



REQUEST FOR PROPOSAL

For

**Selection of Master System Integrator for
Implementation of Integrated Smart Solutions at
Patna**

NIT No: 05/MD/PSCL/2020-21

Dated 16/04/2021

INTERNATIONAL COMPETITIVE BIDDING

Volume II: Scope of Work

PATNA SMART CITY LIMITED

ADDRESS: 5th Floor, Biscomaun Tower, Patna, Bihar

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 Patna Smart City Limited (henceforth referred to as "PSCL" 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 PSCL 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 (MD), PSCL 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 or 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. PSCL accepts no responsibility for the accuracy or otherwise for any interpretation of opinion on law expressed herein. PSCL 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. PSCL 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. PSCL 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 PSCL is bound to select a Bidder or to appoint the Selected Bidder (as defined hereinafter), for implementation and PSCL 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 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 PSCL or any other costs incurred in connection with or relating to its Bid. All such costs and expenses will remain with the Bidder and PSCL 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 or any other costs incurred in connection with or relating to its Bid. All such costs and expenses will remain with the Bidder and PSCL 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.

Definitions/Acronyms

ACRONYMS	MEANING
ABD	AREA BASED DEVELOPMENT
ACD	AUTOMATIC CALL DISTRIBUTION
AMC	ANNUAL MAINTENANCE CONTRACT
ANI	ASIAN NEWS INTERNATIONAL
ANPR	AUTOMATIC NUMBER PLATE RECOGNITION
API	APPLICATION PROGRAM INTERFACE
AQI	AIR QUALITY INDEX
ARP	ADDRESS RESOLUTION PROTOCOL
ATCS	ADAPTIVE TRAFFIC CONTROL SYSTEM
ATM	AUTOMATED TELLER MACHINE
BMS	BUSINESS MANAGEMENT SYSTEM
BoM	BILL OF MATERIAL
CCC	CIRCUIT CROSS-CONNECT
CCTV	CLOSED CIRCUIT TELEVISION
CMM	CAPABILITY MATURITY MODEL
COTS	COMMERCIAL OFF-THE-SHELF
CSP	CLOUD SERVICE PROVIDER
CSV	COMMA SEPARATED VALUES
CTI	COMPUTER TELEPHONY INTEGRATION
DAM	Database Access Monitoring
DBMS	DATA BASE MANAGEMENT SYSTEM
DC	DATA CENTRE
DHCP	DYNAMIC HOST CONFIGURATION PROTOCOL
DMS	DOCUMENT MANAGEMENT SYSTEM
DMZ	DEMILITARIZED ZONE
DNIS	DIALED NUMBER IDENTIFICATION SERVICE
DNS	DOMAIN NAME SERVER
DOC	DOCUMENT
DoS	DENIAL OF SERVICE
DR	DISASTER RECOVERY
DRC	DISASTER RECOVERY CENTRE
DTMF	DUAL-TONE MULTI-FREQUENCY SIGNALLING
ECB	EMERGENCY CALL BOX
EMD	EARNEST MONEY DEPOSIT
EMS	ENTERPRISE MANAGEMENT SYSTEM
EPBAX	ELECTRONIC PRIVATE AUTOMATIC BRANCH EXCHANGE
ER	EQUIVALENT RELATIONAL
FAT	FINAL ACCEPTANCE TEST
FCC	FEDERAL COMMUNICATIONS COMMISSION
FMS	FACILITY MANAGEMENT SERVICES
FRS	FUNCTIONAL REQUIREMENTS STATEMENT
FTP	FILE TRANSFER PROTOCOL
FTP/SMTP	FILE TRANSFER PROTOCOL/ SIMPLE MAIL TRANSFER PROTOCOL
GIS	GEOGRAPHICAL INFORMATION SYSTEM

ACRONYMS	MEANING
GoI	GOVERNMENT OF INDIA
GPRS	GENERAL PACKET RADIO SERVICES
GPS	GLOBAL POSITIONING SYSTEM
GSM	GLOBAL SYSTEM FOR MOBILE COMMUNICATION
GST	GOODS AND SERVICES TAX
GUI	GRAPHICAL USER INTERFACE
HD	HIGH DEFINITION
HDD	HARD DISK DRIVE
HFE	HUMAN FACTORS ENGINEERING
HLD	HIGH LEVEL DESIGN
HTTPS	HYPertext TRANSFER PROTOCOL SECURE
ICCC	INTEGRATED COMMAND AND CONTROL CENTRE
ICMP	INTERNET CONTROL MESSAGE PROTOCOL
ICOMC	INPUT CONTROL OUTPUT MECHANISM
ICT	INFORMATION AND COMMUNICATION TECHNOLOGY
IDS	INTRUSION DETECTION SYSTEM
IEC	INTERNATIONAL ELECTROTECHNICAL COMMISSION'S
IEEE	INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS
IETF	INTERNET ENGINEERING TASK FORCE
IGMP	INTERNET GROUP MANAGEMENT PROTOCOL
IMAP	INTERNET MESSAGE ACCESS PROTOCOL
IoT	INTERNET OF THINGS
IP	INTERNET PROTOCOL
IPF	INFORMATION PROCESSING FACILITY
IPS	INTRUSION PREVENTION SYSTEM
ISO	INTERNATIONAL ORGANIZATION FOR STANDARDIZATION
ISP	INTERNET SERVICE PROVIDER
ISWM	INTEGRATED SOLID WASTE MANAGEMENT
IT	INFORMATION TECHNOLOGY
ITDP	INSTITUTE FOR TRANSPORTATION AND DEVELOPMENT POLICY
ITIL	INFORMATION TECHNOLOGY INFRASTRUCTURE LIBRARY
ITMS	INTELLIGENT TRAFFIC MANAGEMENT SYSTEM
IVA	INTELLIGENT VIDEO ANALYTICS
IVRS	INTERACTIVE VOICE RESPONSE SYSTEM
KML	KEYHOLE MARKUP LANGUAGE
KMZ	KEYHOLE MARKUP LANGUAGE ZIPPED
KPI	KEY PERFORMANCE INDICATOR
LAN	LOCAL AREA NETWORK
LDAP	LIGHTWEIGHT DIRECTORY ACCESS PROTOCOL
LoA	LETTER OF ACCEPTANCE
MAC	MEDIA ACCESS CONTROL
MAF	MINIMUM AUDIBLE FIELD
MEITY	MINISTRY OF ELECTRONICS & INFORMATION TECHNOLOGY
MIS	MANAGEMENT INFORMATION SYSTEM
MLPP	MASTER LEASE PURCHASE PROGRAM

ACRONYMS	MEANING
MPOS	MOBILE POINT OF SALE
SI	MASTER SYSTEM INTEGRATER
NAS	NETWORK ATTACHED STORAGE
NDSAP	NATIONAL DATA SHARING AND ACCESSIBILITY POLICY
NIT	NOTICE INVITING TENDER
NMS	NETWORK MANAGEMENT SYSTEM
NTP	NETWORK TIME PROTOCOL
O&M	OPERATION & MAINTENANCE
OEM	ORIGINAL EQUIPMENT MANUFACTURE
OFC	OPTICAL FIBER CABLE
OGC	OPEN GEOSPATIAL CONSORTIUM
ONVIF	OPEN NETWORK VIDEO INTERFACE FORUM
OS	OPERATING SYSTEM
OWASP	OPEN WEB APPLICATION SECURITY PROJECT
PA	PUBLIC ADDRESS
PDF	PORTABLE DOCUMENT FORMAT
PMO	PROJECT MANAGEMENT OFFICE
PoP	POINT OF PRESENCE
POS	POINT OF SALE
PSCL	PATNA SMART CITY LIMITED
PTZ	PAN TILT ZOOM
RACI	RESPONSIBLE, ACCOUNTABLE, CONFIRM, INFORM
RAID	REDUNDANT ARRAY OF INDEPENDENT DISKS
RFP	REQUEST FOR PROPOSAL
RLVD	RED LIGHT VIOLATION DETECTION
RTCP	REAL-TIME CONTROL PROTOCOL
RTF	RICH TEXT FORMAT
RTO	REGIONAL TRANSPORT OFFICE
RTSP	REAL TIME STREAMING PROTOCOL
SCADA	SUPERVISORY CONTROL AND DATA ACQUISITION
SCM	SMART CITY MISSION
SCP	SMART CITY PROPOSAL
SDC	STATE DATA CENTRE
SEO	SEARCH ENGINE OPTIMIZATION
SLA	SERVICE LEVEL AGREEMENT
SMF	SEALED MAINTENANCE FREE
SMS	SHORT MESSAGING SERVICE
SNMP	SIMPLE NETWORK MANAGEMENT PROTOCOL
SOP	STANDARD OPERATING PROCEDURES
SPV	SPECIAL PURPOSE VEHICLE
SRS	SYSTEM REQUIREMENT SPECIFICATIONS
SRTP	SECURE REAL-TIME TRANSPORT PROTOCOL
SSH	SECURE SHELL
SSL/TLS	SECURE SOCKETS LAYER/TRANSPORT LAYER SECURITY
SVD	SPEED VIOLATION DETECTION

ACRONYMS	MEANING
SWE	SENSOR WEB ENABLEMENT
TARS	TRAFFIC ACCIDENT REPORTING SYSTEM
TCV	TOTAL CONTRACT VALUE
TDS	TAX DEDUCTED AT SOURCE
TPA	THIRD PARTY AUDITOR
TTS	TEXT TO SPEECH
UAT	USER ACCEPTANCE TESTING
UD & HD	URBAN DEVELOPMENT AND HOUSING DEPARTMENT
UDP	USER DATAGRAM PROTOCOL
UPS	UNINTERRUPTED POWER SUPPLY
UTP	UNSHIELDED TWISTED PAIR
VAT	VALUE ADDED TAX
VLAN	VIRTUAL LOCAL AREA NETWORK
VM	VIRTUAL MACHINE
VMS	VIDEO MANAGEMENT SYSTEM
VMSB	VANCOUVER MASONIC SERVICE BUREAU
VOIP	VOICE OVER INTERNET PROTOCOL
VPN	VIRTUAL PRIVATE NETWORK
VRLA	VALVE REGULATED LEAD ACID
WAN	WIDE AREA NETWORK
XML	EXTENSIBLE MARKUP LANGUAGE

Table of Contents

1. Introduction	15
1.1. Project Objectives	15
1.2. Purpose of this RFP	15
2. Project Overview and Components	17
2.1. Components & Services Scope Overview	17
2.1.1. Assessment, Scoping and Survey Study	18
2.1.2. Scope of RFP.....	18
2.1.3. Data Centre	19
2.1.4. Provisioning of City Wide Network backbone	19
2.1.5. Capacity Building.....	22
2.1.6. Operations and Maintenance	22
2.2. Component Architecture of ICCC.....	22
3. Survey & Design Considerations for Technical Architecture & Project Plan	28
3.1. Commencement of Works	36
3.2. Existing Traffic Signal System	36
3.3. Road Signs	36
3.4. Electrical Works and Power Supply	37
3.5. Lightning-Proof Measures.....	37
3.6. Junction Box, Poles and Cantilever	38
3.7. Cabling Infrastructure	38
3.8. Integrated Command& Control Centre (ICCC).....	38
3.9. Integrated City Operation Platform	39
3.9.1. Urban Services and Data APIs	39
3.9.2. Platform Functionality	39
3.10. GIS Mapping.....	40
3.10.1. Video Analytics Usecases in the City.....	41
4. Other Expectation and Consideration from MSI.....	41
4.1. Expectations from MSI/SI	41
4.2. Inception Phase.....	44
4.3. Requirement/Planning & Assessment Phase.....	44
4.4. Design Phase	45

4.5.	Implementation & Installation Phase	45
4.6.	Post Implementation Phase	46
4.7.	Development & Software Customisation Phase.....	46
4.8.	Integration Phase (Existing Datasets & Other Applications).....	48
4.9.	Pilot Deployment	48
4.10.	Go-Live Preparedness and Go-Live	48
4.11.	Handholding and Training	48
4.12.	Operations and Maintenance	51
4.12.1.	Applications Support and Maintenance	51
4.12.2.	ICT Infrastructure Support and Maintenance	54
4.12.3.	Warranty support.....	54
4.12.4.	Maintenance of ICT Infrastructure at DC and ICCC.....	55
4.12.5.	Compliance to SLA	60
4.13.	Compliance to Standards & Certifications	60
4.14.	Testing and Acceptance Criteria	62
4.15.	Factory Testing & Pre-Despatch Inspection.....	64
4.16.	Final Acceptance Testing.....	64
5.	Detailed Scope of Work with Specifications	66
5.1.	Integrated Command Control & Communication Centre (ICCC)	66
5.1.1.	Functional & Technical Requirements for ICCC Platform	66
5.1.2.	Functional & Technical Requirements for Video Display Wall.....	81
5.1.3.	Functional & Technical Requirements for Video Wall Controller	82
5.1.1.1	Video Wall Management Software.....	83
5.1.4.	Functional & Technical Requirements for Monitoring Workstations.....	84
5.1.5.	Functional and Technical Specification of PTZ Joy Stick	84
5.1.6.	Functional and Technical Specification of LED Display (55 inches).....	85
5.1.7.	Functional & Technical Requirements for Desktops.....	86
5.1.8.	Functional & Technical Requirements for IP Phones.....	86
5.1.9.	Functional & Technical Requirements for CTI/PBX System	87
5.1.10.	Functional & Technical Requirements for Fixed Box/Bullet Cameras	88
5.1.11.	Functional & Technical Requirements for Non-IT items.....	90
5.1.11.1.	Functional & Technical Requirements for Ceiling Speakers	90
5.1.12.	Functional & Technical Requirements for ICCC Interiors.....	92

5.1.13.	Functional & Technical Requirements for Network Laser Printer	96
5.1.14.	Functional & Technical Requirements for Biometric Access Control System.....	97
5.2.	ICT Infrastructure Components	99
5.2.1.	ICT Hardware Components for Data Centre	100
5.2.1.1.	Functional & Technical Requirements for Core Router	100
5.2.1.2.	Functional & Technical Requirements for Internet Router	100
5.2.1.3.	Functional & Technical Requirements for Data Centre Firewall.....	101
5.2.1.4.	Functional & Technical Requirements for WAF	104
5.2.1.5.	Functional & Technical Requirements for AAA: (Authentication, Authorization and Accounting)	106
5.2.1.6.	Functional & Technical Requirements for DLP	110
5.2.1.7.	Functional & Technical Requirements for DC Core Switch	112
5.2.1.8.	Functional & Technical Requirements for DC Switches	115
5.2.1.9.	Functional & Technical Requirements for Servers: (Blade Servers, GPU Servers. AAA servers and A.I./Training Server).....	119
5.2.1.10.	Functional & Technical Requirements for GPU Based Rack Servers (Video Analytics & FRS Servers).....	121
5.2.1.11.	Functional & Technical Requirements for AAA Server	122
5.2.1.12.	Functional & Technical Requirements for Continuous Learning Server A.I/Training Server	127
5.2.1.13.	Functional & Technical Requirements for Blade Chassis	128
5.2.1.14.	Functional & Technical Requirements for SAN Switch	129
5.2.1.15.	Functional & Technical Requirements for Scale Out Storage	130
5.2.1.16.	Functional & Technical Requirements for Unified Storage.....	133
5.2.1.17.	Functional & Technical Requirements for Backup Appliance	135
5.2.1.18.	Functional & Technical Requirements for Aggregation Switches.....	139
5.2.1.19.	Functional & Technical Requirements for 24 Port L3 Switch.....	140
5.2.1.20.	Functional & Technical Requirements for PoE Ruggedized Switches.....	141
5.2.1.21.	Functional & Technical Requirements for Online UPS - 100 KVA	144
5.2.1.22.	Functional & Technical Requirements for Online UPS - 300 KVA	151
5.2.1.23.	Functional & Technical Requirements for Online UPS – 1/2/3/5 KVA.....	157
5.2.1.24.	Functional & Technical Requirements for Online UPS - 500 VA	159
5.2.1.25.	Functional & Technical Requirements for HIPS & NIPS	160
5.2.1.26.	Functional & Technical Requirement for SIEM	163

5.2.2.	Intelligent Integrated Infrastructure.....	164
5.2.2.1.	Fire Proof Enclosure	165
5.2.2.2.	Structured Cabling.....	165
5.2.2.3.	Technical Specifications for Indoor Copper cable	165
5.2.2.4.	Technical Specifications for Outdoor Copper cable	166
5.2.2.5.	Electrical System & cabling	166
5.2.2.6.	Cooling System.....	167
5.2.2.7.	Precision Air Conditioning System	167
5.2.2.8.	Safety and Security System	169
5.2.2.9.	Monitoring System.....	176
5.2.2.10.	42U Racks and PDU	177
5.2.2.11.	9U Rack.....	179
5.2.2.12.	KVM Switch	179
5.2.2.13.	Anti-Climb & Cantilever Poles for Mounting Camera etc.	180
5.2.2.14.	DG Set (Diesel Genset)	180
5.2.2.15.	NOVEC 1230 Gas based Fire Suppression System	181
5.2.2.16.	The Rodent Repellent System	181
5.2.2.17.	Water Leak Detection System.....	182
5.2.2.18.	High Sensitivity Smoke Detection System.....	182
5.2.2.19.	Raised Floor.....	187
5.2.2.20.	False Ceiling.....	189
5.2.2.1.	Building Management System	190
5.2.3.	ICT Software Components for Data Canter.....	191
5.2.3.1.	Functional Enterprise Management System.....	191
5.2.3.2.	Functional & Technical Specifications for Server Load Balancer	201
5.2.3.3.	Functional & Technical Requirements for Link Load Balancer	202
5.2.3.4.	Functional & Technical Requirements for Centralized AV & Anti-Spam	204
5.2.3.5.	Functional & Technical Specifications for Network Management System	206
5.2.3.6.	Functional & Technical Specifications for Centralised Helpdesk	206
5.2.3.7.	IDAMFunctional & Technical Requirements for Mailing & Messaging Solution	207
5.2.3.8.	Functional & Technical Requirements for Identity Access Management.....	213
5.2.3.2.	Functional & Technical Requirements for Enterprise Database	218
5.2.3.3.	Functional & Technical Requirements for Directory Services.....	220

5.3.	Data Centre and Disaster Recovery Centre	220
5.3.1.	Disaster Recovery and DR Cloud	221
5.3.2.	Preparation of Disaster Recovery Operational Plan	222
5.3.3.	Functional & Technical Requirement for DR Management	223
5.3.4.	Periodic Disaster Recovery Plan	223
5.4.	Mobile App.....	223
5.5.	Network Backbone and Internet Connectivity	224
5.5.1.	Scope of work.....	227
5.5.2.	General Specifications.....	228
5.5.3.	Technical Specifications	231
5.6.	Public Address (PA) System.....	231
5.7.	Emergency Call Box (ECB) System.....	233
5.8.	Variable Message Sign boards	233
5.9.	Variable Message Sign Board application	236
5.9.1.	Remote Monitoring.....	238
5.10.	Environmental Management System	239
5.11.	Trenching using HDD/ Optical Fibre Cable.....	242
5.11.1.	Specification of Permanently Lubricated HDPE Pipe	242
5.11.2.	Technical Specifications of Single Mode Optical Fibre Cable	244
6.	SOW and Functional Requirement For Integrated Traffic Management System (ITMS)	
	Components:	248
6.1.	Adaptive Traffic Control System (ATCS).....	248
6.1.1.	Key Components of Adaptive Traffic Control System (ATCS)	248
6.1.2.	ATCS application software requirement	252
6.1.3.	Detailed Specifications for Vehicle Detector Sensor	256
6.2.	Automatic Number Plate Recognition (ANPR) System	257
6.3.	Traffic Violations and Enforcement System.....	260
6.4.	Automated e-Challan System	263
6.5.	Traffic Accident Reporting System (TARS)	264
6.6.	Traffic Sensors Lights and Signals	264
7.	CCTV Surveillance System	266
7.1.	Scope of Work.....	266
7.2.	Overview	267

