	ATCS Centralize Software	Lot	1		
1.2.14	Off Line Simulation Solution	Lot	1		
1.2.13	ATCS System Design , Commissioning & Training Charges	Lump-Sum	1		

S. No.	Description of Item	UOM	Tender QTY	Make	Model
1.2.16	Command Centre Integration	Nos	1		
1.3	<b>E-Challan System for ITMS</b>				
1.3.1	E-Challan Hand held devices (terminal) with E-Challan s/w for Handheld along with 3G/4G (or above) enabled SIM Cards	Nos	64		
1.3.2	E-Challan MASTER Software	Nos	1		
1.4	<b>Additional Requirements</b>				
1.4.1	Any other Hardware or Software required to meet the RFP requirements (Bidder to list individual items and provide costing)	LS	1		
2.0	<b>City Surveillance System</b>				
2.1	<b>CCTV Camera at different location in the city</b>				
2.1.1	Indoor Dome Camera	Nos	23		
2.1.2	Outdoor Bullet /Fixed Camera	Nos	1423		
2.1.3	Outdoor PTZ Camera	Nos	160		
2.1.4	Poles for CCTV Cameras with Accessories	Nos	638		
2.1.5	Junction Box / Control Unit Cabinet for CCTV: including AC Power supply with all cabling, fittings, earthing, lighting arrester , etc.	Nos	757		
2.1.6	Industrial Grade Outdoor - L2-PoE switches - 4 Port +2 SFP	Nos	757		
2.1.7	UPS with Battery (appropriate Backup per technical specification and SLA mentioned in volume II of this RFP)	Nos	757		
2.1.8	VMS Software with all Camera License	Nos	1		
2.1.10	Digging, Piping & Re-filling, including digging for electrical cabling - All camera locations	LS	757		
2.2	<b>Additional Requirements</b>				
2.2.1	Any other Hardware or Software required to meet the RFP requirements (Bidder to list individual items and provide costing)	LS	1		
3.0	<b>OFC - Network</b>				
3.1	<b>Optical Transmission Equipment's for POP Sites</b>				
3.1.1	Core Router - with 1Gbps, 10km Transceivers - 16, 10Gbps, 10km Transceivers -16, 10Gbps, 40km Transceivers- 4, 40Gbps, 10km Transceivers -8, 40Gbps, 40km Transceivers -02, 40Gbps Cables/Transceivers (Multimode) -04	Nos	2		

S. No.	Description of Item	UOM	Tender QTY	Make	Model
3.1.2	DWDM/OTN Base Equipment (Min 2x100G (Line OTU4) + min 20x10G interfaces with Redundant PSU and Redundant Fabric Crossconnect , accessories and Patch cords)without CFP/ XFP/SFP	Nos	25		
3.1.3	Optical, CFP, 100GBase-ER4, OTU4, 100G to support 40 km	Nos	50		
3.1.4	Optical, SFP+, 10GBASE-LR/LW, STM64, 9.95Gbps to 11.3Gbps to support 10Km with required patch cord	Nos	250		
3.1.5	Server Hardware( Include Server/ Switch/Rack or any other hardware to manage the Network)	Set	1		
3.1.6	NMS Software for DWDM/OTN	Nos	1		
3.1.7	Switch with 24 Port SFP GigE and 4 x 1/10G SFP+ with Redundant AC PSU and Layer2+ Software and Installation Kit/Power cable)	Nos	23		
3.1.8	Optical, SFP, 1000BASE-LX, 1.25Gbps, 1310nm to support 10 km with required patch cord	Nos	552		
3.1.9	Optical, SFP+, 10GBASE-LR/LW, STM64, 9.95Gbps to 11.3Gbps to support 10Km with required patch cord	Nos	46		
3.1.10	Overhead OFC Deployment Cost (Including OFC, Pole, RM, JC Closure & Fixture)	Kms	150		
3.1.11	Underground OFC Deployment Cost (Including OFC, HDPE Ducts, Couplers, RM, Chambers JC Closures)	Kms	200		
3.1.12	36U Racks for Tx Equipment's	Nos	23		
3.1.13	FDMS/LIU Equipment	Nos	23		
3.1.14	Patch Cord - 3 Meters (OFC)	Nos	92		
3.1.15	UTP Cat 6 Armoured Cable (As per Bidder's Solution)	LS (Box)	5		
3.2	<b>Additional Requirements</b>				
3.2.1	Any other Hardware or Software required to meet the RFP requirements (Bidder to list individual items and provide costing)	LS	1		
4.0	<b>Wireless RF Connectivity</b>				