7.3.	Functional and Technical Requirements for VMS.....	268
7.4.	Video Analytics Software for 1000 Cameras with average 2 use cases per camera	275
7.5.	Functional & Technical Requirements for Facial Recognition System.....	276
7.6.	Video Summarization Functional & Technical Specification:.....	281
7.7.	Picture Intelligence Unit- Functional Requirement & Technical specification	284
7.8.	AI with continuous Learning & Improvement System - Functional Requirement & Technical specification	288
7.9.	Functional & Technical Requirements for Outdoor Fixed Cameras/Bullet/Dome(HD)	293
7.10.	Functional & Technical Requirements for PAN, Tilt & Zoom(PTZ) Camera	294
7.11.	Functional & Technical Requirements for ANPR System	296
7.12.	Functional & Technical Requirements RLVD System	299
7.13.	Infrared Illuminators- Functional & Technical Specification.....	302
8.	Project Governance and Change Management	302
8.1.	Project Management and Governance	302
8.1.1.	Project Management Office (PMO)	302
8.1.2.	Helpdesk and Facilities Management Services	303
8.1.3.	Steering Committee	303
8.1.4.	Project Monitoring and Reporting.....	304
8.1.5.	Risk and Issue management.....	304
8.2.	Governance procedures.....	304
8.2.1.	Planning and Scheduling	304
8.2.2.	License Metering / Management.....	305
8.3.	Manpower Deployment.....	305
8.4.	Change Management & Control	307
8.4.1.	Change Orders / Alterations / Variations.....	307
8.5.	Exit Management	308
8.5.1.	Cooperation and Provision of Information	308
8.5.2.	Confidential Information, Security and Data	309
8.5.3.	Transfer of Certain Agreements.....	309
8.5.4.	General Obligations of SI.....	309
8.5.5.	Exit Management Plan	310
9.	Project Implementation Schedule, Deliverables and Payment Terms.....	311
9.1.	Payment Schedule.....	316

10. Annexures:	318
10.1. Annexure 1 : Bill of Quantity	318
10.2. Annexure 2 : Floor Wise Layout for Final Building	334
10.3. Annexure 3 : Existing Wi-Fi Hotspots in City	339
10.4. Annexure 4 : Existing Installed Adaptive Traffic Management System	341
10.5. Annexure 5 : List of Sites for CCTV Surveillance at Police Station and Railway Station Area	343
10.6. Annexure 6 : Existing Installed Camera for City Surveillance under DIAL 100	351
10.7. Annexure 7 : Existing Locations of Installed cameras for Patna Police on PPP Mode	355
10.8. Annexure 8 : Existing VASUDHA CENTRES in Pan City	358
10.9. Annexure 9 : Services being offered by VASUDHA CENTRE	359
10.10. Annexure 10 : IT Infrastructure Installed in existing Bihar State Data Center	360
10.11. Annexure 11 : Application Hosted on existing State Data Center	360
10.12. Annexure 12 : Application Hosted on existing State Data Center Cloud Platform	362
10.13. Annexure 13 : IT & Non IT Equipments in existing State Data Center	362
10.14. Annexure 14 : Block Diagram of existing BSWAN Network	364
10.15. Annexure 15: Existing e-Governance Services offered by e-Municipality	365
10.16. Annexure 16 : BSNL Optical Fiber Network in ABD Area	365
10.17. Annexure 17 : Existing BSNL OFC Layout Diagram for ABD area of Patna City	366
10.18. Annexure 18 : Analytics Use Cases Required with the Type of Locations	367
10.19. Annexure 19 : ICC Design Considerations	368
10.20. Annexure 20 : Common guidelines regarding compliance of systems / equipment	386
10.21. Annexure 21 : Standards for Bio-Metrics	388
10.22. Annexure 22 : Standards for Digital Preservation Standards	392
10.23. Annexure 23 : Standards for Localization and Language Technology	395
10.24. Annexure 24 : Standards for Metadata and Data	398
10.25. Annexure 25 : Standards for Mobile Governance	400
10.26. Annexure 26 : Standards for GIGW	410
10.27. Annexure 27 : Standards for Open APIs	415
10.28. Annexure 28 : Standards for Internet of Things	417
10.29. Annexure 29 : Standards for Disaster Management	419

LIST OF TABLES

Table 1 : Key Foundation Components.....	17
Table 2: Description of Block Diagram of Proposed Solution.....	26
Table 3: Standards & Certifications for Compliance	61
Table 4 : Various Testing envisaged for the project	62
Table 5: Fiber Mechanical Characteristics	245
Table 6 : Fiber Parameters and Values	246

LIST OF FIGURES

Figure 1 : Data Center Architecture.....	20
Figure 2 : Logical Architecture of Patna City Wide Network	21
Figure 3: Indicative Architecture of ICCC	24
Figure 4: Building blocks of an Integrated Command and Control Center	25
Figure 5: Design of Distribution and Access Network.....	226
Figure 6 : Typical Manhole Dimensions	247
Figure 7 : Layout of Ground Floor at Final Building	334
Figure 8 : Layout of Floor-1 at Final Building.....	335
Figure 9 : Layout of Floor-2 at Final Building.....	336
Figure 10 : Layout of Floor-3 at Final Building.....	337
Figure 11 : Layout of Floor-4 at Final Building.....	338
Figure 12 : Block Diagram of BSWAN Network	364

1. Introduction

1.1. Project Objectives

The key objective of this project is to establish a collaborative framework where input from different smart solutions implemented by PSCL, and other stake holders can be assimilated and analyzed on a single platform; consequently, resulting in aggregated city level information. Further this aggregated city level information can be converted to actionable intelligence, which would be propagated to relevant stakeholders and citizens in coordinated and collaborative manner. Following are the key outcomes expected to be achieved by the proposed interventions:

- Improved visualization of ambient or emergency situation in the city and facilitation of data driven decision making
- Efficient traffic management
- Enhanced safety and security
- Better management of utilities and quantification of services
- Asset Management
- Disaster Management and Emergency Response
- Efficiency improvement in public service delivery
- Inter-departmental coordination and collaboration for faster execution of services
- Implementation and Integration with all existing and future services as identified by Patna Smart City limited(PSCL) in the city including but not limited to (with provision for future scalability):
 - i. CCTV Surveillance System
 - ii. Smart Lighting
 - iii. ICT Enabled Solid Waste Management
 - iv. Intelligent Transportation System
 - v. E-Challan System
 - vi. Public Bike Sharing
 - vii. Smart Education
 - viii. Smart Health Management System
 - ix. e-Municipality
 - x. Smart Road Network
 - xi. eBuses Live Tracking and Monitoring System
 - xii. eToilet Monitoring System
 - xiii. Environment Management System
 - xiv. ICT component of eLibrary System
 - xv. ICT component of Smart Bus Stop System
 - xvi. ICT component of Smart Parking System
 - xvii. Any other upcoming solutions

1.2. Purpose of this RFP

The purpose of this Tender is for the Patna Smart City Corporation Limited (PSCL) to enter into a contract with a qualified firm for the Supply, Installation, Configuration, Integration, Commissioning, Operations and Maintenance of integrated solutions to support the command, and control centre initiative for smart city initiative of PSCL. PSCL is looking to engage a Master Service Integrator -

- a) Who brings strong technology experience in smart city implementation, integration and operations through integrated and multi-agency coordination platform
- b) Who can develop Standard Operating Procedures for the various components of the project and link with uses cases prepared by them
- c) Who has a quality control plan in place to demonstrate that all equipment is tested and passed prior to shipping
- d) Who is capable of providing high quality installations of the project equipment
- e) Who is capable of maintaining and operating the complex smart city systems to provide maximum decision making support and performance of the systems
- f) Who brings forth expertise for traffic management, incident and emergency management
- g) Who has experience implementing city-wide ICT and surveillance system coupled with using the said systems efficiently through data analytics
- h) Who will strongly build capacity of various stakeholders for efficient operations and management of the proposed solutions

This tender is designed to provide interested bidders with sufficient basic information to submit proposals meeting minimum requirements, but is not intended to limit a proposal's content or exclude any relevant or essential data. Bidders are at liberty and are encouraged to expand upon the specifications to evidence superior bid understanding and service capability.

2. Project Overview and Components

Key foundation components for PSCL Smart City considered for this RFP are as follows for implementation:

Table 1 : Key Foundation Components

S.No.	Component
1.	OFC laying and Network Backbone
2.	Command Control & Communication Centre
3.	Data Centre and DR Site
4.	ITMS
5.	Variable Message System
6.	Public Address System
7.	Emergency Call Box (ECB) System
8.	Environmental Monitoring System
9.	Enterprise GIS for Web GIS with Geo Analytics (Only for adding layers)
10.	Mobile App
11.	CCTV Surveillance
12.	Video Analytics
13.	Artificial Intelligence & Machine Learning
14.	Facial Recognition system
15.	Traffic and Transportation Management
16.	Smart Parking Integration

2.1. Components & Services Scope Overview

The selected SI shall ensure the successful implementation of the proposed ICCS solutions as well as provide capacity building support to city authorities as per the scope of services described below. Any functionality not expressly stated in this document but required to meet the needs of the PSCL to ensure successful operations of the system shall essentially be under the scope of SI and for that no extra charges shall be admissible. Any requirement beyond the outlined SOW will be considered after approval of Change Request from PSCL on additional cost. SI shall implement

and deliver the systems and components which are described in this RFP. SI's 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 Annexures.

2.1.1. Assessment, Scoping and Survey Study

Conduct a detailed assessment, survey, gap analysis, scoping study and develop a comprehensive project plan, including:

- Assess existing ICT systems, Network connectivity with in the city and the green-field site for the scope items mentioned in this Volume of the RFP.
- Conduct site survey for finalization of detailed technical architecture, gap analysis, final Bill of Quantities and project implementation plan.
- Conduct site surveys to identify the need for site preparation activities.

Obtain site clearance obligations & other relevant permissions with the support of PSCL.

2.1.2. Scope of RFP

I. Scope of this RFP includes, Design, Supply, Configuration, Installation, Implementation, Testing and Commissioning of the following primary components:

- Integrated Command and Control Centre
- Data Centre within ICCB Building
- Disaster Recovery Centre (Hosted on cloud data centre of any MEITY empanelled cloud Service Provider)
- City Surveillance
- Intelligent Traffic Management System
 - i. Adaptive Traffic Control System (ATCS)
 - ii. Automatic Number Plate Recognition (ANPR) System
 - iii. Red Light Violation Detection (RLVD) System
 - iv. Speed Violation Detection (SVD) System
 - v. Traffic Violation Cameras
 - vi. Variable Message Sign boards
 - vii. Public Address (PA) System
 - viii. Emergency Call Box (ECB) System
- Environmental Monitoring Sensors
- Mobile App
- Enterprise GIS for Web GIS with Geo Analytics (Only for adding layers)
- Video Analytics
- Facial Recognition System
- OFC laying

The detailed requirements of the above would be delineated within the subsequent sections.

II. Integration with existing ICT systems (If any) within PSCL ICT landscape, not limited to:

- Smart Lighting
- ICT Enabled Solid Waste Management
- Intelligent Transportation System
- e-Challan System
- Public Bike Sharing
- Smart Education
- Smart Health Management System
- e-Municipality
- Smart Road Network
- e-Buses Live Tracking and Monitoring System
- eToilet Monitoring System
- Environment Management System
- ICT component of eLibrary System
- ICT component of Smart Bus Stop System
- ICT component of Smart Parking System
- Any other upcoming solutions

2.1.3. Data Centre

Provisioning of Hardware, Network and Software Infrastructure, which includes design, supply, installation and commissioning of ICT Infrastructure at the Command Control and Communication Centre & Data Centre. This scope consists of:

- Site preparation services
- IT Infrastructure including server, storage, other required hardware, application portfolio, licenses
- Command Centre infrastructure including Video Walls, workstations, IP phones, joystick controller etc.
- Establishment of LAN and WAN connectivity at Command Centre and DC limited to scope of infrastructure procured for the project
- Application Development and integration services for the applications mentioned in 2.1.2

2.1.4. Provisioning of City Wide Network backbone

- Assessment of ISP service provider available in city
- Connectivity between field device and DC and ICC
- Connectivity between DC & proposed DR
- Internet Connectivity at DC
- Network shall be sized with sufficient capacity to support redundancy and future traffic growth in order to complete traffic rerouting on the network in the event of failure without affecting overall network performance.

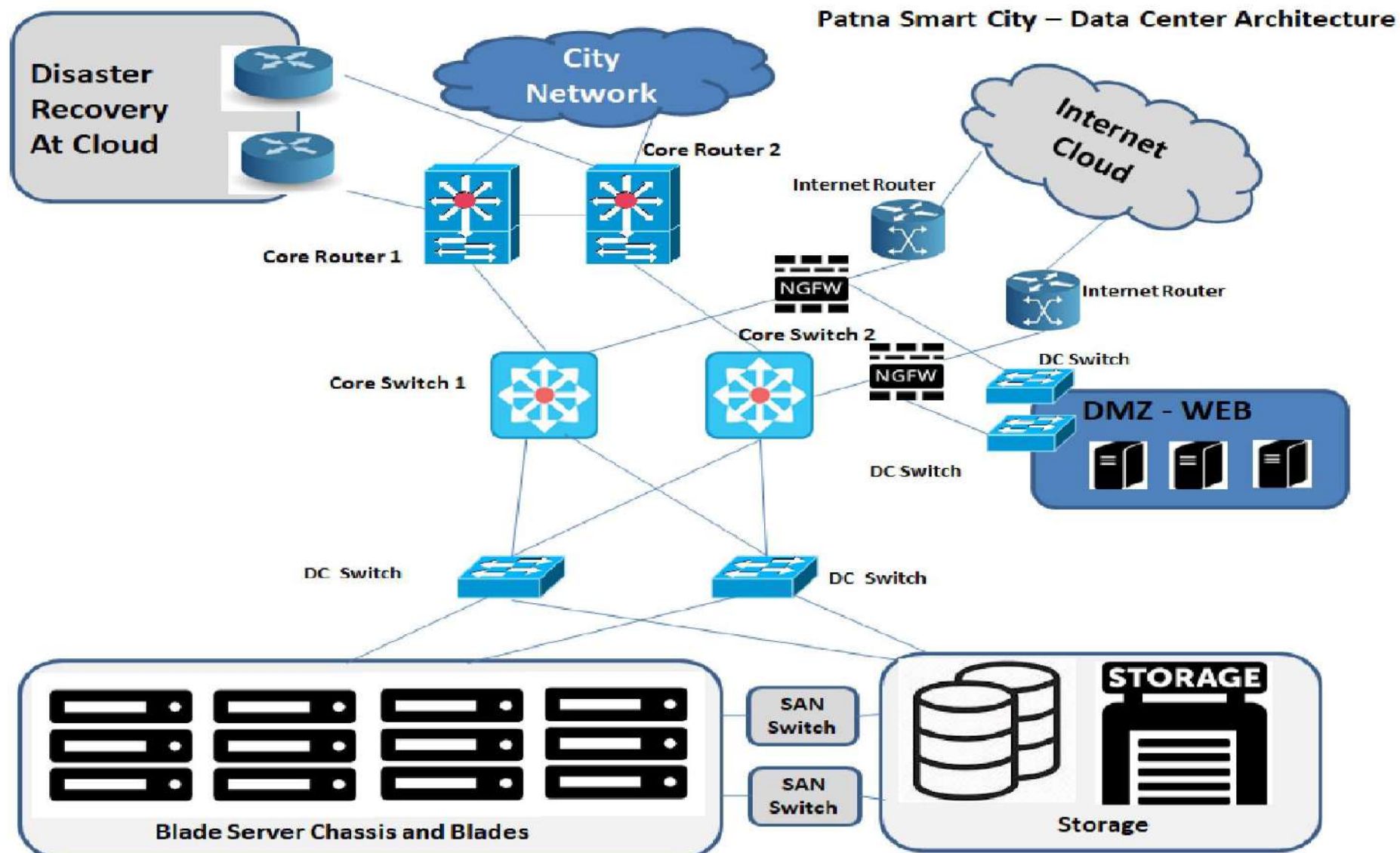


Figure 1 : Data Center Architecture

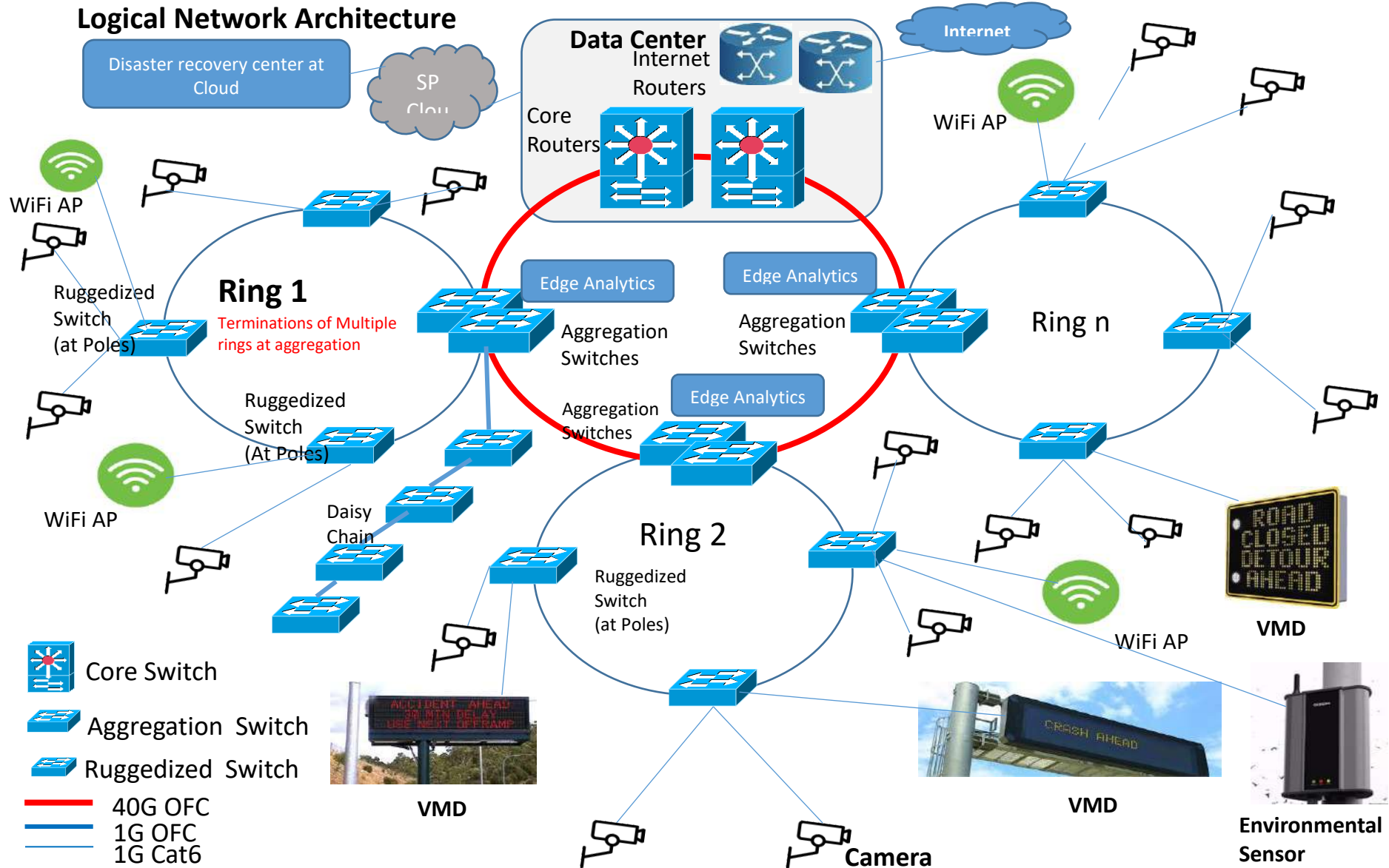


Figure 2 : Logical Architecture of Patna City Wide Network

2.1.5. Capacity Building

Capacity Building for PSCL and any other department which includes preparation of operational manuals, training documents and capacity building support, including:

- Training of city authorities, operators and other stakeholders on operationalization of the system

Support during execution of acceptance testing

Preparation and implementation of the information security policy, including policies on backup and redundancy plan

Preparation of revised KPIs for performance monitoring of various urban utilities monitored through the system envisaged to be implemented

Developing standard operating procedures for operations management and other services to be rendered by ICCC

Preparation of system documents, user manuals, performance manuals, Operation manuals, etc.

2.1.6. Operations and Maintenance

MSI shall also be responsible for the maintenance and management of entire systems, solutions, application deployed as part of this RFP for a period of 5 years from the Go-Live date of implemented solutions in an efficient and effective manner.

2.2. Component Architecture of ICCC

Indicative architecture of the components envisaged under the “Integrated Command Control and Communication Centre” as well as the Building Blocks are as given in the figures below. This component architecture is indicative in nature and is given in the RFP to bring clarity to prospective bidders on the overall scope of project and its intended use. SI shall carry out the detail requirement analysis and finalize technical architecture. The architecture layers of the complete network of smart elements is as follows:-

a) Sensor or Field instrument layer

The sensor layer will help the city administration gather information about the ambient city conditions or capture information from the edge level devices like intelligent traffic signals, cameras, enforcement sensors, emergency call boxes, etc. PSCL city is expected to have environmental IoT sensors installed at multiple locations across the city, to measure & report ambient conditions such as light intensity, temperature, water level (for chronic flood spots), air pollution, noise pollution and humidity for decision makers to take preventive, pro-active and execute responses in case of emergency/natural calamity.

b) Data Collection and Transmitting Layer

Controller processes the input data from the sensor which applies the logic of control and causes an output action to be generated. This signal may be sent directly to the controlled device or to other logical control functions.

The controllers function is to compare its input (from the sensor) with a set of instructions such as set point, throttling range and action, then produce an appropriate output signal. It usually consists of a control response along with other logical decisions that are unique to the specific control application. After taking the logical decision of the information it will hand over the information to the next layer (Network Layer) which will be subsequently available at the ICCC.

c) Network/Communication Layer

The secured network layer will serve as the backbone for the project and provide connectivity to gather data from sensors and communicate messages to display devices and actuators. It will

support the Wi-Fi services and other smart elements (sensors and displays) at given locations wherever applicable. The network layer will be scalable such that additional sensors, actuators, display devices can be seamlessly added.

d) Data Centre Layer

The Data Centre layer will house centralized computing power required to store, process and analyze the data to decipher actionable information. This layer includes HCI infrastructure for running complete virtualized infrastructure and physical servers, storage, ancillary network equipment elements, security devices and corresponding management tools. Similar to the network layer, it will be scalable to cater to the increasing computing and storage needs in future.

e) Security Layer

As ambient conditions, actuators and display devices are now connected through a network, security of the entire system is of paramount significance and SI will have to provide:

- i. Infrastructure Security- including policies for identity and information security policies
- ii. Network Security- including policies and practices adopted to prevent and monitor unauthorized access, misuse, modification, or denial of a computer network and network-accessible resources, etc.
- iii. Identity and Access Management – including user authentication, authorization, SSL & Digital Signatures.
- iv. Application Security- including hosting of Government Websites and other Cloud based services, adoption of Technical Standards for Interoperability Framework and other standards published by GoI for various e-Governance applications.
- v. End Device Security, including physical security of all end devices such as display boards, emergency boxes, kiosks etc.

Following security parameters should be included for all smart elements, but not limited to:

- i. User/administrator audit log activity (logon, user creation, date-time of PA announcements, voice recording etc.)
- ii. Secured data storage (storage of video/image/voice/location/data captured by various smart elements)
- iii. SSL/TLS encryption for web and mobile application based interfaces for sensitive data transfer
- iv. Protection against Denial of Service (DoS) and Interference attacks to public Wi-Fi Devices

f) Smart Application and Integration Layer

The smart applications layer will contain data aggregation and management systems (rules engines, alerting systems, diagnostics systems, control systems, messaging system, events handling system), and reporting / dashboard system to provide actionable information to city administrators and citizens. It will be an evolving layer with applications added and integrated as and when new applications are developed at PSCL. While aspects of ambient conditions within the city will be gathered through various sensors deployed, some city specific data will come from other government and non-government agencies. It is through the integration layer– that data will be exchanged to and from the underlying architecture components and other data from system developed by the State Government (such as police department, meteorological department, energy department, water department, irrigation department, transport organizations within PSCL, etc.) and non-government agencies.

g) Service delivery and Publishing Layer

The output field devices layer will contain display devices or bi-directional (input & output) devices connected to the network which will be used by citizens to consume - and for administrators to provide - actionable information. Such field devices include digital messaging boards, environmental data displays, etc. The Command Centre publishes the information which will enable citizens and administrators alike to get a holistic view of city conditions. The implementation vendor will have to develop a Command Centre at the site location identified by PSCL and web/ mobile based viewing tools for understanding the ambient city conditions.

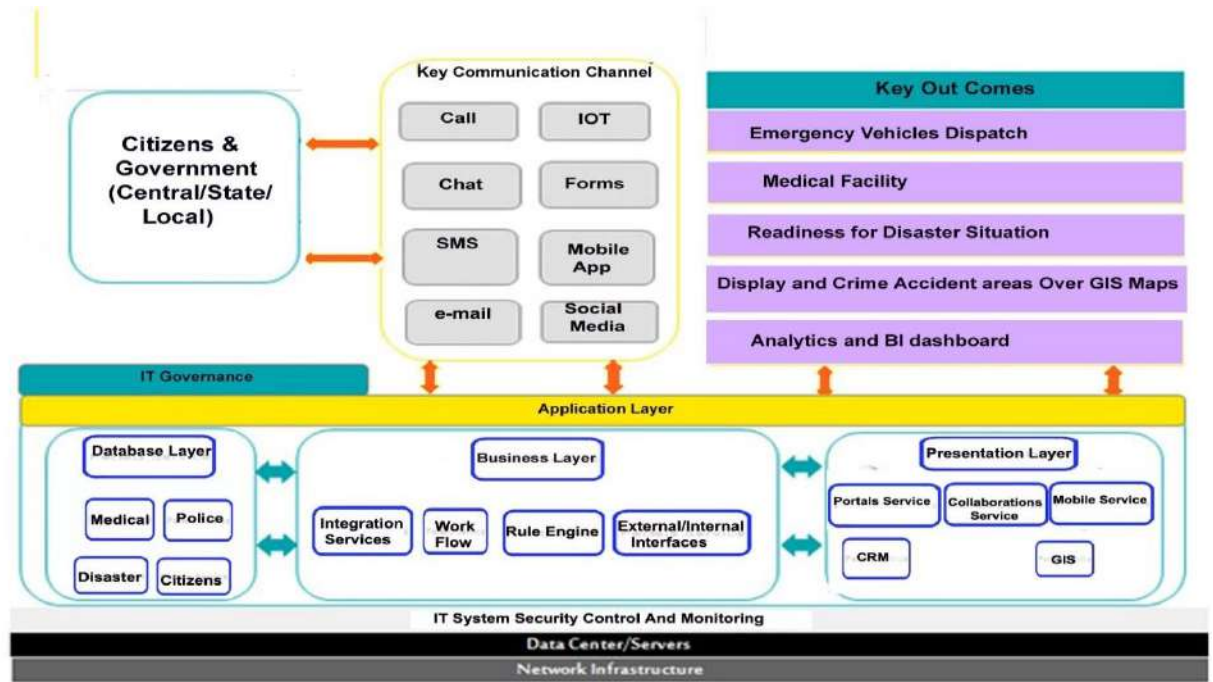


Figure 3: Indicative Architecture of ICC

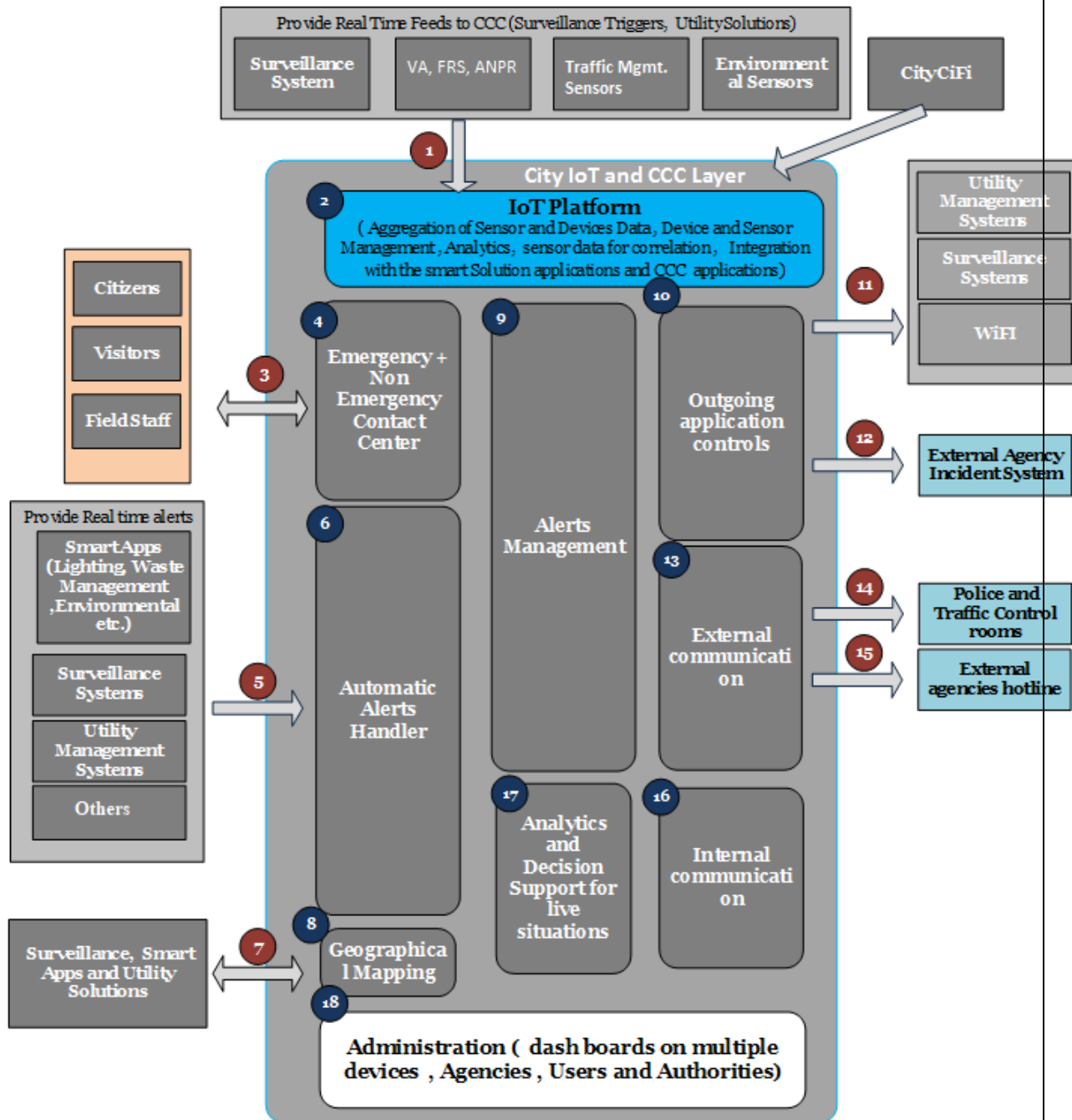


Figure 4: Building blocks of an Integrated Command and Control Center

The proposed functionality of each block, as depicted in the Figure-2, is described below (S.No. mentioned in the table below are mapped to the block numbers mentioned in the diagram):

Table 2: Description of Block Diagram of Proposed Solution.

S. No. (Mapped to ref numbers in the diagram)	Type	Description
1.	Interface	Surveillance, Environmental Sensor and utility management systems will provide real time, at pre-defined frequency and on-demand feeds into the CCC.
2.	IoT Function	Platform will do the conversion of the different form of data form devices and Sensors to a single format, Perform the device and sensor management, Correlation between different Sensors/ Devices data, Perform rule base and analytics on sensors and devices data. Integration with the Smart Solution application interface, Integration with command and Control centre Visualization and Response layer.
3.	Interface	The contact centre interface will provide citizens and field staff of various agencies with the single point where they will be able to record their grievances / feedback / incidents. This interface will enable citizens to interact with CCC through audio call, SMS, mobile interface and web interface. This will be a two-way interface enabling citizens to pass information to CCC and receive updates from CCC on the actions taken by CCC.
4.	CCC Function	The contact centre function will enable CCC to record and update both day to day incidents such as electricity break down and emergency situations such as accidents. The contact centre will receive the information from citizen and record in the database which will trigger the workflow for resolution of the incident.
5.	Interface	<p>The Interface will enable automatic capture of the following Data: Sensor Data from the various sensor platform including IoT based Gateways deployed as a part of the Smart City Systems</p> <p>The systems deployed throughout the city will be monitoring the various incidents taking place as per the rules defined in the respective systems. The incidents captured automatically by these monitoring systems shall be reported into the CCC via this automated interface</p>

S. No. (Mapped to ref numbers in the diagram)	Type	Description
		<p>This will enable CCC to aggregate and create a centralized repository of all Data & incidents reported throughout the city either manually (as in 3 & 4 above) or through this automated interface. The envisaged systems that will be generating these alerts are –</p> <ul style="list-style-type: none"> a) Surveillance Systems b) Mobile Apps (Mobile Interface for stakeholders to record incidents if any)
6.	CCC Function	This function within the CCC will enable it to receive the sensor data from IoT Platform and generate alerts or receive the alerts directly from other system, add relevant data to the alerts incident and pass on to next entity as per pre-defined workflow
7.	Interface	Surveillance, Smart and Utility Management Systems would use the geographical functions and geo-spatial data stored in the central GIS application for implementing their functionality that requires GIS layer. The required data and functionality exchange would be done through this system.
8.	CCC Function	This block refers to the centralized GIS layer that would be created at CCC for access by other systems.
9.	CCC Function	The incidents reported manually through contact center as well as automatically received through alerts handler shall be handled by this functional block. Further, it will enable the CCC to carry out complex event processing for data received from Sensor system directly, correlate the data through rule engine for alerts creation and will enable execution of workflow for managing the incident life cycle as per pre-defined business rules and SOPs. This will ensure consistency of response to incidents.
10.	CCC Function	The CCC will control the Surveillance, Smart and Utility Management systems via this interface enabling them to be controlled through a common interface.
11.	Interface	This interface will enable CCC to pass data to be used by various systems e.g. view triggers into various systems such as viewing a specific camera view into CCC, sending SMS through a SMS gateway etc.

S. No. (Mapped to ref numbers in the diagram)	Type	Description
12.	Interface	This interface will enable CCC to pass data to intimate the respective agency about incident reported in CCC e.g. creating incident in incident management system of electricity department about power failure
13.	CCC Function	This function will enable CCC to interact with external stakeholders. This block shall use tools such as Video Conferencing, Agency hot-lines etc.
14.	Interface	This interface shall enable transfer of video feeds to traffic and police control rooms
15.	Interface	This interface shall enable audio and video hotlines to agencies and offices in case of emergency situations
16.	CCC Function	The internal communication within CCC shall be managed through video conferencing and IP telephony systems
17.	CCC Function	This block will enable CCC to perform analytics on the data gathered during lifecycle of various incidents thereby enabling it to make informed changes to SoPs and business rules .
18.	CCC Function	This block will enable CCC to define the security access rights, Standard Operating Procedures, Business Rules, and Workflows , Integration with the IoT Platform for Device Provisioning and Management (Sensor System) etc. to enable the CCC to function in the desired manner

3. Survey & Design Considerations for Technical Architecture & Project Plan

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

- a) Names of the Project Team members, their roles & responsibilities and deliverables
- b) 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)
- c) Responsibility assignment matrix for all stakeholders
- d) Risks that SI anticipates and the plans they have towards their mitigation
- e) Detailed project plan specifying dependencies between various project activities / sub-activities and their timelines

f) Installation locations for field devices geo mapped to visually identify the geographical area

SI shall conduct a comprehensive As-Is study of the existing system and infrastructure. The report shall also include the expected measurable improvements against each KPI in 'As-Is' study after implementation of smart solutions under this project. The benchmarking data should also be developed to track current situation and desired state.

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

SI will be responsible to propose transition strategy for dismantling of existing signals, and setting up of new smart signals and field components. The proposed strategy should clearly provide approach and plan for implementing the new signals and field components while ensuring minimum disturbance to the road traffic and shall use appropriate static signage designating the work in progress status.

Additionally, SI should provide a detailed To-Be designs specifying the following:

- a) High Level Design (including but not limited to) Application architecture, Logical and physical database design, Data dictionary and data definitions, ER (Entity Relationship) diagrams and other data modeling documents and Physical infrastructure design for devices on the field.
- b) Application component design including component deployment views, control flows, etc.
- c) 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 Bihar.
- d) Location of all field systems and components proposed at the junctions, (KML /KMZ file plotted on map) with GEO coordinates.
- e) Height and foundation of Cameras, Traffic Signals and Poles for Pedestrian signals, Height and foundation of Poles, cantilevers, gantry and other mounting structures for other field devices.
- f) Location of Junction Boxes.
- g) Electrical power provisioning.

SI shall also identify the customizations/ workaround that would be required for successful implementation and operation of the project. The SI would be offering the products and solutions which meet the 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 report should take into consideration following guiding principles:

- a) **Transformational Nature of Smart City applications** - Applications should look to fully embrace mobile adoption, online authentication, etc. to transform the processes completely and offer wider choice and no/low touch point for residents to interact directly.

It is critical that project design is aligned to larger trends and designed for next decade rather than past.

- b) **Use of Open Standard for evolving Technology:** The entire system would be built to be open (standards, open API, plug-n-play capabilities like virtual environments, creating sandbox), components coupled loosely to allow changes in sub- system level without affecting other parts, architected to work completely within a heterogeneous compute, storage, and multi-vendor environment. Use of the latest & best available standards to avoid locking in obsolescent technologies simulated services environment can help agencies to save cost, infrastructure and time in testing multiple application integrations. Large integrated systems of Smart City operations should be designed to get the best cost and performance advantages of natural technology curve (constant increase of speed and decrease of cost), architecture should be open and vendor neutral, and designed for horizontal scale. The technology shall scale linearly and shall have the provision to infuse new technologies without any disruption to running environment. It shall be support hardware agnostic and hypervisor agnostic so that we are not bind or dependent on buying a particular hardware of virtualization solution.
- c) **Distributed, PKI,AAA based Authentication and Authorization** - The solution shall support 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.
- **Security and privacy of data** –The security services will cover the user profile management, authentication and authorization aspects of security control. This service run across all the layers since service components from different layers will interact with the security components. All public contents should be made available to all users without authentication. The service will authenticate users and allows access to other features of the envisaged application for which the user is entitled to. The system should be designed to provide the appropriate security levels commensurate with the domain of operation. Also the system will ensure data confidentiality and data integrity. 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 endeavor to make use of the SSL/VPN technologies to have secured communication between Applications and its end users. Furthermore, all the system logs should be properly stored & archived for future analysis and forensics whenever desired. The authority would carry out the Security Audit of the entire system upon handover and also at regular intervals during O&M period. Bidder’s solution shall adhere to the model framework of cyber security requirements set for Smart City (K-15016/61/2016-SC-1, Government of India, and Ministry of Urban Development).
- **Security Configuration Baseline Management (SCBM):** Automatically and constantly keep infrastructure secure via automated checks and self-healing. Logs all corrective changes for audit.

Insurance and Security - 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 it is burnt/stolen/damaged/faulty due to any reason.

Appropriate insurance cover from Nationalized Insurance Company must be provided to all the equipment's supplied under this project till end of O&M period. SI has to provide copy of Insurance Policy at the time of Go-Live for all equipments. In case of annual policy, SI has to provide renewed policy before 15 days of expiry of previous policy. The Insurance will be in the name of Patna Smart City Ltd. The documentation regarding the claims, renewal will be done by SI and this will be signed and approved PSCL.

- a) 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.
- b) The security services used to protect the solution shall include: Identification, Authentication, Access Control, Administration and Audit and support for industry standard protocols.
- c) The solution shall support advanced user authentication mechanisms including digital certificates and biometric authentication.
- d) 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.
- e) 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.
- f) The overarching requirement is the need to comply with ISO 27001 standards of security.
- g) The application design and development should comply with OWASP top 10 principles.
- h) A secure solution should be provided at the hardware infrastructure level, software level, and access level.
- i) Authentication, Authorization & Access Control: 3 factors (User ID & Password, Biometric, and Digital Signature) security mechanisms should be implemented to enable secure login and authorized access to portal information and services.
- j) Encryption and Confidentiality of sensitive information and data of users and portal information should be ensured.
- k) Appropriate mechanisms, protocols, and algorithms necessary to protect sensitive and confirmation data and information both during communication and storage should be implemented.
- l) Data security policies and standards to be used as per Government of India guidelines.
- m) In order to adequately provide access to secured information, security needs must be identified and developed at the data level. Database design must consider and incorporate data integrity requirements.
- n) Role based access for all the stake holders to be implemented to access and use the system.
- o) Ability to adopt other authentication mechanism such as Electronic Signature Certificates.
- p) Authorization validity to be ensured for the users providing the Data to the system. Data should be accepted only from the entity authorized.
- q) Audit trails and Audit logging mechanism to be built in the system to ensure that user action can be established and can be investigated if any can be aided (e.g. logging of IP address etc.)