S. No.	Description of Item	UOM	Tender QTY	Make	Model
<b>4.1</b>	<b>RF Connectivity - for ITMS Crossing</b>				
<b>4.1.1</b>	RF connectivity at all ITMS crossing with complete solutions - 50 Mbps- Including Tower, Pole, BTS, CPE, Power Backup -- (64-ITMS Crossing)	Nos	64		
<b>4.2</b>	<b>Additional Requirements</b>				
<b>4.2.1</b>	Any other Hardware or Software required to meet the RFP requirements (Bidder to list individual items and provide costing)	LS	1		
<b>5.0</b>	<b>Integrated Command and Control Centre (ICCC)</b>				
<b>5.1</b>	<b>Video Wall System</b>				
<b>5.1.1</b>	Video Wall Cubes for - Wall size 6.5 x 2.5 Meter - with complete stand and accessories	Nos	1		
<b>5.1.2</b>	Video Wall Controller with Wall Management System	Nos	1		
<b>5.2</b>	<b>ICT Equipment in ICCC</b>				
<b>5.2.1</b>	Multi-Function Laser Printer (City Control Room)	Nos	2		
<b>5.2.2</b>	Operator Workstations with Triple Monitor (City Control Room)	Nos	15		
<b>5.2.3</b>	IP PABX System	Nos	1		
<b>5.2.4</b>	IP Phones	Nos	15		
<b>5.2.5</b>	Office Desktop	Nos	5		
<b>5.2.6</b>	KVM Switches - 4 Port USB/HDMI	Nos	10		
<b>5.2.7</b>	PRI Modem	Nos	1		
<b>5.3</b>	<b>Network , ICCC Platform and Switching Devices</b>				
<b>5.3.1</b>	Switches - Core	Nos	2		
<b>5.3.2</b>	Internet Router (L-3)	Nos	1		
<b>5.3.3</b>	Networking/ IT racks - 42 U	Nos	4		
<b>5.3.4</b>	UTM for 50 concurrent users	Nos	2		
<b>5.3.5</b>	Supply of ICCC Application Software Integration with Operator Console, Integration of Video Management Software all CCTV Camera with 4 Analytics (min), Integration of ITMS (ATCS, ANPR, RLVD, SVDS, e-Challan), SMS Gateway Integration , Email Gateway Integration, Integration with EMS / NMS, Integration with Video Wall at Command Centre, Integration of City GIS, and other services related to this RFP.	Nos	1		
<b>5.4</b>	<b>Building Utilities for ICCC</b>				

S. No.	Description of Item	UOM	Tender QTY	Make	Model
5.4.1	DG Set - 75 KVA with AMF Panel with Change-over Switch	Nos	1		
5.4.2	UPS with battery backup - 50 KVA	Nos	1		
5.4.3	Electrical and Power Cabling work in ICCC	LS	1		
5.4.4	Electrical Cabling & Necessary illumination devices	LS	1		
5.4.5	LAN and CAT-6 cabling	LS	1		
5.4.6	Fire & Smoke Detection System	Nos	1		
5.4.7	Fixed Dome Cameras with 32	Nos	6		
5.5	<b>Civil Works, Floor &amp; Interior Work</b>				
5.5.1	Civil Work - False-Ceiling, Raised flooring in Server Room, etc.	SQF	5000		
5.5.2	Floor Carpet	SQF	5000		
5.5.3	Painting	SQF	20000		
5.5.4	HVAC System for Video Monitoring Room (20 TR)	Nos	1		
5.5.5	Ductable Split AC (10 TR) for Equipment Room & Meeting Rooms	Nos	1		
5.5.6	Furniture (Work Stations - Desk and Chairs) for ICCC - 15 Seater	Nos	15		
5.5.7	Furniture (Work Stations - Desk, Chairs) for ICCC Operation Manager Cabin	Nos	4		
5.5.8	Furniture for Meeting Rooms (6-Seats x 2 Nos)	Nos	2		
5.5.9	Furniture for Security Desk /Guard Room	Nos	1		
5.5.10	Furniture for Help Desk - 5 Seater	Nos	5		
5.6	<b>Additional Requirements</b>				
5.6.1	Any other Hardware or Software required to meet the RFP requirements (Bidder to list individual items and provide costing)	LS	1		
7.0	<b>Data Centre (Hosted at State Data Centre)</b>				
7.1	<b>Servers, Switches &amp; Application SW</b>				
7.1.1	Data Centre Spine Switch (Core)	Nos	2		
7.1.2	Data Centre Leaf Switch (Aggregate)	Nos	4		
7.1.3	Data Centre Out of Band Switch	Nos	4		
7.1.4	GIS Enterprise Software	Nos	1		
7.2	<b>Storage &amp; Other Components</b>				
7.2.1	Primary Storage (3 PB) - 30 Days	Nos	1		
7.2.2	Secondary Storage (5 PB) / Compressed Form - 90 Days	Nos	1		

S. No.	Description of Item	UOM	Tender QTY	Make	Model
7.2.3	Hyper Converged Infrastructure (HCI)	Set (As per design)	12		
7.2.4	Internet Firewall with IPS	Nos	2		
7.2.5	Nest Generation Firewall (NGFW) with Anti APT	Nos	2		
7.2.6	Server Load Balancer with Web application Firewall	Nos	2		
7.2.7	Security Information & Event Management (SIEM) System	Nos	1		
7.2.8	Authentication, Authorization and Accounting – Network Access Control (AAA – NAC)	Nos	1		
7.2.9	Network Management System (NMS)/ Enterprise Management System - EMS	Nos	1		
7.2.10	End Host Antivirus	Nos	1		
7.3	<b>Additional Requirement</b>				
7.3.1	Any other Hardware or Software required to meet the RFP requirements (Bidder to list individual items and provide costing).	LS	1		