- r) Data alterations etc. through unauthorized channel should be prevented.
- s) Industry good practice for coding of application so as to ensure sustenance, Application, Vulnerability and Assessment
- i. Build a complete audit trail of all activities and operations using log reports, so that errors in system – intentional or otherwise – can be traced and corrected.
- ii. Access controls must be provided to ensure that the system is not tampered or modified by the system operators.
- iii. The security of the field devices must be ensured with system architecture designed in a way to secure the field devices in terms of physical damage & unauthorized access.
- iv. The message exchange between various applications in the smart city should be fully encrypted and authenticated. Any application outside the Data Centre (DC) should talk to the applications hosted in the data center through predefined APIs only.
- v. APIs should be published and the IT systems be running on standard protocols like JSON / XML or REST etc.
- vi. From a network security perspective all information that flows on the network should be encrypted to ensure safety and privacy of confidential data. The devices at each endpoint of the network should be authenticated (using mechanisms based on attributes one of which could use passwords). The authentication system so used on these endpoint devices should ensure that only authorized users are sending data over the network, and there is no rogue data that is sent to the control systems to generate false alarms or sabotage the systems.
- vii. All IoT sensors deployed as part of Smart cities system should talk only to the authorized wireless network, and do not hook on to the rogue networks. The guidelines to secure Wi-Fi networks as published by Department of Telecom must be followed.
- viii. Wireless layer of the Smart City Network should be segmented for public and utility networks by using Virtual Private Networks (VPNs) or separate networks in the wired core, so that any traffic from the internet users is not routed into the sensor networks and vice-versa.
- ix. All traffic from the sensors in the Smart city to the application servers should be encrypted by Secure Socket Layer (SSL) and authenticated prior to sending any information. The data at rest and in transit must be encrypted.
- x. Authentication of sensors in the Smart city should happen at the time of provisioning the sensors, and adding them into the system, and should be based on physical characteristics of the sensors like MAC ID, Device ID etc.
- xi. Sensors deployed in solutions to set up Smart city should be hardened devices with the ability to be upgraded remotely for firmware through encrypted image files.
- xii. The Sensors or edge device deployed in Smart city should not have any physical interface for administration. Monitoring of systems and networks should be undertaken remotely.
- xiii. All the sensors in the Smart city should be connected to a completely separate network.
- xiv. As various sensors use multiple protocols to communicate with the underlying network with varied security capability, the system should allow provisioning necessary authentication and encryption at the gateway or the nearest data aggregation level if the sensor is not able to do the same.
- xv. Secured Information and Event Management system - monitoring of all Smart City networks,

devices and sensors to identify malicious traffic.

- xvi. Activities such as anti-spoofing (no one should be able to masquerade for inappropriate access), anti-sniffing (no one should be able get data and interpret it), anti-tampering (no one should be able to put/change data which was not meant to be put/changed) should be taken care for data in transit, as well as data at rest, from internal and external threats.

- t) **Sustainable & Scalable Solution-** 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 centre 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. The expectation is that the system should sustain at least 10 years from GO-Live. There must not be any system imposed restrictions on the upward scalability in number of field devices.

- u) **Availability** - Components of the architecture must provide redundancy and ensure that are no single point of failures in the key project components. Considering the high sensitivity of the system, design should 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. SI shall make the provision for high availability for all the services of the system. Redundancy has to be considered at the core / data center components level and offering system High Availability and failover. The solution should meet the minimum of following availability requirements:-
- i. Load Balanced across two or more Web Server avoiding single point of failure
 - ii. Deployment of multiple application instances should be possible
 - iii. Distributed or load balanced implementation of application to ensure that availability of services is not compromised at any failure instance.
 - iv. Network, DC and DR should be available as per required respective up time and SLA.
 - v. Comply with the published e-Governance standards, frameworks, policies and guidelines available on <http://egovstandards.gov.in> (updated from time-to-time)
 - vi. Provide analytic tools build into the system that shall support automatic detection of anomalies and their quick mitigation.
- v) **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 scalability of the system
- w) **Interoperability** - 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:

- i. comply with the published e-Governance standards, frameworks, policies and guidelines available on <http://egovstandards.gov.in> (updated from time-to-time); and
- ii. be of leading industry standards and as per standards mentioned at Annexures.

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 Command / viewing centers & Mobile Vans during post-implementation
- c) FMS staff for non- IT support during post-implementation

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 city and approved by the Authority before resource mobilisation.

Other Integrations:

- a) **Convergence** - PSCL has already initiated many projects which have state of the art infrastructure at field locations deployed under them. The ITMS Infrastructure should be made scalable for future convergence needs. Under the smart city program, PSCL has envisaged to create a state of the art infrastructure and services for the citizens of PSCL, hence it is imperative that all infrastructure created under the project shall be leveraged for maximum utilization. Hence 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 ITMS project at the field locations will be utilized to accommodate field equipment’s created under the other projects of PSCL. The procedure for utilization of the infrastructure will be mutually agreed between the PSCL and SI.

Sub-contracting / Outsourcing shall be allowed only for the work which is mentioned in the relevant clauses of Volume I of this RFP with prior written approval of PSCL. However, even if the work is sub-contracted / outsourced, the sole responsibility of the work shall lie with SI. SI shall be held responsible for any delay/error/non-compliance etc. of its sub-contracted vendor. The details of the sub-contracting agreements (if any) between both the parties would be required to be submitted to PSCL.

- b) **GIS Integration**- SI shall undertake detail assessment for integration of the Smart Governance, 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 Centers. 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.

- c) **SMS Gateway Integration-** SI shall carry out SMS 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.
- d) **Application Architecture**
- i. 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. The standards should (a) at least comply with the published e-Governance standards, frameworks, policies and guidelines available on <http://egovstandards.gov.in> (updated from time-to-time); and (b) be of leading industry standards and as per standards mentioned at Annexure –V.
 - ii. 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.
- SI shall design and develop the Smart City System as per the Functional and System requirement specifications.
- a) The Modules specified will be developed afresh based on approved requirement.
 - b) Apart from this, if some services are already developed/under development phase by the specific department, such services will be integrated with the Smart City System. These service will be processed through department specific Application in backend.
 - c) 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 have provision for uniform user experience across the multi lingual functionality covering following aspects:
 - i. Front end web portal in English and local language
 - ii. e-forms (Labels & Data entry in local languages). Data entry should be provided preferably using the Enhanced Inscript Standard (based on Unicode version 6.0 or later) keyboard layout with option for floating keyboard.
 - iii. Storage of entered data in local language using UNICODE (version 6.0 or later) encoding standard.
 - iv. Retrieval & display in local language across all user interfaces, forms and reports with all browsers compliant with Unicode version 6.0 and above.
 - v. Facility for bilingual printing (English and the local language)
 - d) 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:
 - i. Feature to use the master data for the auto-populating the forms and dropdowns
 - ii. Creation of application form, by “drag & drop” feature using meta data standards
 - Defining the workflow for the approval of the form

- First in First out
- Defining a citizen charter/delivery of service in a time bound manner
- iii. Creation of the “output” of the service, i.e. Certificate, Order etc.
- iv. Automatic reports
 - of compliance to citizen charter on delivery of services
 - delay reports
- e) 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.
- f) 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.
- g) The Smart City Application should have roadmap to integrate with key initiatives of State namely Portal Services, Citizen Contact Centre, Certifying Authority etc.
- h) Complete mobile enablement of the Smart City System.

3.1. Commencement of Works

Site Clearance obligations & other relevant permissions –

Prior to starting the site clearance, SI shall carry out survey of field locations as specified in RFP, for buildings, structures, fences, trees, existing installations, etc. The PSCL 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 PSCL before executing the plan.

3.2. Existing Traffic Signal System

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

3.3. Road Signs

All existing road signs which are likely to be affected by the works are to be carefully taken down and restored. Signs to be re-commissioned shall be cleaned, provided with new fixings

where necessary and the posts re-painted in accordance with PSCL guidelines. Road signs, street name plate, etc. damaged during their operation by SI shall be repaired or replaced by SI at no additional cost.

3.4. Electrical Works and Power Supply

SI shall directly interact with electricity board for provision of mains power supply at all desired locations for ITMS field solution. SI shall be responsible to submit the electricity bill including connection charge, meter charge, recurring charges etc. to the electricity board directly. SI shall have to submit the challan of bill submission to PSCL. Patna Municipal Corporation /PSCL will reimburse the amount submitted to SI after verification in next billing cycle.

3.5. Lightning-Proof Measures

SI shall comply with lightning-protection and anti –interference measures for system structure, equipment type selection, equipment earthing, power, signal cables laying. SI shall describe the planned lightning-protection and anti –interference measures in the As-Is report. Corresponding lightning arrester 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.

Earthing System

All electrical components are to be earthed 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 earthed through the cable glands. The entire applicable IT infrastructure i.e. signal junction or command centre shall have adequate earthing. Further, earthing should be done as per Local/State/National standard in relevance with IS standard.

- 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. PSCL shall provide the necessary space required to prepare the earthing pits. All metallic objects on the premises that are likely to be energized by electric currents should be effectively grounded.

There should be enough space between data and power cabling and there should not be any cross wiring of the two, in order to avoid any interference, or corruption of data.

The earth connections shall be properly made.

A complete copper mesh earthing grid needs to be installed for the server farm area, every rack need to be connected to this earthing grid. A separate earthing pit needs to be in place for this copper mesh.

Provide separate Earthing pits for Servers, & UPS as per the standards.

The metallic housing of electronic equipment/junction box/panel shall be connected to the earthing system.

The active electronic parts of an electronic equipment system shall be connected to the earthing system.

3.6. Junction Box, Poles and Cantilever

- a) SI shall provide the Junction Boxes, Posts and Cantilever to mount the field sensors, cameras, traffic sensors, traffic light aspects, active network components, controller and power backup (UPS/Alternate energy sources) at all field locations, as per the specifications given in the RFP.

Junction Box needs to be appropriately sized in-order to accommodate the systems envisaged at the Junctions, and SI should design the Junction box for 1.5 times the actual size required for utilization under the ITMS project.

Additional 50% space in the Junction Box shall be utilized by PSCL to accommodate any future requirements under other projects.

Junction Box for UPS with Battery bank needs to be considered separately. Bidder may propose solar based solutions to power the equipment. In this case, raw power can be used as backup supply whenever solar power is not able to meet the requirement.

It should be noted that SI would have designed the Junction box keeping in mind the scalability requirements of ITMS project, and the additional 50% volume needs to be considered over and above such requirement.

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.

3.7. Cabling Infrastructure

SI shall provide standardized cabling for all devices and subsystems.

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.

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. Cabling must be carried out per relevant BIS standards. All cabling shall be documented in a cable plan by SI.

3.8. Integrated Command& Control Centre (ICCC)

The vision of the Command and Control (ICCC) is to have an integrated view of all the smart initiatives undertaken by PSCL with the focus to serve as a decision support engine for city administrators in day-to-day operations or during exigency situations. ICCC involves leveraging on the information provided by various departments and providing a comprehensive response mechanism for the day-to-day challenges across the city. ICCC shall be a fully integrated solution that provides seamless traffic management, incident – response management, collaboration and geo-spatial display. 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. Following are the integration capabilities from this platform. The platform should be able to integrate with any type of sensor platform being used for the urban services irrespective of the technology used.

The platform should be able to normalize the data coming from different devices of same type (i.e. lighting sensors from different OEMs, energy meters from different OEMs etc.) and provide secure access to that data using data API(s) to application developers.

ICCC shall facilitate the viewing and controlling mechanism for the selected field locations in a fully automated environment for optimized monitoring, regulation and enforcement of services. The smart city operations center shall be accessible by operators and concerned authorized entities with necessary authentication credentials. Various smart elements are able to use the data and intelligence gathered from operations of other elements so that civic services are delivered lot more efficiently and in an informed fashion. ICCC should be able to integrate with various Utility systems such as Water/SCADA, Power, Gas, ITMS, Parking, Sewerage/ Drainage system, Disaster Mgmt. System etc.

SI has to integrate all smart components of the project at Command Control and Communication Centre with an integrated operations and dashboard application that will integrate various Smart City components implemented in this project and in future. As part of this RFP, SI shall ensure that redundancy and fault tolerance is considered at the ICCC components level in the actual deployment.

High Availability / Up Time Targets for ICCC operations are identified as follows:

- i. Availability Target (24Hr operation): 99.741%
- ii. Maximum Downtime Tolerated per Day: 6 minutes
- iii. Maximum Downtime Tolerated per Week: 42 minutes

3.9. Integrated City Operation Platform

3.9.1. Urban Services and Data APIs

- **Live data and visual feed** from diverse sensors should be connected to the platform

Normalized APIs: for listed domain (Parking, Outdoor Lighting, Traffic, Environment, Urban mobility etc.) to monitor, control sensor and/or actuators functionality

For example, Lighting APIs: Vendor agnostic APIs to control Lighting functionality

Cross APIs Integration: Enabling contextual information (API-API Bi-directional) and correlation across domains and verticals (Multiple vendor and Multi-sensor in future)

3.9.2. Platform Functionality

- **API management and gateway:** Provides secure API lifecycle, monitoring mechanism for available APIs

User and subscription management: Provides different tier of user categorization, authentication, authorization, and services based on the subscriptions

Application management: Provides role-based access view to applications

Enabling analytics: Time shifted and real-time data available for big data and analytics

Domain and/or Insight reports- Parking occupancy, energy reports, AQI report (environmental pollution)

3.10. GIS Mapping

GIS city map which shall be a common platform across all the solutions including City Wi-Fi, City Surveillance, Smart Lighting, solid waste management, Environmental sensor etc. across City/ Region of Interest. The GIS solutions shall also be responsible for appropriate geo referencing & geo tagging on the map covering all relevant assets like Surveillance Camera , Wi-Fi Hotspots, bin locations, street poles, Environmental sensor , Lighting etc.

GIS Maps Features

- b) GIS maps shall be comprehensive and detailed up to Complete Road Network, Building Foot Prints and Land use level. Solution shall ensure that the GIS Map provides complete Spatial and Attribute Information Pertaining to All the features of the city as various digital vector layers and allows for zoom in/out, searching, and retrieving information capabilities.

GIS system of City would provide the following details include the following data with attributes:

- i. Road Network
 - City Arterial Roads
 - Streets
- ii. Administrative boundaries
 - District and Sub District Boundary
 - Town and Ward Boundaries
- iii. Building footprints and names
- iv. Points of Interest data to include:
 - Health services (Hospitals, Blood Banks, and Diagnostics center, Ambulance Services, Other Medical Services, etc.)
 - Community services (fire stations, police stations, banks, ATMs, post offices, educational facilities, Govt. Buildings etc.)
 - Business Centres (Shopping malls, markets, commercial complexes etc.
 - Transportation (bus stops/Terminus, parking areas, petrol bunks, metro stations, seaports, airports, Railway Stations etc.)
 - Recreation facilities (Restaurants, theatres, auditoriums etc.)
 - Other utilities such as travel and tourism facilities, religious places, burial grounds, solid waste locations etc.
 - Local landmarks with locally called names.
- v. All data procured shall be imported into a central database.
- vi. System Functionalities:
 - The system shall have capability to perform attribute or spatial queries on data from selected sources.
 - The system shall support Android, IOS and Windows Mobile platform,
 - The system shall support server side Geo-processing
 - The application shall have standard and modern map navigation tools of pan and zoom.
- vii. The application shall support client requests to print the spatial data. The system shall be concurrent users.
 - The system shall support geocoding and reverse geocoding

- The system shall allow the users to perform advanced spatial analysis like geocoding, routing, buffering and attribute based analysis.
 - The application shall have standard and modern map navigation Tools
 - 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, ESRI File Geodatabase, Micro Station, AutoCADG/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 color fill.
 - The system shall allow the user to find Address/Location
 - 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.
- viii. Application shall be OGC compliant for database and shall provision conversion to other database formats.
- ix. GIS base maps shall be installed on work stations at Command control Centre and City Command and Control Center. GIS maps and data replication shall happen from central system remotely.

3.10.1. Video Analytics Usecases in the City

AI based Video Analytics usecases to be implemented on the surveillance CCTV cameras installed in the city. The advanced analytics system should be supported by continuous learning abilities. SI must implement the AI based video analytics on the GPU based servers in centralized architecture at datacenter.

The SI must provide AI based Video Analytics usecases as defined in the technical specifications to meet the requirements of the RFP focussing on the outcome, future scalability, security, reliability and adherence to SLAs and best practices in the industry.

4. Other Expectation and Consideration from MSI

4.1. Expectations from MSI/SI

- a) SI shall engage early in active consultations with the Authority, City Police and other key stakeholders to establish a clear and comprehensive project plan and understanding in line with the priorities of all project stakeholders and the project objectives.
- b) 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. Surveillance Infrastructure – CCTV Cameras, Data communication, monitoring, control room and Infrastructure
 - ii. Other Smart City initiatives envisaged
- c) 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.
- d) SI shall judiciously evaluate the resources and time planned for undertaking the current state assessment, given the overall timelines and milestones of the project.

- e) SI shall be responsible for supply of all the Products/equipment such as optical fiber cable, Network, 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.
- f) SI shall be responsible for supply of passive components indicated in the Bill of Materials section of the RFP viz. Housings, Fiber Patch Cords, Racks etc. Civil work required for the site shall be undertaken by the SI.
- g) Validate / Assess the re-use of the existing infrastructure if any within Authority site.
- h) Supply, Installation, and Commissioning of entire solution at all the locations.
- i) SI has to provide Enterprise version for all Open source software with support of 5 years mentioned in RFP. No community version will be accepted.
- j) SI shall provide the bandwidth required as standby arrangement for operationalizing each smart city critical locations initiative if the time extends due to any unforeseen reason and SI could not execute the fibre project within the time decided in the contract/agreement. The Authority's own fiber is laid by the SI is the part of the scope of work of this RFP. The bandwidth requirement shall be analyzed and procured by the SI at its own cost / risk.
- k) SI shall Install and commission connectivity across all designated locations.
- l) SI shall establish high availability, reliability and redundancy of the network elements to meet the Service Level requirements.
- m) 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 approved location.
- n) SI shall be responsible for up-gradation, enhancement and provisioning additional supplies of network (including active / passive components), hardware, software, etc. as requisitioned by Authority at additional cost as per the price mentioned in final LOA/Contract/PO for each item.
- o) SI shall ensure that the infrastructure provided under the project shall not have an end of life within 24 months from the date of bidding. However it is desired to have a life span of 7 years of each item quoted in RFP.
- p) SI shall ensure that the end of support is not reached during the concurrency of the contract and for 5 years thereafter.
- q) SI shall ensure compliance to all mandatory government regulations as amended from time to time.
- r) 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.
- s) 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.
- t) All the software licenses that the SI proposes shall be perpetual software licenses along with maintenance, upgrades and updates for the currency of the contract. 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.

- u) The SI shall ensure there is a 24x7 comprehensive onsite support for duration of the contract for respective components & services to meet SLA requirement. The SI shall ensure that all the OEMs have an understanding of the service levels required by Authority. However the ownership and accountability of service delivery for components lies with SI. SI is also required to provide the necessary MAF (Manufacturer Authorization Form) and undertaking as per the format provided in the RFP in support of for OEMs active support in the project along with SI.
- v) 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.
- w) SI shall be responsible for periodic updates & upgrades of all equipment, cabling and connectivity provided at all locations during the contract.
- x) Although, PSCL will facilitate to provide all Government approvals like, for Pollution Clearance, Fire Audit & Clearance, Right of Way, etc., but SI has to bear the cost/fees for the same (if any).
- y) SI shall be responsible for setting up / building / renovating the necessary physical infrastructure including provisioning for network, power, rack, etc. at all the locations.
- z) SI is expected to provide following services, including but not limited to:
 - i. Provisioning hardware and network components of the solution, in line with the proposed authority's requirements.
 - ii. 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.
 - iii. Size and provision the WAN bandwidth requirements across all locations considering the application performance, data transfer, DR and other requirements for smart city initiatives.
 - iv. Size and provision the internet connectivity for Service Provider network and Network Backbone.
 - v. Size and provision for bandwidth as a service for operations of CCTV surveillance till operationalization of network backbone.
 - vi. Liaise with service providers for commissioning and maintenance of the links.
 - vii. Furnish a schedule of delivery of all IT/Non-IT Infrastructure items.
 - viii. All equipment proposed as part of this RFP shall be rack mountable.
 - ix. Authority may at its sole discretion evaluate the hardware sizing document proposed by the SI. SI needs to provide necessary explanation for sizing to the Authority and same declaration will be submitted in the technical bid and will be demonstrated in technical bid & POC by SI at the time of Technical Presentation by SI..
 - x. Complete hardware sizing for the complete scope with provision for upgrade. The SI will provide the sizing as per 20% scalability in future. The undertaking for the scalability will be given by SI in the Technical Bid.

- xi. Specifying the number and configuration of the racks (size, power, etc.) that shall be required at all the locations. Every component installed in the field will have Patna Smart City Logo Printed.
- xii. The SI shall provide for all required features like support for multiple routing protocols, congestion management mechanisms and Quality of Service support.
- xiii. SI shall ensure that all networking 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.

4.2. Inception Phase

SI will be responsible for preparation of detailed project plan. The plan shall address at the minimum the following:

Define an organized set of activities for the project and identify the interdependence between them.

Resource planning and loading for each phase/activity. This must also indicate where each resource would be based during that phase, i.e. onsite at the PSCL office or off site at SI premises Establish and measure resource assignments and responsibilities Highlight the milestones and associated risks Communicate the project plan to stakeholders with meaningful reports Measure project deadlines and performance objectives

Project Progress Reporting. During the implementation of the project, SI should present weekly reports. This report will be presented in the Steering Committee meeting to PSCL. The report should contain at the minimum the under mentioned:

- Results accomplished during the period (weekly)
- Cumulative deviations from the schedule date as specified in the finalized Project Plan
- Corrective actions to be taken to return to planned schedule of progress
- Plan for the next week
- Proposed revision to planned schedule provided such revision is necessitated by reasons beyond the control of SI
- Support needed
- Highlights/lowlights
- Issues/Concerns
- Risks/Show stoppers along with mitigation

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

4.3. Requirement/Planning & Assessment Phase

SI must perform the detailed assessment of the business requirements and 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 PSCL and its representatives. While doing so, SI at least is expected to do following:

- a. SI shall conduct a detailed survey and prepare a gap analysis report, detailed survey report of the physical and field infrastructure requirements. SI shall duly assist the

department in preparing an action plan to address the gaps.

- b. SI shall study and revalidate the requirements given in the RFP with PSCL and submit as an exhaustive FRS document. SI shall develop the FRS and SRS documents.
- c. SI shall develop and follow standardized template for requirements capturing and system documentation.
- d. SI must maintain traceability matrix from SRS stage for the entire implementation.
- e. SI must get the sign off from user groups formed by PSCL.
- f. For all the discussion with PSCL team, SI shall be required to be present at PSCL office with the requisite team members.
- g. Prior to starting the site clearance, SI shall carry out survey of field locations for buildings, structures, fences, trees, existing installations, etc.
- h. 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 such as poles, cantilevers, cabling, aspects etc. should be reused to derive economies for the project with prior approval of PSCL. The dismantled infrastructure shall be delivered at the PSCL designated location without damage at no extra cost.
- i. All existing road signs which are likely to be effected 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 PSCL guidelines. Road signs, street name plate, etc. damaged by SI during their operation shall be repaired or replaced by SI at no additional cost.
- j. SI shall directly interact with electricity boards for provision of mains power supply at all desired locations for field solution. PSCL shall facilitate the same. The recurring electricity charges will be borne by PSCL as per actual consumption.

4.4. Design Phase

SI shall make a detailed Design document for proposed the solution as per the Design Considerations detailed in Section – 5,6,7,8 and all Annexures. Separate design for ICCC should be made based on both layouts as provided at Annexure – 2 & 3.

4.5. Implementation & Installation Phase

- Supply, Installation, Commission & Configure Cameras
- Obtain all necessary Legal/Statutory Clearance for Installing Poles & Junction Boxes
- Provisioning for Electricity
- Develop, Deploy, Test & Commission the surveillance system
- Supply, Install & Configure all User Level Components (Active & Passive)
- Installation of DC, DR IT Infrastructure
- Installation of Video wall, Workstations, LEDs, UPS, TV at ICCC, Police Area Offices, Railway Offices, SP Offices & DC
 - Project Implementation & Phase wise Planning
 - Information Security Policy, Backup Policies
 - Training to Officials
 - UAT and Phase Wise Go-Live

- Final Acceptance Test & GO Live
- Submission of System Documents, User Documents
- Project Commencement Documentation
 - Equipment Manual
 - Training Manual
 - Installation Manual
 - User Manual
 - System Manual
 - Standard Operational Procedure (SOP) Manual
- Testing Phase
 - Unit & Integration Testing
 - End to End Testing
 - User Acceptance Testing
 - Roll Out

4.6. Post Implementation Phase

- Helpdesk & Facilities Management Services in coordination with TSP (This will include operating manpower at all ICCC, Police Offices, Railway Offices, SP Offices)
- Review Mechanism in coordination with Authority of Patna Smart City
- Patch Management, Preventive Maintenance, Log Reports, System Hardening
- Preparing the report as per KPIs
- Handover of The system in coordination with Authority of Patna Smart City
- Exit Management Plan in coordination with Authority of Patna Smart City

4.7. Development & Software Customisation Phase

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, 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:

- a) Software Products (Configuration and Customization): Following needs to be adhered for the proposed software products:
 - i. SI will be responsible for supplying the application and licenses of related software products and installing the same so as to meet project requirements.
 - ii. SI shall have provision for procurement of licenses in a staggered manner as per the actual requirement of the project.
 - iii. 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. SI shall report any exceptions to license terms and conditions at the right time to PSCL. However, the responsibility of license compliance solely lies with SI. Any financial penalty imposed on PSCL during the contract period due to license non-compliance shall be borne by SI.
 - iv. As per requirement of complex solution implementation SI has to ensure that OEM owned/certified resources & SI best technical resources are deployed in this project.

- v. The OEM should provide the specific design (OEM Low Level Design, Core Implementation) support expertise to make sure that their supplied technology & products work as per the design objectives.
- vi. OEM to design and implement the complete security policy and workflow as per industry best practice in consultation with Customer to meet their Business requirements.
- vii. SI should provide the overall program management and OEM to ensure that the solution which may include multiple technologies from various OEM, to work together seamlessly as per the design goals. The seamless integration with all devices would be SIs responsibility for the respective products offered.
- viii. SI shall also supply any other tools & accessories required to make the integrated solution complete as per requirements. For the integrated solution, SI shall supply:
 - c) Software & licenses
 - d) Supply tools, accessories, documentation and provide a list of the same. Tools and accessories shall be part of the solution. System Documentation
 - e) 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 PSCL regularly :
 - i. Functional Requirement Specification (FRS)
 - ii. High level design of whole system
 - iii. Low Level design for whole system / Module design level
 - iv. System Requirements Specifications (SRS)
 - v. Any other explanatory notes about system
 - vi. Traceability matrix
 - vii. RACI Matrix
 - viii. Technical and product related manuals
 - ix. Installation guides
 - x. User manuals
 - xi. System administrator manuals
 - xii. Toolkit guides and troubleshooting guides
 - xiii. Other documents as prescribed by PSCL
 - xiv. Quality assurance procedures
 - xv. Change management histories
 - xvi. Version control data
 - xvii. SOPs, procedures, policies, processes, etc. developed for PSCL
 - xviii. Programs
 - 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 cases

(These documents need to be updated after each phase of project and to be maintained and updated during entire project duration. The entire documentation will be the property

of PSCL.)

4.8. Integration Phase (Existing Datasets & Other Applications)

The Command and control Centre should be integrated with feeds of all tracks/component deployed under this PSCL Project. 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 ICC will be intergarted with existing Datasets and applications implemented in other projects. PSCL will provide the SDK/API for all the existing softwares /applications which needs to be integrated. This will have a detailed study at the time of preparing the detailed scope of work and preparation of agreement between SI & PSCL. The testing should be comprehensive and should be done at each stage of development and implementation to enable city for better decision management and planning.

4.9. Pilot Deployment

- i. MSI shall conduct Pilot deployment and testing for meeting PSCL’s business requirements before rolling out the complete system. The pilot will be run for four weeks to study any issues arising out of the implementation. MSI shall also review health, usage and performance of the system till it is stabilized during pilot deployment. Based on PSCL’s feedback for incorporating changes as required and appropriate, MSI shall train staff involved in the Pilot implementation.
- ii. Pilot shall be demonstrated to the PSCL’s representatives. If for any reason the Pilot is found to be incomplete, these will be communicated to the MSI in writing on the lapses that need to be made good. A one-time extension will be provided to the MSI for making good on the lapses pointed out before offering the system to Client for review. Failure to successfully demonstrate the Pilot may lead to termination of the contract with no liability to Client.

4.10. Go-Live Preparedness and Go-Live

- a) SI shall prepare and agree with PSCL, the detailed plan for Go-Live (in-line with PSCL’s implementation plan as mentioned in RFP).
- b) SI shall define and agree with PSCL, the criteria for Go-Live.
- c) SI shall ensure that all the data migration is done from existing systems. (Storage Planning??)
- 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 PSCL team on the same.
- f) Go-live of the application shall be done as per the finalized and agreed upon Go-Live plan at the time of preparing the Agreement.

4.11. Handholding and Training

In order to strengthen the staff, structured capacity building programmes shall be undertaken for identified resources of PSCL, UD&HD and stakeholder departments. It is important to understand the training needs to be provided to each and every staff personnel of ICC. These officers shall be handling emergency situations with very minimal turnaround time. The actual number of trainees will be provided at design stage by PSCL and SI will give them the training. The documents/Training Material will be provided by SI. However the final Training of All the Officers and Users will be provided at the time before Go-Live of the project.

- a) SI shall prepare and submit detailed Training Plan and Training Manuals to PSCL 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 also be responsible for full capacity building. Training and capacity building shall be provided for all individual modules along with their respective integrations.
- d) SI shall be responsible for necessary demonstration environment setup including setup of cameras, sensors and application 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 ICC, DC, field locations etc. End user training shall be conducted at a centralized location or any other location as identified by PSCL with inputs from the SI.
- e) 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.
- f) SI shall impart operational and technical training to internal users on solutions being implemented to allow them to effectively and efficiently use the ICC system.
- g) SI shall prepare the solution specific training manuals and submit the same to PSCL for review and approval. Training Manuals, operation procedures, visual help-kit etc. The training material shall be provided in Hindi & English language.
- h) SI shall provide training to selected officers of the purchaser covering functional, technical aspects, usage and implementation of the products and solutions.
- i) 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. This will be mentioned in the agreement at the time of discussion of SOW.
- j) An annual training calendar shall be clearly chalked out and shared with the PSCL along with complete details of content of training, target audience for each year etc.
- k) SI shall update training manuals, procedures, manuals, deployment/installation guidelines etc. on a regular basis (Quarterly/ Biannual) to reflect the latest changes to the solutions implemented and new developments.
- l) SI shall ensure that training is a continuous process for the users. Basic intermediate and advanced application usage modules shall be identified by the SI.
- m) 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.
- n) Time Schedule and detailed program shall be prepared in consultation with PSCL and respective authorized entity. 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.

- o) SI is required to deploy a Master Trainer who shall be responsible for planning, designing and conducting continuous training sessions.
- p) The master trainer shall demonstrate a thorough knowledge of the material covered in the courses, familiarity with the training materials used in the courses, and the ability to effectively lead the staff in a classroom setting. If at any stage of training, the PSCL feels that on-field sessions are required, the same shall be conducted by the SI.
- q) If any trainer is considered unsuitable by PSCL, either before or during the training, SI shall provide a suitable replacement without disrupting the training plan.
- r) Training sessions and workshops shall comprise of presentations, demonstrations and hands-on mandatorily for the application modules.
- s) PSCL shall be responsible for identifying and nominating users for the training. However, SI shall be responsible for facilitating and coordinating this entire process.
- t) SI has to ensure that training sessions are effective and the attendees shall be able to carry on with their work efficiently. For this purpose, it is necessary that effectiveness of the training session is measured through a comprehensive feedback mechanism. SI shall be responsible for making the feedback available for the PSCL/authorized entity to review and track the progress, In case, after feedback, more than 40% 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:

- Functional Training
 - i. Basic IT skills
 - ii. Web portal, Mobile App, ITMS, environmental sensors, Video Analytics, ANPR, Smart Solutions etc.
 - iii. Software Applications (Command Control and Communication Centre)
 - iv. Networking, Hardware Installation
 - v. Centralized Helpdesk
 - vi. Feed monitoring

Administrative Training

- i. System Administration Helpdesk, BMS Administration etc.
- ii. Master trainer assistance and handling helpdesk requests etc.

Senior Management Training

- i. Usage of all the proposed systems for monitoring, tracking and reporting,
- ii. MIS reports, accessing various exception reports

Post-Implementation Training

- i. Refresher Trainings for senior officials
- ii. Functional/Operational training and IT basics for new operators
- iii. Refresher courses on System Administration

iv. Change Management programs

4.12. Operations and Maintenance

SI will operate and maintain all the components of the ICCC System for a period of five (5) years after Go-Live date. During O&M phase, SI shall ensure that service levels are monitored on continuous basis; service levels are met and are reported to PSCL. After Go-Live, if any system/sub-system/appliance that is deployed during the O&M phase must be added in the System only after proper induction procedures are followed including hardening and security testing. SI needs to implement suitable Performance Improvement Process (PIP) in the project.

PIP program applies to all the processes of ICCC project. SI need to submit its detailed approach for PIP in its technical proposal. Every process and procedure implemented in this project must be reviewed and updated by SI at least on annual basis from the Go-Live Date. All the manpower engaged for O&M support of the project should be citizens of India. SI will ensure that at no time shall any data of ICCC System be ported outside the geographical limits of the country. Some broad details of O&M activities are mentioned at later sections.

4.12.1. Applications Support and Maintenance

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

- Compliance to SLA

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

- Annual Technology Support

SI shall be responsible for arranging for annual technology support for the OEM products to PSCL provided by respective OEMs during the entire O&M phase.

- Application Software Maintenance

- SI shall provide unlimited support through onsite team/telephone/Fax/E-mail/Video Conferencing/installation visit as required
- SI shall address all the errors/bugs/gaps in the functionality in the solution implemented by the SI (vis-à-vis the FRS, BRS and SRS signed off) at no additional cost during the O&M phase.
- All patches and upgrades from OEMs shall be implemented by the SI ensuring customization done in the solution as per the PSCL's requirements are applied. Technical upgrade of the installation to the new version, as and when required, shall be done by the SI. Any version upgrade of the software / tool / appliance by

SI to be done after taking prior approval of PSCL and after submitting impact assessment of such upgrade.

- iv. Any changes/upgrades to the software performed during the support phase shall subject to the comprehensive and integrated testing by the SI to ensure that the changes implemented in the system meets the specified requirements and doesn't impact any other function of the system. Release management for application software will also require PSCL's approval. A detailed process in this regard will be finalized by SI in consultation with PSCL.
- v. Issue log for the errors and bugs identified in the solution and any change done in the solution shall be maintained by the SI and periodically submitted to the PSCL.
- vi. SI, at least on a monthly basis, will inform PSCL about any new updates/upgrades available for all software components of the solution along with a detailed action report.
- vii. In case of critical security patches/alerts, the SI shall inform about the same immediately along with his recommendations. The report shall contain SI's recommendations on update/upgrade, benefits, impact analysis etc. The SI shall need to execute updates/upgrades through formal change management process and update all documentations and Knowledge databases etc. For updates and upgrades, SI will carry it out free of cost by following defined process.

- **Problem identification and Resolution**

- i. Errors and bugs that persist for a long time, impact a wider range of users and is difficult to resolve becomes a problem. SI shall identify and resolve all the application problems in the identified solution (e.g. system malfunctions, performance problems and data corruption etc.).
- ii. Monthly report on problem identified and resolved would be submitted to PSCL along with the recommended resolution.

- **Change and Version Control**

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

- i. Detailed impact analysis
- ii. Change plan with Roll back plans
- iii. Appropriate communication on change required has taken place
- iv. Proper approvals have been received
- v. Schedules have been adjusted to minimize impact on the production environment
- vi. All associated documentations are updated post stabilization of the change

vii. Version control maintained for software changes

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

- Maintain configuration information

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

- Training

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

- Maintain System documentation

SI shall maintain at least the following minimum documents with respect to the ICCS System:

- i. High level design of whole system
- ii. Low Level design for whole system / Module design level
- iii. System Requirements Specifications (SRS)
- iv. Any other explanatory notes about system
- v. Traceability matrix
- vi. Compilation environment

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

- i. Source code is documented
- ii. Functional specifications are documented
- iii. Application documentation is updated to reflect on-going maintenance and
- iv. Enhancements including FRS and SRS, in accordance with the defined standards
- v. User manuals and training manuals are updated to reflect on-going
- vi. Changes/enhancements

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

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

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

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

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

Structure (WBS) basis in the proposal.

4.12.2. ICT Infrastructure Support and Maintenance

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

4.12.3. Warranty support

- SI shall provide comprehensive and on-site warranty for 5 years from the date of Go-Live for the infrastructure deployed on the project. SI need to have OEM support for these components and documentation in this regard need to be submitted to PSCL on annual basis.
- SI shall provide the comprehensive & onsite manufacturer's warranty in respect of proper design, quality and workmanship of all hardware, equipment, accessories etc. covered by the RFP. SI must warrant all hardware, equipment, accessories, spare parts, software etc. procured and implemented as per this RFP against any manufacturing defects during the warranty period.
- SI shall provide the performance warranty in respect of performance of the installed hardware and software to meet the performance requirements and service levels in the RFP.
- SI is responsible for sizing and procuring the necessary hardware and software licenses as per the performance requirements provided in the RFP. During the warranty period SI shall replace or augment or procure higher-level new equipment or additional licenses/hardware at no additional cost to the PSCL in case the procured hardware or software is not enough or is undersized to meet the service levels and the project requirements.
- During the warranty period SI shall maintain the systems and repair/replace at the installed site including all consumables, at no charge to PSCL, all defective components that are brought to the SI's notice.
- The SI shall carry out Preventive Maintenance (PM) of all hardware and testing for virus, if any, and should maintain proper records at each site for such PM. The PM should be carried out at least once in six months as per checklist and for components agreed with PSCL.
- The SI shall carry out Corrective Maintenance for maintenance/troubleshooting of supplied hardware/software and support infrastructure problem including network (active/passive) equipment, security and rectification of the same. The SI shall also maintain complete documentation of problems, isolation, cause and rectification procedures for building knowledge base for the known problems in centralized repository, accessible to PSCL team as well.
- SI shall monitor warranties to check adherence to preventive and repair maintenance terms and conditions.
- The SI shall ensure that the warranty complies with the agreed technical standards, security requirements, operating procedures, and recovery procedures.

- i. SI shall have to stock and provide adequate onsite and offsite spare parts and spare component to ensure that the uptime commitment as per SLA is met.
- ii. Any component that is reported to be down on a given date should be either fully repaired or replaced by temporary substitute (of equivalent configuration) within the time frame indicated in the Service Level Agreement (SLA).
- iii. The SI shall introduce a comprehensive Assets Management process & appropriate tool to manage the entire lifecycle of every component of ICCC system.

4.12.4. Maintenance of ICT Infrastructure at DC and ICCC

Management of DC and ICCC

SI need to deploy requisite mix of L1, L2 and L3 resources (on 24X7 basis) for management of entire ICCC System including ICT infrastructure deployed at DC and ICCC. All resources deployed in the project should be employees of SI and be Indian citizens. All the L1 and L2 resources proposed for the project need to be dedicated for the project. Any change in the team once deployed will require approval from PSCL. It is expected that resources have proven track record and reliability. Considering the criticality of the project, PSCL may ask for security verification (Police verification) of every resource deployed on the project and SI need to comply the same before deployment of the resource at the project. At all times, the SI need to maintain the details of resources deployed for the project to PSCL and keep the same updated. Detailed process in this regard will be finalized between PSCL and SI. The SI shall maintain an attendance register for the resources deployed. Attendance details of the resources deployed also need to be shared with PSCL on monthly basis. PSCL reserves the right to interview resources deployed for Operations and maintenance and assess the suitability of the resource for the role. In case a resource is not found suitable, SI will change the resource on request of PSCL. SI shall comply with this.

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

- i. DC operations to be in compliance with industry leading ITSM frameworks like ITIL, ISO
- ii. ISO 20000 & ISO 27001
- iii. Ensure compliance to relevant SLA's
- iv. 24x7 monitoring & management of availability & security of the infrastructure and assets
- v. Perform regular hardening, patch management, testing and installation of software updates issued by OEM/vendors from time to time after following agreed process
- vi. Ensure overall security – ensure installation and management of every security component at every layer including physical security
- vii. Prepare documentation/policies required for certifications included in the scope of work
- viii. Preventive maintenance plan for every quarter
- ix. Performance tuning of system as required
 - x. Design and maintain Policies and Standard Operating Procedures
 - xi. User access management
 - xii. Other activities as defined/to meet the project objectives
- xiii. Up-dation of all Documentation.

During operations phase the SI needs to submit proof of renewal of support for all IT infrastructure products and other system software's for whom it is mandated to have

OEM support.

This needs to be submitted on an annual basis and needs to be verified before release of 2nd quarter payment of each year.

System Maintenance and Management

- i. SI shall be responsible for tasks including but not limited to setting up servers, configuring and apportioning storage space, account management, performing periodic backup of data and automating reporting tasks, and executing hardware and software updates when necessary. It shall be noted that the activities performed by the SI may also be reviewed by PSCL.
- ii. SI shall provision skilled and experienced manpower resources to administer and manage the entire system at the Data Center.
- iii. On an ongoing basis, SI shall be responsible for troubleshooting issues in the IT infrastructure solution to determine the areas where fixes are required and ensuring resolution of the same.
- iv. SI shall be responsible for identification, diagnosis and resolution of problem areas pertaining to the IT Infrastructure and maintaining the defined SLA levels.
- v. SI shall implement and maintain standard operating procedures for the maintenance of the IT infrastructure based on the policies formulated in discussion with PSCL and based on the industry best practices/frameworks. SI shall also create and maintain adequate documentation/checklists for the same.
- vi. SI shall be responsible for managing the user names, roles and passwords of all the relevant subsystems, including, but not limited to servers, other devices, etc. SI shall be required to set up the directory server. Logs relating to access of system by administrators shall also be kept and shall be made available to PSCL on need basis.
- vii. SI shall implement a password change mechanism in accordance with the security policy formulated in discussion with PSCL and based on the industry best practices/frameworks like ISO 27001, ISO 20000 etc.
- viii. The administrators shall also be required to have experience in latest technologies so as to make provision for the existing and applicable infrastructure on a requirement based scenario.

System Administration

- i. 24*7*365 monitoring and management of the servers in the DC.
- ii. SI shall also ensure proper configuration of server parameters and performance tuning on regular basis. SI shall be the single point of accountability for all hardware maintenance and support the ICT infrastructure. It should be noted that the activities performed by the SI may be reviewed by PSCL.
- iii. SI shall be responsible for operating system administration, including but not limited to management of users, processes, preventive maintenance and management of upgrades including updates, upgrades and patches to ensure that the system is properly updated.
- iv. SI shall also be responsible for installation and re-installation of the hardware(s) as well as the software(s) in the event of system crash/failures.
- v. SI shall also be responsible for proactive monitoring of the applications hosted
- vi. SI shall appoint system administrators to regularly monitor and maintain a log of the monitoring of servers to ensure their availability to PSCL at all times.

- vii. PSCL shall undertake regular analysis of events and logs generated in all the sub systems including but not limited to servers, operating systems etc. The system administrators shall undertake actions in accordance with the results of the log analysis. The system administrators shall also ensure that the logs are backed up and truncated at regular intervals. SI shall refer to CERT-In Guidelines so as to ensure their alignment with the practices followed.
- viii. The system administrators shall adopt a defined process for change and configuration management in the areas including, but not limited to, changes in servers, operating system, applying patches, etc.
- ix. The system administrators shall provide hardening of servers in line with the defined security policies. Validation of hardening configuration will be carried out quarterly and deviations must be tracked through SLA reporting.
- x. The system administrators shall provide integration and user support on all supported servers, data storage systems etc.
- xi. The system administrators shall be required to trouble shoot problems with web services, application software, server relationship issues and overall aspects of a server environment like managing and monitoring server configuration, performance and activity of all servers.
- xii. The system administrators should be responsible for documentation regarding configuration of all servers, IT Infrastructure etc.
- xiii. The system administrators shall be responsible for managing the trouble tickets, diagnosis of the problems, reporting, managing escalation, and ensuring rectification of server problems as prescribed in Service Level Agreement.
- xiv. The administrators will also be required to have experience in latest technologies so as to provision the existing and applicable infrastructure on a requirement based scenario.

Storage Administration

- i. SI shall be responsible for the management of the storage solution including, but not limited to, storage management policy, configuration and management of disk array, SAN fabric/switches, tape library, etc. It should be noted that the activities performed by the SI may be reviewed by PSCL.
- ii. SI shall be responsible for storage management, including but not limited to management of space, SAN/NAS volumes, RAID configuration, LUN, zone, security, business continuity volumes, performance, etc.
- iii. The storage administrator will be required to identify parameters including but not limited to key resources in the storage solution, interconnects between key resources in the storage solution, health of key resources, connectivity and access rights to storage volumes and the zones being enforced in the storage solution.
- iv. The storage administrator will be required to create/delete, enable/disable zones in the storage solution.
- v. The storage administrator will be required to create/delete/modify storage volumes in the storage solution.
- vi. The storage administrator will be required to create/delete, enable/disable connectivity and access rights to storage volumes in the storage solution.
- vii. To facilitate scalability of solution wherever required.
- viii. The administrators will also be required to have experience in technologies such as virtualization and cloud computing so as to provision the existing and applicable infrastructure on a requirement based scenario.

Database Administration

- i. SI shall be responsible for monitoring database activity and performance, changing the database logical structure to embody the requirements of new and changed programs.
- ii. SI shall be responsible to perform physical administrative functions such as reorganizing the database to improve performance.
- iii. SI shall be responsible for tuning of the database, ensuring the integrity of the data and configuring the data dictionary.
- iv. SI will follow guidelines issued by PSCL in this regard from time to time including access of data base by system administrators and guidelines relating to security of data base.
- v. Database administration should follow the principle of segregation of duties to ensure no single DBA can update production tables/data singularly.
- vi. In addition to restrictions on any direct change in Data by any administrator, the Databases shall have Auditing features enabled to capture all activities of administrators.

Backup/Restore/Archival

- i. SI shall be responsible for implementation of backup & archival policies as finalized with PSCL. The SI is responsible for getting acquainted with the storage policies of PSCL before installation and configuration. It should be noted that the activities performed by the SI may be reviewed by PSCL.
- ii. SI shall be responsible for monitoring and enhancing the performance of scheduled backups, scheduled regular testing of backups and ensuring adherence to related retention policies.
- iii. SI shall be responsible for prompt execution of on-demand backups of volumes and files whenever required by PSCL or in case of upgrades and configuration changes to the system.
- iv. SI shall be responsible for real-time monitoring, log maintenance and reporting of backup status on a regular basis. SI shall appoint administrators to ensure prompt problem resolution in case of failures in the backup processes.
- v. SI shall undertake media management tasks, including, but not limited to, tagging, cross-referencing, storing, logging, testing, and vaulting in fire proof cabinets (onsite and offsite as per the detailed process finalized by during project implementation phase).
- vi. SI shall also provide a 24 x 7 support for file and volume restoration requests at the Data Centre.

Network monitoring

- i. SI shall provide services for management of network environment to maintain performance at optimum levels on a 24 x 7 basis. It should be noted that the activities performed by the SI may be reviewed by PSCL.
- ii. SI shall be responsible for creating and modifying VLAN, assignment of ports to appropriate applications and segmentation of traffic.
- iii. SI shall also be responsible for break fix maintenance of the LAN cabling within DC/ICCC etc.
- iv. SI shall also provide network related support and will coordinate with connectivity service providers of PSCL/other agencies who are terminating their network at the DC/ICCC for access of system.

Security Management

- i. Regular hardening and patch management of components of the ICCS System as agreed with PSCL
- ii. Performing security services on the components that are part of the PSCL environment as per security policy finalized with PSCL
- iii. IT Security Administration – Manage and monitor safety of information/data
- iv. Reporting security incidents and resolution of the same
- v. Proactively monitor, manage, maintain & administer all security devices and update engine, signatures, and patterns as applicable.
- vi. Managing and monitoring of anti-virus, anti-malware, phishing and malware for managed resources.
- vii. Ensuring 100 percent antivirus coverage with patterns not old more than period agreed on any given system
- viii. Reporting security incidents and co-ordinate resolution
- ix. Monitoring centralized pattern distribution (live update) and scan for deficiencies
- x. Maintaining secure domain policies
- xi. Secured IPsec/SSL/TLS based virtual private network (VPN) management
- xii. Performing firewall management and review of policies on at-least quarterly basis during first year of O&M and then after at-least on half-yearly basis
- xiii. Resolution of calls for security notifications, system alerts, vulnerabilities in hardware/software and alerting PSCL as appropriate
- xiv. Performing patch management using software distribution tool for all security applications including content management system, antivirus and VPN
- xv. Providing root cause analysis for all defined problems including hacking attempts
- xvi. Monthly reporting on security breaches and attempts plus the action taken to thwart the same and providing the same to PSCL
- xvii. Maintaining documentation of security component details including architecture diagram, policies and configurations
- xviii. Performing periodic review of security configurations for inconsistencies and redundancies against security policy
- xix. Performing periodic review of security policy and suggest improvements
- xx. Reviewing logs daily of significance such as abnormal traffic, unauthorized penetration attempts, any sign of potential vulnerability. Security alerts and responses. Proactive measures in the event a problem is detected
- xxi. Policy management (firewall users, rules, hosts, access controls, daily adaptations)
- xxii. Modifying security policy, routing table and protocols
- xxiii. Performing zone management (DMZ)
- xxiv. Sensitizing users to security issues through regular updates or alerts – periodic updates/Help PSCL issuance of mailers in this regard
- xxv. Performing capacity management of security resources to meet business needs
- xxvi. Rapidly resolving every incident/problem within mutually agreed timelines
- xxvii. Testing and implementation of patches and upgrades
- xxviii. Network/device hardening procedure as per security guidelines from PSCL
- xxix. Implementing and maintaining security rules
- xxx. Performing any other day-to-day administration and support activities

Other Activities

- i. SI shall ensure that it prepares configuration manual for OS, appliances, middleware, all tool, servers/devices and all equipment's and the same need to be submitted to PSCL, any changes in the configuration manual need to be approved by PSCL. Configuration manual to be updated periodically.
- ii. SI shall maintain data regarding entitlement for software upgrades, enhancements, refreshes, replacements and maintenance.
- iii. If the Operating System or additional copies of Operating System are required to be installed/reinstalled/un-installed, the same should be done as part of O&M.
- iv. SI should carry out any requisite adjustments/changes in the configuration for implementing different versions of Application Software.
- v. Updates/Upgrades/New releases/new versions: The SI shall provide from time to time the Updates/Upgrades/new releases/new versions of the software and operating systems as required. The SI should provide free upgrades, updates & patches of the software and tools to PSCL as and when released by OEM.
- vi. SI shall provide patches to the software as part of IT infrastructure, operating system, databases and other applications.
- vii. Software License Management: The SI shall provide for software license management and control. SI shall maintain data regarding entitlement for software updates, enhancements, refreshes, replacements, and maintenance.
- viii. Data backup/recovery management services
- ix. All other activities required to meet the project requirements and service levels.
- x. It is responsibility of the SI to scale up the Operations & Maintenance (O&M) team as and when required to ensure smooth project execution throughout the project duration.

4.12.5. Compliance to SLA

- SI shall ensure compliance to uptime and performance requirements of project solution as indicated in the SLA (as per Volume III of RFP) table of RFP and any upgrades/major changes to the ICCS System shall be accordingly planned by SI for ensuring the SLA requirements. SI shall be responsible for measurement of the SLAs at the ICCS System level as well as at the user level with the help of the enterprise monitoring tool on a periodic basis. Reports for SLA measurement must be produced PSCL officials as per the project requirements.

4.13. Compliance to Standards & Certifications

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, SI will ensure that the entire Project is developed in compliance with the applicable standards.

During project duration, SI will ensure adherence to prescribed standards as provided below:

Table 3: Standards & Certifications for Compliance

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 (wherever applicable) specifications for documentation

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

- i. The Information Technology Act, 2000 and amendments thereof and
- ii. Guidelines and advisories for information security published by CERT-In/MeitY (Government of India) issued till the date of publishing of tender notice. Periodic changes in these guidelines during project duration need to be complied with.

While writing the source code for application modules 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:

- i. The name of the module
- ii. The date when module was created
- iii. A description of what the module does
- iv. A list of the calling arguments, their types, and brief explanations of what they do
- v. A list of required files and/or database tables needed by the module
- vi. Error codes/Exceptions
- vii. Operating System (OS) specific assumptions
- viii. A list of locally defined variables, their types, and how they are used
- ix. Modification history indicating who made modifications, when the modifications were made, and what was done.

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

- i. Proper and consistent indentation
- ii. Inline comments
- iii. Structured programming
- iv. Meaningful variable names
- v. Appropriate spacing
- vi. Declaration of variable names
- vii. Meaningful error messages

Quality Audits

- i. PSCL, at its discretion, may also engage independent auditors to audit any/some/all standards/processes. SI shall support all such audits as per calendar agreed in advance. The result of the audit shall be shared with SI who has to provide an effective action plan for mitigations of observations/non-compliances, if any.
- ii. SI should comply with all the technical and functional specification provided in various sections in this RFP document.

4.14. 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. SI may propose further detailed Acceptance criteria which the PSCL will review. Once PSCL provides its approval, the Acceptance criteria can be finalized. In case required, parameters might be revised by PSCL 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.

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

Table 4 : Various Testing envisaged for the project

Type of Testing	Responsibility	Scope of Work
System Testing	✓ SI	<ul style="list-style-type: none"> ▪ SI to perform System testing ▪ SI to prepare test plan and test cases and maintain it. PSCL may request SI to share the test cases and results ▪ Should be performed through manual as well as automated methods ▪ Automation testing tools to be provided by SI. PSCL doesn't intend to own these tools
Integration Testing	✓ SI	<ul style="list-style-type: none"> ▪ SI to perform Integration testing ▪ SI to prepare and share with PSCL the Integration test plans and test cases ▪ SI to perform Integration testing as per the approved plan ▪ Integration testing to be performed through manual as well as automated methods ▪ Automation testing tools to be provided by SI
Performance and Load Testing	✓ SI ✓ PSCL/ Third Party Auditor(to monitor the performance testing)	<ul style="list-style-type: none"> ▪ SI to do performance and load testing. ▪ Various performance parameters such as transaction response time, throughput, and page loading time should be taken into account. ▪ Load and stress testing of the Project to be performed on business transaction volume ▪ Test cases and test results to be shared with PSCL ▪ Performance testing to be carried out in the exact same architecture that would be set up for production

Type of Testing	Responsibility	Scope of Work
		<ul style="list-style-type: none"> SI need to use performance and load testing tool at the time of Go-Live and at the end of every 6 months during O&M Phase. PSCL if required, could involve third party auditors to monitor/validate the performance testing. Cost for such audits to be paid by PSCL
Security Testing (including Penetration and Vulnerability testing)	✓ SI ✓ PSCL/ Third Party Auditor (to monitor the security testing)	<ul style="list-style-type: none"> 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, datacenter, security monitoring system deployed by SI. Solution shall pass vulnerability and penetration testing for roll out 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. SI should carry out security and vulnerability testing on the developed solution. Security testing to be carried out in the exact same environment/architecture that would be setup for production. Security test report and test cases should be shared with PSCL Testing tools if required, to be provided by SI. During O&M phase, penetration testing to be conducted on yearly basis and vulnerability assessment to be conducted on half-yearly basis. PSCL 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 PSCL
User Acceptance Testing of Project	✓ PSCL or PSCL appointed third party auditor	<ul style="list-style-type: none"> PSCL/PSCL appointed third party audit or to perform User Acceptance Testing SI to prepare User Acceptance Testing test cases UAT to be carried out in the exact same environment/architecture that would be set up for production SI should fix bugs and issues raised during UAT and get approval on the fixes from PSCL/third party auditor before production deployment Changes in the application as an outcome of UAT shall not be considered as Change Request. SI has to rectify the observations.

Note:

- 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. PSCL does not intend to own the tools.
- SI shall work in a manner to satisfy all the testing requirements and adhere to the

testing strategy outlined. SI must ensure deployment of necessary resources and tools during the testing phases. 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 SI meets all the requirements specified in the RFP. SI shall take remedial action based on outcome of the tests.

- c. 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 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 PSCL directly. All tools/environment required for testing shall be provided by SI.
- e. STQC/Other agencies appointed by PSCL 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 SI.

4.15. Factory Testing & Pre-Despatch Inspection

- a) Successful SI shall have to submit Factory Test Certificate for all the ICC, DC & ICT Equipment (Active & Passive) before the actual supply of the items. SI has to provide MAF (OEM warranty certificate) for all the ICC, DC & ICT Active Equipment.
- b) Pre-Despatch Inspection by PSCL shall be necessary and accordingly, PSCL reserve all the right to visit the OEM premises of all the ICC, DC & ICT Active Equipment through the Technical team at the cost of SI. All the supply for the approved quantity will happen after clearance of such Technical team of PSCL.
- c) Technical Committee may get the 72 hours Burn-in test of all the Desktops, Workstations, Servers and its associated accessories before recommending release of payment.

4.16. Final Acceptance Testing

The final acceptance shall cover 100% of the PSCL Project, after successful testing by the PSCL; a Final Acceptance Test Certificate (FAT) shall be issued by the PSCL to SI.

Prerequisite for Carrying out FAT activity:

- a) Detailed test plan shall be developed by SI and approved by PSCL. This shall be submitted by SI before FAT activity to be carried out.
All documentation related to PSCL Project and relevant acceptance test document (including IT Components, Non IT Components etc.) should be completed & submitted before the final acceptance test to the PSCL.
The training requirements as mentioned should be completed before the final acceptance test.
Successful hosting of Application, NMS and MIS Software.

For both IT & Non-IT equipment's / software manuals / brochures / Data Sheets / CD / DVD / media for all the PSCL Project supplied components.

The FAT shall include the following:

- a) All hardware and software items must be installed at respective sites as per the specification.

Availability of all the defined services shall be verified.

SI shall be required to demonstrate all the features / facilities / functionalities as mentioned in the RFP.

SI shall arrange the test equipment required for performance verification, and will also provide documented test results.

SI shall be responsible for the security audit of the established system to be carried out by a certified third party as agreed by PSCL.

Any delay by 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 PSCL and SI. In the event SI is not able to complete the installation due to non-availability of bandwidth from the bandwidth service providers, the Supplier and PSCL may mutually agree to redefine the Network so that SI can complete installation and conduct the Final Acceptance Test within the specified time.

5. Detailed Scope of Work with Specifications

5.1. Integrated Command Control & Communication Centre (ICCC)

It is envisaged that the city will implement multiple Smart City use cases over a period of time. The potential example Smart City use cases are-

- a) Smart Parking
 - b) Smart Traffic Management
 - c) Public Safety and Safe City Operations
 - d) Connected Public Transport
 - e) Environmental monitoring
 - f) Smart Waste Management
- Integrated Command and Control Centre of Patna Smart City will be primary command centre acting as a HUB which will get the feed from all the above and other CCC at the Districts which would be integrated in full/partial as per the requirements of the district CCCs.
 - The ICCC should be scalable and should be able to integrate all the ULBs of the State of Bihar as and when required.

5.1.1. Functional & Technical Requirements for ICCC Platform

S. No	Technical Specification
A	General
1.	The Unified Command & Control Platform (UC&C) shall be an enterprise class IP-enabled Cloud ready application for future scalability purpose. The UC&C shall support the seamless unification of various Public Safety elements IP video management system (VMS), IP automatic number plate recognition system (ALPR), Incident management, Emergency response system. Criminal tracking, record management with future scalability to include Traffic management solutions also under a single platform. The UC&C user interface (UI) applications shall present a unified security interface for the management, configuration, monitoring, co - relation, intelligence and reporting of various embedded systems and associated devices.
2.	The platform must have native failover with no dependency on external virtualized or clustered applications. The failover must support both local & over geographical redundancy for all the modules outlined under the UC & C platform.
4.	The UC&C platform must be a true unified management experience for critical infrastructure, simplifying control room operation and system integration, minimizing total cost of ownership, and increasing operational efficiency critical to rapid decision-making.

5.	The UC&C Platform Shall Maximize real-time monitoring and control efficiency from one workstation through the synchronized control of high-resolution images, streaming video data, and system alerts which allows for interaction between all relevant data
6.	Allows simple and accessible Integration with other independent control systems through a single Unification point with consistent user interface and better operational efficiency.
7.	UC&C shall be open architecture based, highly scalable and able to integrate multiple disparate systems seamlessly on a common platform
8.	UC&C system shall provide a real time Common Operating Picture (UC&C) of the area involving all agencies using a simple Operator / User friendly interface.
9.	The system shall support various sensors like Cameras, GPS, Voice devices, Storage devices, Sensor inputs from other Utility applications/ systems
10.	The UC&C platform shall provide a dashboard functionality to manage workflows by integrating information from different agencies and systems to facilitate responsive decision making in City.
11.	The UC&C platform should provide a cross-agency collaboration tool to support instant communication between various user groups and authorities.
12.	The ICCC software should have biometric authentication facility for operators using the software.
B	UC&C Architecture:
	The Application shall be an IP enabled solution. All communication between the servers and other clients shall be based on standard TCP/IP protocol and shall use TLS encryption with digital certificates to secure the communication channel.
2	The Application shall protect against potential database server failure and continue to run through standard off-the-shelf solutions.
3	The Application shall support up to one thousand instances of Clients connected at the same time. However, an unrestricted number of Clients can be installed at any time
4	The Application shall support an unrestricted number of logs and historical transactions (events and alarms) with the maximum allowed being limited by the amount of hard disk space available.
5	The UC&C Application shall support native and off-the-shelf failover options without any dependency on external application for both Hardware and Application level fail over.

C	Native Map module (Both GIS and Offline Maps): Note : Maps and layers will be provided by PSCL. Enterprise GIS for Web GIS with Geo Analytics (Only for adding layers) is envisaged as the current scope of this RFP.
1	The GIS MAP shall support the following file format PDF, JPG, PNG Web Map Service (WMS) defined by the Open Geospatial Consortium (OGC).
2	It shall be possible to configure a mixed set of maps made of GIS, online providers and private imported files and link them together.
3	The UC&C shall provide a map centric interface with the ability to Command & Control all the system capabilities from a full screen map interface.
4	It shall be possible to span the map over all screens of the UC&C client station. In the scenario where the map is spanned over all the screens of the UC&C client station it shall be possible to navigate the map including pan and zoom, and the map's moves shall be synchronized between all screens. Spanning the map over multiple screens must provide the same Command & Control capabilities than in a single screen display.
5	The GIS MAP shall provide the ability to display layer of information in Keyhole Mark-up Language (KML) format.
6	It shall be possible to monitor the state of entities on the map. It shall be possible to customize the icons of any entities represented on the map.
7	It shall be possible to select a location by drawing a zone of interest on the GIS MAP, and to display all the entities that are part of that zone of interest at once.
8	The user shall be able to select and display the content of multiple UC&C entities on the map in popup windows.
9	The GIS MAP shall provide the following search capabilities:
a.	Search within the map by entity name, street name, or point of interest.
b.	Drag and drop entities from the UC&C to the map to center their location.
c.	Map to support event-based response actions for decision making in case of any emergency / critical situation
d.	CCTV feeds to be viewed on the Map in case of any event triggers
D	Alarm management:
1	The UC&C shall support the following Alarm Management functionality:

2	Create and modify user-defined alarms. An unrestricted number of user-defined alarms shall be supported.
3	Assign a time schedule or a coverage period to an alarm. An alarm shall be triggered only if it is a valid alarm for the current period.
4	Set the priority level of an alarm and its reactivation threshold.
5	Define whether to display live or recorded video, still frames or a mix once the alarm is triggered.
6	Provide the ability to display live and recorded video within the same video tile using picture-in-picture (PiP) mode.
7	Provide the ability to group alarms by source and by type.
8	Define the recipients of an alarm. Alarm notifications shall be routed to one or more recipients. Recipients shall be assigned a priority level that prioritizes the order of reception of an alarm.
9	The workflows to create, modify, add instructions and procedures, and acknowledge an alarm shall be consistent for various systems.
10	The UC&C shall also support alarm notification to an email address or any device using the SMTP protocol.
11	The ability to create alarm-related instructions shall be supported through the display of one or more HTML pages following an alarm event. The HTML pages shall be user-defined and can be interlinked.
12	The user shall can acknowledge alarms, create an incident upon alarm acknowledgement, and put an alarm to snooze.
13	The user shall be able to spontaneously trigger alarms based on something he or she sees in the UC&C system Dashboard.
14	UC&C platform should generate Notification, Alert and Alarm messages as per the incidences / events that are received, that should be visible within the Dashboard and the Field Responder Mobile App or web services/portal if required
15	1. All system messages (notifications, alerts and alarms) should always be available from the Notifications View, which provides controls that operator can use to sort and filter the messages that it displays
16	2. ICCP platform should support to deliver message to a set of subscribers. The Notification service should support min two types of notification methods: a. Email notification b. Short Messaging Service (SMS) notification

E	Incident management (IM) module:
1	The IM MODULE shall be seamlessly embedded and must be a native module in the UC&C Platform.
2	The UC&C and IM MODULE shall be forward compatible so upgrade of one does not prevent from using the other.
3	The IM MODULE shall be seamlessly compatible with the UC&C and any of its components including VMS, ALPR, Big Data Co relation tool and external SDK integrations with 3rd party systems.
4	The IM MODULE shall offer the following native operational tools: <ul style="list-style-type: none"> a. Incident management b. Document management c. Rules Engine d. Workflow automation e. Standard operating procedures f. Incident monitoring operator interface g. Incident reports
5	The IM MODULE shall provide situational intelligence to the operator with a map-centric approach and detailed overview of incident data, combining incident history, operator comments, workflow and operator action logs, standard operating procedures, relevant live and playback video, and an aggregated events sequence of the incident.
6	The IM MODULE shall log all configuration changes in an audit trail with before and after configurations.
7	The IM MODULE shall log all the user activities that are executed during the time that an incident is active.
8	The IM MODULE shall provide the ability to configure incidents in a test mode that would allow user with the appropriate privilege to validate different parameters before activating the incident configuration.
9	The IM MODULE shall be the interface that displays all situations as incidents.

10	The IM MODULE Incident management shall provide the ability to trigger incidents manually or automatically, based on a correlation of events.
11	The Incident management shall provide management of incident ownership. It shall be possible to explicitly request or release the ownership of an incident. Ownership of an incident shall be provided immediately to an operator who starts working on an incident.
13	A supervisor shall be able to view all incidents that are under his supervision and see the ownership of each incident. In the same view, the supervisor shall also be provided with real-time information about who is currently monitoring an incident.
14	The IM MODULE shall notify the supervisor when an operator skips a step in the standard operating procedure (SOP).
15	<p>For each incident, it shall be possible to open the incident details. The incident details will open on a configurable screen and provide, based on the incident type configuration, the following information:</p> <p>A layout of all live and playback video related to the incident, including the camera associated to the source and location of the incident, as well as the local map centered on the incident location.</p> <p>History of the incident including:</p> <ol style="list-style-type: none"> All events related to the incident System workflow activities Operator actions for the incident Comments about the incident
16	<p>Operators shall be able to perform the following actions:</p> <ol style="list-style-type: none"> Change the incident state. Forward the incident. Transfer the incident. Edit the incident: <ol style="list-style-type: none"> Change the description Change the priority level Release the ownership Attach additional entities to the incident. Link related incidents. Attach a document as a URL link to the incident.

	8. Link the flagged incident data.
17	The IM MODULE shall provide the ability to dispatch an incident to a user or group of users. Dispatching an incident to a restricted number of users will secure the access to information.
18	The IM MODULE shall allow the distribution of specific tasks (managed as sub-incidents) that are associated to a unique incident, to different teams. Procedures can be performed in parallel.
19	Incident supervisors shall be able to see all sub-incidents associated with a main incident.
20	The IM MODULE shall offer a task to manage and generate reports. The ability to run a report is a user privilege.
21	It shall be possible to query the incident history filtering by: <ul style="list-style-type: none"> a. Incident type b. Incident state c. Location d. Priority e. Trigger time range f. Incident owner d. Description
22	The result of a report query shall provide a list of incidents as well as a visual of these incident locations on the map. When more than one incident is reported at the location, the GUI will cluster these incidents on the map.
23	For closed incidents, the incident shall be in read-only mode with the exception of adding links to related incidents.
24	The Report task shall also report the user activity log of the UC&C for the time in which the operator was owner of the incident and was monitoring it, in order to provide a view of all actions taken towards the resolution of this incident.
25	The IM MODULE shall offer all reports in a visual presentation format (such as pie charts, lines, columns, and rows) native within the platform with no necessary for additional external tools or software modules.
26	The IM MODULE shall support the following report formats: <ul style="list-style-type: none"> a. HTML b. PDF

	c. XML etc.
27	The IM must have native document management tool and UC&C platform shall provide the ability to dynamically index documents to an incident in order to improve the efficiency of access to information for an operator.
28	A document shall be automatically attached to an incident if the document properties match the incident properties. The following properties shall be available: <ul style="list-style-type: none"> a. Incident type b. Schedule c. Location. Location can be an entity or an area. d. User or user group of the operator monitoring the incident.
29	The IM MODULE shall offer the ability to automatically link a document to a step in a standard operating procedure.
30	Document Management shall provide a file system to store all documents as well as the document URLs for the use of third-party file systems.
31	The Incident Management module should have facility to configure a sequence of events using logical AND /OR /NOT operators to trigger and incident.
32	Configuring the Rules Engine shall be graphical without need for a script.
33	It shall be possible to configure a complex sequence of rules by applying the occurrence, the interval, and event filtering.
34	It shall also be possible to script the rules in advance and import them into the system later.
35	The IM Module shall provide a native Workflow Engine to automate the response to an incident type.
36	The IM Module shall provide a graphical workflow designer. No scripting competence shall be required to implement a workflow.
37	It shall be possible to define a workflow for each incident type. The workflow shall be a series of activities that are sequentially executed.
38	The IM Workflow Engine tool shall provide a framework to create custom activities that allow integration into a global business process.
39	The IM Module shall provide guidance for operators in the form of a standard operating procedure (SOP) for the response to an incident type.

40	The SOP shall be interactive and offer an operator-acknowledgement- audit for each SOP Step
41	The SOP shall be dynamic and provide the ability to adapt the next steps in a procedure based on the responses to previous steps in the procedure.
42	The IM Module shall provide the ability to skip a step of the SOP and request a justification for skipping the step.
43	Each step shall be optionally associated to a document in the form of a URL, or a document in a supported format (such as Word, PDF, or HTML).
44	The tool shall track the elapsed time for each step of the SOP, as well as the total elapsed time from the initial response to resolution and enable the authorities to determine the steps which are getting delayed and plan the training needs for the crime analysts and UC & C operators.
45	The IM MODULE shall provide the ability to configure standard options when defining dynamic steps of the SOP.
46	A maximum delay shall be allowed for a user to initiate the procedure. Automated actions associated with this time to response threshold shall be configurable.
47	A minimum time shall be allocated for a user to complete the procedure. Closing the incident before passing this time to resolution threshold shall trigger automated actions.
48	A visual indicator shall be displayed when maximum time to response or the maximum time to resolution for the incident is exceeded.
F	Big Data and Co Relation Tool (BDCR)
1	The UC & C platform either native or through external module must have the below big data mining and Co Relation tools
2	The BDCR must have a native Correlation engine which can assesses both temporal and geospatial data from multiple data sets like CCTNS, Court management, Dial 112 / emergency call system, Video Analytics, VMS, ANPR systems, GIS, Vehicle location systems, FRS and any other public safety or crime intelligence tools.
3	The crime analyst or the operator in the Command Center through the UC & C module should be able to query data specific to incidents and gather all the meaningful information related to incident from discreet data sets through the native Correlation tool.
4	The tool must generate correlation data for specific incident based on specific Query or Geospatial location-based analysis.
5	The tool must provide relevant information during any incident Based on geospatial and temporal criteria, by detecting and displaying all relevant

	information from cameras, people, vehicles, and events that would be interest to specific incident or crime and also needs immediate attention.
6	<p>The tool must support native following Crime analytics and Insights module for proactive policing, Authority may want to activate this module on need basis when the needed technology platforms like centralized data lake etc. are available – Prediction can happen for the following entities (indicative)</p> <p>Crimes - Using historical crime data, determining when certain areas will be more vulnerable, identifying geographical features.</p> <p>Offenders - Criminal groups, Criminal profiles, juvenile offenders likely to become major criminals.</p> <p>Perpetrator identities - Patterns in crimes done by the offender, profiling the kind of weaponry he keeps</p> <p>Point in time Analysis on areas like resource invested Vs Crimes going down in specific areas / Police Area Offices, Railway Offices, SP-Offices.</p> <p>Crime victims - Identifying groups likely to be hurt (religious targets), people at risk of domestic violence, etc.</p> <p>Time and Geography - Patterns in the area which is likely to experience unrest and time of the day, week or year within which a particular geography should be kept in check.</p>
G	Reporting:
1	The UC&C shall support report generation (database reporting) for various systems Unified into the platform access control, ALPR, video, and intrusion.
2	The workflows to create, modify, and run a report shall be consistent for all systems.
3	The UC&C shall support the following types of reports:
4	Alarm reports.
a.	Video-specific reports (archive, bookmark, motion, and more).
b.	Configuration reports
c.	ALPR-specific reports (mobile ALPR playback, hits, plate reads, reads/hits per day, reads/hits per ALPR zone, and more).
d.	System Health activity and health statistics reports for proactive maintenance.
e.	Generic Reports, Custom Reports and Report Templates

f.	The user shall be able to customize the predefined reports and save them as new report templates. There shall be no need for an external reporting tool to create custom reports and report templates. Customization options shall include setting filters, report lengths, and timeout period. The user shall also be able to set which columns shall be visible in a report. The sorting of reported data shall be available by clicking on the appropriate column and selecting a sort order (ascending or descending).
11	The UC&C shall support comprehensive data filtering for most reports based on entity type, event type, event timestamp, custom fields, and more.
12	The user shall be able to click on an entity within an existing report to generate additional reports from the Monitoring UI.
13	The UC&C shall support the following actions on a report: print report, export report to a PDF/Microsoft Excel/CSV file, and automatically email a report based on a schedule and a list of one or more recipients.
14	Reporting function is part of Command & Control dashboard visualization tool. It shall provide information about status of the Command & Control on managing the security incidents across the locations. Reporting function should enable operator to create reports in either graphical format or flat tabular format. Reports shall be created automatically or manually by operator whenever required. The reports should be generated and exported as a Microsoft word excel format or an acrobat format by operator.
15	It shall be possible to generate a report from UC & C interface based on the profiles defined for the Incident management and associated tools defined with in IM Module. a. The profile report shall be exportable and printable. b. Profile reports shall allow filtering on profile identifier, initiators, recipient, and modification time. c. Columns for the profile reports shall be configurable.
G	Real Time Dashboard:
1	Real time dashboard should provide the real-time information about the security situation so called Situational Awareness for the Authorities and senior officials in a single go.
2	The Monitoring UI shall dynamically adapt to what the operator is doing. This shall be accomplished through the concept of widgets that are grouped in the Monitoring UI dashboard.
3	Widgets shall be mini-applications or mini-groupings in the Monitoring UI dashboard that let the operator perform common tasks and provide them with

	fast access to information and actions. ICCC software should have drag and drop facility for all widgets for user to move the required alerts and other windows on priority basis.
4	Analysts / Operators shall be allowed to view dashboards if they are granted the appropriate privilege. Modification to the dashboards should also be allowed to users granted the appropriate privilege.
5	Dashboard widget types shall be: Image: provides the ability to display an image (JPG, PNG, GIF, and BMP) on a dashboard. Text: provides the ability to display a text on a dashboard. The text style shall be configurable, so font, size, colour, and alignment can be specified by the user. Tile: provides the ability to display any entity of the USP inside of a tile. Web page: provides the ability to display a URL on a dashboard. Entity Count: provides the ability to display the total number of a specific entity type in the UC&C.
	f. Reports: provides the ability to display the results of any saved reports in the system. The results shall be displayed either by showing the total number of results in the report, a set of top results from the report, or a visual graph from the data returned by the report.
6	It shall be possible to extend the widgets of a dashboard using the SDK. This will provide the ability to develop custom widgets to the system.
H	Threat Level Indication:
1	UC&C should display the threat level based on the number of alerts and criticality of the alerts using color coded display. It should also follow a pre-defined system to alert different users on different hierarchy based on the criticality of alerts. It should be possible to activate various threat situations from Web / Mobile client application for those users with appropriate privileges.
I	Incident Management & Reporting:
1	The UC&C shall support the configuration and management of events. A user shall be able to add, delete, or modify an action tied to an event if he has the appropriate privileges.
2	The UC&C shall receive all incoming events from one or more Unified Systems. The UC&C shall take the appropriate actions based on user- define event/action relationships.

3	Incident reports shall allow the security operator to create reports on incidents that occurred during a shift. Both video-related and other Unified Systems related incident reports shall be supported.
4	The operator shall be able to create standalone incident reports or incident reports tied to alarms.
5	The operator shall be able to link multiple video sequences to an incident, access them in an incident report.
6	It shall be possible to create a list of Incident categories, tag a category to an incident, and filter the search with the category as a parameter.
7	Incident reports shall allow the creation of a custom form on which to input information on an incident.
8	Incident reports shall allow entities, events, and alarms to be added to support at the report's conclusions.
9	Incidents reports shall have facility for generating escalation matrix for alerts and incidents.
J	Configuration User Interface:
1	The Configuration UI application shall allow the administrator or users with appropriate privileges to change the system configuration.
2	The configuration of all embedded systems shall be accessible via the Configuration UI.
3	The Configuration UI shall have a home page with single-click access to various tasks.
4	The Configuration UI shall include a variety of tools such as troubleshooting utilities, import tools, and a unit discover tool, amongst many more.
5	The Configuration UI shall include a static reporting interface to:
6	View historical events based on entity activity. The user shall be able to perform such actions as printing a report and troubleshooting a specific access event from the reporting view.
7	View audit trails that show a history of user/administrator changes to an entity.
8	Common entities such as users, schedules, alarms and many more, can be reused by all embedded systems in platform.
9	The application must have single user unified interface for configurations of all the systems of Video, ANPR and Emergency response.

10	There should not be any limitation on the number of end client licenses for the UC & C application for web based UI
K	Smartphone and Tablet App General Requirements:
1	The UC&C shall support mobile apps for various off-the-shelf smartphones and tablets. The mobile apps shall communicate with the Mobile Server of the UC&C over any WIFI or mobile network connection.
2	All the communication between the mobile apps and UC&C platform will be on HTTP and by adding TLS encryption on https.
L	Mobile app Functionalities:
1	<p>Ability to logon/logoff the UPS using an authorized use profile of the system.</p> <p>Ability to change the picture or the password of the user of the mobile app.</p> <p>Ability to view the current Threat Level of the system. Ability to change the current Threat Level of the system. Ability to execute hot actions configured in the user profile.</p> <p>Ability to view below minimum devices Unified with the UC&C platform:</p> <p>Cameras</p> <p>ii. ALPR cameras</p> <p>iii. GIS and Offline Maps</p> <p>iv. Ability to navigate the system hierarchical view of the devices & entities with ability to search entities in the system.</p>
2	It shall be possible to download the mobile apps from the Central application store (Apple iTunes App Store,/Google Play).
M	System Health Monitor:
1	The UC&C shall monitor the health of the system, log health-related events, and calculate statistics.
2	Detailed system care statistics will be available through a web-based dashboard providing health metrics of UC&C entities and roles, including Uptime and mean-time-between- failures.
3	Health events shall be accessible via the API SDK (can be used to create SNMP traps with external EMS / NMS systems).
N	UC&C Audit and User Activity Trails:

1	The UC&C shall support the generation of audit trails. Audit trails shall consist of logs of operator/administrator additions, deletions, and modifications.
2	Audit trails shall be generated as reports. They shall be able to track changes made within specific time periods. Querying on specific users, changes, affected entities, and time periods shall also be possible.
3	For entity configuration changes, the audit trail report shall include detailed information of the value before and after the changes.
4	The UC&C shall support the generation of user activity trails. User activity trails shall consist of logs of operator activity on the UC&C such as login, camera viewed, badge printing, video export, and more.
5	The UC & C shall support the following actions on an audit and activity trail report: print report and export report to a PDF/ Microsoft Excel/CSV file.
O	Third Party System Unification:
1	Directory service like MS – AD / LDAP or Similar integration shall permit the central user management of the UC&C users, user groups and other Access control groups.
2	The UC&C shall support multiple approaches to integrating third party systems and other Smart city application. These shall include: Application Programming Interface (API) / Software Development Kits (SDKs), Driver Development Kits (DDKs), REST-based Web Service API/SDK and RTSP Service API/SDKs.
3	A UC&C API SDK shall be available to support custom development for the platform if required in future.
4	The SDK shall enable end-users to develop new functionality (user interface, standalone applications, or services) to link the UC&C to third party business systems and applications such as Badging Systems, Human Resources Management Systems (HRMS), and Enterprise Resource Planning (ERP) systems.
5	The API/ SDK shall provide an extensive list of programming functions to view and/or configure core entities such as: users and user groups, alarms, custom events, and schedules, and more.
P	Cyber Security Requirements:
1	The UC&C Application shall be an IP enabled solution. All communication between the Servers, Clients and external systems shall be based on standard TCP/IP protocol and shall use TLS encryption with digital certificates to secure the communication channel.

2	The Application shall limit the IP ports in use and shall provide the Administrator with the ability to configure these ports.
3	The VMS system Unified with the UC&C application shall support only secured media stream requests, unless explicitly configured otherwise. Secured media stream requests shall be secured with strong certificate-based authentication leveraging RTSPS (aka RTSP over TLS). Client authentication for media stream requests is claims-based and may use a limited lifetime security token.
4	All other needed best practices for best Cyber Security Standards must be followed and adopted in the development, deployment and adoption phases of the project.
5	The OEM of UC&C application shall have an online or offline Cyber Security emergency response center to update on latest vulnerabilities and provide needed assistance during any cyber- attacks on the system. Details of response center must be available on the OEM global website.
6	All other needed best practices for best Cyber Security Standards must be followed and adopted in the development, deployment and adoption phases of the project.

5.1.2. Functional & Technical Requirements for Video Display Wall

Sr. No	Item	Specifications
1.	Display Wall Individual Cube Size	70"±5%
2.	Projection Technology	DLP Rear Projection with each cube having 4K-UHD resolution
3.	Cube Depth	Less than 600 mm
4.	Light Source	Laser
5.	Light Output of projection engine	1800 Lumens or more
6.	Brightness Uniformity	95%
7.	Dynamic Contrast ratio	100,000:1
8.	Dust Proof	Projection Engine to be certified IP6X by a third-party laboratory to ensure prevention from ingress of dust ensuring long life of the video wall
9.	Power Supply	Dual Redundant Power Supply Built in inside the cubes

10.	Half Gain viewing angle	Horizontal $\pm 180^\circ$, Vertical $\pm 180^\circ$
-----	-------------------------	---

5.1.3. Functional & Technical Requirements for Video Wall Controller

Sr. No	Item	Specifications
1.	Display controller	Each Controller to be able to control each PATNA SMART CITY OFFICE video wall with a total resolution to support all Video Wall displays.
2.	Redundancy in the controller	Power supply and HDD should be redundant in the controller
3.	Platform	Windows 10 with processor with Quad core 3 Ghz or Core i7/Xeon
4.	RAM	16 GB
5.	Chassis Type	19" Rack mount industrial chassis
6.	Network	2 Network Ports
7.	Scalability	The system should be able to add additional inputs as required in the future using additional chassis/cards
8.	Redundancy	Redundant Hot Swappable in RAID Configuration
9.	Redundancy	Redundant Hot Swappable Power Supply
10.	24 x 7 operation	The controller shall be designed for 24 x 7 operation
11.	Others	The Video Wall and the Controller should be of the same make to ensure better performance and compatibility
12.	OEM Certification	All features and functionality should be certified by the OEM. The Display Modules, Display Controller & Software should be from a single OEM.
13.	Ticker	There should be a possibility in the controller to create user defined multiple tickers. It should also be possible to place these tickers anywhere on the wall

Video Wall Management Software		
1.	Layouts	The software should be able to pre configure various display layouts and access them at any time with a simple mouse click or schedule/timer based.
2.	Sources	The software should be able display multiple sources anywhere on video wall in any size.
3.	Workspace Allocation	The video wall administrator should be able to allocate workspace to each operator
4.	Software features	Video Wall Control Software shall allow commands on wall level or cube level or a selection of cubes: <ul style="list-style-type: none"> Switching the entire display wall on or off. Snap sensitivity to ensure quick and accurate aligning of sources Fine-tune colour of each cube
5.	License	Should have a software license key to protect from unauthorized use
6.	Authentication	Should offer 4 levels of authentication
7.	Scaling	Each source should be capable of being scaled to required size
8.	Display	The software should be able to create layouts and launch them as and when desired
9.	Remote Control	The Display Wall should be controllable from Remote PC also.
10.	Offline Layouts	Should be possible to create offline layouts
11.	Layout Scheduler	All the Layouts can be scheduled as per user convince.
12.	Layout Scheduler	Software should support auto launch of Layouts according to specified time event by user
13.	Layout Management	It should be possible to create layouts comprising of screen scrapped content of Workstations, DVI inputs, URLs configured as sources.
14.	Layouts Configuration	Can be pre-configured or changed in real time
15.	Scheduling	It should be possible to schedule specific Layout based on time range

16.	OEM Certification	All features and functionality should be certified by the OEM.
17.		The Display Modules, Display Controller & Software should be from a single OEM.

5.1.4. Functional & Technical Requirements for Monitoring Workstations

Sr. No.	Parameters	Technical Specifications
1.	Form Factor	Tower
2.	Processor	Intel Xeon Processor, 8 Cores, 16MB Cache, 3.8Ghz base frequency, 4.7Ghz Turbo frequency or higher processor
3.	Operating System	Windows 10 Pro, 64bit or latest
4.	Office	Microsoft office standard edition latest.
5.	Chipset	Intel Workstation Chipset 400 Series or higher
6.	Memory	32GB in combination
7.	Hard Drive	256GB SSD
8.	Graphic Card	Nvidia Quadro P2200 GPU or higher
9.	Keyboard & Mouse	Wired Keyboard & Mouse (Same make as PC)
10.	Monitor	Should be supplied with min 3x 27" LED Monitors
11.	PSU	80PLUS Gold Certified Energy Star Compliant
12.	Expansion Slots	Minimum "1" PCIe x16 Gen3; "2" PCIe/ PCI x4/x8 Gen3 and "1" M.2 or more (As per OEM)
13.	Network Card	Dual Intel Ethernet Connection 10/100/1000 or better
14.	I/O	4 - USB 3.1 1 - USB 3.1 Type C 1 - Audio Jack/ Microphone & Headphone 4 - DisplayPort 2 - RJ45 Network Connector
15.	Warranty	5 Years

5.1.5. Functional and Technical Specification of PTZ Joy Stick

S.No.	Minimum Technical Requirements
1	The Digital Keyboard (Joystick) shall be fully functional, multipurpose keyboard used for controlling of connected PTZ Camera.
2	Digital Keyboard shall include an integral variable speed Pan/Tilt/Zoom joystick and shall be able to select PTZ Camera.
3	Digital Keyboard shall support RS-232/RS-485 or Ethernet or USB port connectivity and shall be supplied along requisite interface units.

4	The Digital Keyboard (Joystick) should be ONVIF compliant and supports all features/ functionality of the VMS and NVR.
---	--

5.1.6. Functional and Technical Specification of LED Display (55 inches)

Sr. No.	Features	Specifications
1	Display Size	55 inches or above
2	Native Resolution	3840 x 2160 (UHD)/4K
3	Brightness	Minimum 400 cd/m2 or above
4	Contrast Ratio (Native)	Minimum 1100 : 1 or better
5	Viewing Angle	178 * 178
6	Response Time	12 ms or better
	Connectivity	
7	Input Ports	HDMI-3, USB 2.0 - 1, RS232C, RF, RJ45
8	Output Ports	Digital audio out
9	Special features	Smart Home , Web Browser, Pre-loaded App, Soft AP, WiFi, Screen Share, DIAL, Bluetooth Audio Playback, Sound Sync/bluetooth
11	Wi-Fi	built-in Wifi required
	Working Hours	14 Hrs Per Day
	Environment Conditions	
12	Operation Temperature	0 °C to 40 °C or lower
13	Operation Humidity	10 % to 80 % or better
14	Audio	20W (10W * 2)
	POWER	
15	Power Supply	100-240V~, 50/60Hz
16	Power Type	Built-In Power
	Power Consumption	
17	Typ.	150 W or Less
	STANDARD (CERTIFICATION)	
18	Certificates	BIS, CE, FCC
19	Accessories	Table stand/Wall Mount, Remote with Batteries and standard cables
20	OEM Warranty	5 Years

5.1.7. Functional & Technical Requirements for Desktops

Sr. No.	Parameter	Minimum Specification
S.No	Parameters	Minimum Technical Requirements
1.	Processor	Intel Core i5-latest generation (3.0 Ghz) or higher
2.	Memory	8 GB DDR4 RAM @ 2400 MHz. One DIMM Slot must be free for future upgrade
3.	Motherboard	OEM Intel Motherboard
4.	Hard Disk Drive	Minimum 1 TB Hard Disk @7200 RPM or higher
5.	Audio	Line/Mic In, Line-out/Speaker Out (3.5 mm)
6.	Network port	10/100/1000 Mbps auto-sensing on-board integrated RJ-45 Ethernet Port
7.	Graphics card	Minimum Graphics card with 2 GB video memory (non-shared) with HDMI/mini display port.
8.	Wireless Connectivity	Wireless LAN - 802.11b/g/n/
9.	USB Ports	Minimum 4 USB ports
10.	Display Port	Minimum 1 Display Port (HDMI/VGA) port
11.	Keyboard	104 keys Heavy Duty Mechanical Switch Keyboard (USB Interface) with 50 million keystrokes life per switch. Rupee Symbol to be engraved.
12.	Mouse	Optical with USB interface (same make as of desktop)
13.	Monitor	Minimum 21.5” diagonal LED Monitor with 1920x1080 or higher resolution. (Same make as desktop). Must be TCO05 certified.
14.	Operation System and Support	Pre-loaded Windows 10 (or latest) Professional 64 bit, licensed copy All Utilities and driver software, bundled in CD/DVD/Pen-drive media.
15.	Certification for Desktop	Energy Star 5.0 or above / BEE star certified

5.1.8. Functional & Technical Requirements for IP Phones

Sr. No	Parameter	Specification
1	Protocols/Standards	SIP RFC3261, TCP/IP/UDP, RTP/RTCP, HTTP/HTTPS, ARP, ICMP, DNS (A record, SRV, NAPTR), DHCP, PPPoE, TELNET, TFTP, NTP, STUN, SIMPLE, LLDP, LDAP, TR-069, 802.1x, TLS, IPV6
2	Network Interfaces	Dual switched auto-sensing 10/100/1000 Mbps Gigabit Ethernet ports with integrated PoE
3	Graphic Display	Min 2.5-inch
4	Bluetooth	Yes, integrated
5	Feature Keys	4-line keys with up to 4 SIP accounts

6	Video Codec	Support for G.729A/B, G.711μ/a-law, G.726, G.722(wide-band), in-band and out-of-band DTMF (in audio, RFC2833, SIP INFO)
7	Auxiliary Ports	RJ9 headset jack
8	Telephony Features	Hold, transfer, forward, 3 way conference, call park, call pickup, shared-call appearance /bridged-line-appearance, downloadable phonebook, call waiting, call log XML
9	HD audio	Yes, HD handset and speakerphone with support for wideband audio
10	Language Support	English
11	Upgrade/Provisioning	Firmware upgrade via TFTP / HTTP / HTTPS, mass provisioning using TR-069 or AES encrypted XML configuration file
12	Power	Input:100-240V; Output: +12V, 0.5A Integrated Power-over-Ethernet (802.3af) Max power consumption: 6.4W (power adapter) or 6.49W (PoE)
13	Security	QoS Layer 2 QoS (802.1Q, 802.1P) and Layer 3 (ToS, DiffServ, MPLS) QoS User and administrator level passwords, 256-bit AES encrypted configuration file, SRTP, TLS, 802.1x or better
14	Compliance	FCC: Part 15 (CFR 47) Class B CE: EN55022 Class B; EN55024 Class B; EN61000-3-2; EN61000-3-3; EN60950-1 RCM: AS/ACIF S004; AS/NZS CISPR22/24; AS/NZS 60950.1or Equivalent Indian Standards

5.1.9. Functional & Technical Requirements for CTI/PBX System

S.No	Minimum Technical Requirements
1	IP based Computer Telephony Integration (CTI) System should be a converged communication System with ability to run analog and IP on the same platform using same software load based on server and Gateway architecture
2	Proposed Solution should support remote site survivability on local gateways and the survivable system should provide all the telephony features as of main site. Survivability features and options that allow gateways to continue operating even if the primary server fails or in the event a WAN failure affects communications between the gateway and the IP PBX.

S.No	Minimum Technical Requirements
3	System should support High availability and seamless failover from primary server to secondary server. It should allow the administrator to make configuration changes even when primary server is down.
4	The single IP PBX system should be scalable to support up to 500 stations (any mix/percentage of Analog/IP) to achieve the future capacity
5	The system should be based on server gateway architecture with external server running on Linux OS. No card based processor systems should be quoted
6	The voice network architecture and call control functionality should be based on SIP
7	The call control system should be fully redundant solution with no single point of failure & should provide 1:1 redundancy
8	The communication server and gateway should support IP V6 from day one so as to be future proof
9	The entire solution (IP PBX, its hardware, IP Phones, Voice Gateway, recording, headsets, Citizen automated center, etc.) should preferably be from a single OEM
10	Should support signaling standards/Protocols – SIP, H.323, Q.Sig
11	Voice Codec support - G.711, G.729, G.729ab, g.722
12	The System should have GUI support web based management console
13	The protection of signaling connections over IP by means of authentication, Integrity and encryption should be carried out using TLS
14	System should support MLPP / equivalent feature
15	Proposed system should support SRTP for media encryption and signaling encryption by TLS
16	Secure HTTP support for Call Server Administration, Serviceability, User Pages, and Call Detail Record Analysis and Reporting Tool. Should support Secure Sockets Layer (SSL) for directory
17	The administrator logging on to the call control server needs to authenticate by suitable mechanism such as User Login Information and Passwords/ Radius Server
18	System should allow custom client applications to support all call operations like make call, receive call, hold call, voice mail etc using REST API available from PABX.
19	There should be seamless integration of video between Video IP phone and Video End point for point to point and multipoint conferences. For this both the components should be from the same OEM.
20	Voice gateway to be provided with 1 PRI card scalable to 3 PRI in future for PSTN (PRI) line termination.

5.1.10. Functional & Technical Requirements for Fixed Box/Bullet Cameras

S.No	Features	Specifications
1.	Form Factor	Box Type / Bullet Camera
2.	Image Sensor	1/2.8" Progressive CMOS or better
3.	Day/NightvOperation	ICR with IR range of 100m or better
4.	Minimum Illumination	Color 0.1 lux , B/W 0.0005 lux
5.	Lens	Motorised Lens (12 mm to 40 mm / 5 mm to 50 mm)or as per requirement
6.	Electronic Shutter	1 ~ 1/10000 sec.
7.	Image Resolution	1920X1080 @ 25/30 fps (2MP)or better

8.	Compression	MJPEG, H.265,H.264 or better
9.	Frame Rate and Resolution	Full HD (2MP 1920x1080 or better) @ 25/30 FPS
10	Simultaneous Stream	Minimum 3 streams should be configurable at 1920 X 1080 @ 25 fps simultaneously
11	White Balance	Auto / Manual / ATW / One Push
12	Noise Reduction	3DNR / 2DNR / Color NR
13	Zoom	Digital Zoom
14	Video Streams	Three Stream supportable , All stream should be H.265
15	Image Setting	Saturation, Brightness, Contrast, Sharpness, Hue adjustable
16	Two way audio	Line in / Line out
17	Audio Compression	G.711 / G.726 / AAC / LPCM
18	Iris	P – Iris /Auto-Iris
19	Wide Dynamic Range	120 dB
20	Alarm	1 x Input / 1 x output
22	Network Interface	1 x RJ45
23	Storage backup on network failure	Camera should support network failure detection , Camera should have the capability to start the recording automatically on SD card(32 GB min at all locations) in case of connectivity between camera and NVR/Storage device goes down
24	Protocols	ARP,IPv4/v6, TCP/IP, UDP,RTP,RTSP,HTTP, HTTPS, ICMP,FTP,SMTP,DHCP,PPPoE,UPnP, IGMP, SNMP, QoS, ONVIF
25	Text Overlay	Date & time, and a customer-specific text etc.
26	Security	HTTPS / IP Filter / IEEE 802.1X
27	Firmware Upgrade	The firmware upgrade shall be done through web interface, the firmware shall be available free of cost
28	Power	PoE / DC 12V / AC 24V
29	Operating Temperature	0°C ~ 60°C
30	Operating Humidity	,10% ~ 90%, No Condensation
31	Certification	UL/BIS , CE , FCC
32	ONVIF	ONVIF profile S & G
33	User accounts	10

34	Supported Web Browser	Internet Explorer (7.0+) / Firefox / Safari / Chrome
----	-----------------------	--

5.1.11. Functional & Technical Requirements for Non-IT items

The selected bidder should adhere to the specifications given below for Non-IT components. It is essential that Fire Proof material be used as far as possible and Certification from Fire Department be taken for Command Centre and Office premises before Go-Live.

5.1.11.1. Functional & Technical Requirements for Ceiling Speakers

S.No.	Minimum Technical Requirements
1.	The ceiling speakers shall have high power with extended frequency responses.
2.	The ceiling speakers shall have wide, controlled constant directivity dispersions for optimum coverage.
3.	The ceiling speakers shall have output of at least 15W peak. They shall have in-built amplifiers or shall be supported by an external amplifier.
4.	The ceiling speakers shall have a conical coverage pattern .
5.	The ceiling speakers shall be in a White colour to match the ceiling and surrounding interior design.
6.	The ceiling speaker shall have a diameter not greater than 8.5”.
7.	MSI shall quantify and space speakers to provide full audio coverage within the command centre room and conference room.
8.	The ceiling speakers shall follow the manufacturer recommendation for connectivity.
9.	The Ceiling Speakers shall automatically adjust the output audio level based on ambient noise. This may require either in-built noise sensors with the ceiling speakers or an independent ambient noise monitoring system.

5.1.11.2. General Standards

The ICOMC interiors shall be state of the art adhering to the various best practices norms for integrated control centres, including:

- Development of ergonomic reports for the ICOMC covering Human Factors Engineering (HFE), ISO9241 (Ergonomic requirements for office work with visual display terminals - VDTs) and ISO11064 (Ergonomic Design of Control Centres)

The proposed interior material should meet to basic control room norms, including but not limited to:

- i. ASTM E84 or equivalent fire norms,
- ii. High scratch resistant surfaces,
- iii. Seismic zone compliance and Green Guard passed Desk for ensuring safe environment for operators.

5.1.11.3. Civil and Architectural Work

The scope of civil works shall include but not limited to the following:

- i. Interior design

- ii. Pest Control
- iii. Permanent walls and partitions (Fire rated)
- iv. Temporary removable Partitions (Fire rated)
- v. False Ceiling as per specifications
- vi. False Flooring as per specifications.
- vii. Thermal Insulation
- viii. Painting (Fire rated)
- ix. Doors (Fire rated)
- x. Furniture
- xi. Ramp
- xii. Glass partitions (fire rated) if required
- xiii. Any civil, masonry, trenching and fabrication works required for Electrical installation, Earthing, HVAC installation and other subsystems installations.
- xiv. Any other civil works required at site

5.1.12. Functional & Technical Requirements for ICCC Interiors

SN	Specifications
1.	The entire interior has to be designed as per ISO 11064 (International Norms to Design the Control Center). It should be state-of-art and the design should conform to provisions under ISO 14001 and OHSAS 18001, HFE and ISO 9241, covering various aspects of CCC/NOC.
2.	It must be safe, and the components used should not PROVOKE FIRE. So, ASTM E84 (Standard Test Method for Surface Burning Characteristics of Building Materials) certified materials to be used for wall cladding, flooring, panelling, partitions and ceilings. Safety of User & control room equipment is a high concern area therefore ceiling, paneling, partition and desk must be seismically tested and qualified. The test must be carried out by authorized government agency and certificate to be submitted.
3.	Wall panelling, and ceiling must be 100% modular to accommodate future technological expansions/retrofitting without taking any shutdowns and must be easily replaceable in case of damage. OEM to submit an undertaking for the same.
4.	The scope of the project includes designing; engineering, supply & installation of 24X7 mission critical Control Centre Interiors. Being a project of National repute this state-of-the-art facility & all its components like ceiling, flooring, control desk, panelling, Glass partitions, ceiling light & luminaries' wiring etc. shall be treated as a part of the solution i.e. operational control room.
5.	Look and feel of the control room shall be ultra-modern & unique. To solve monotony in control room in future, the panelling shall have inbuilt design in 20% tiles of panelling to change the colour without ordering new. The control room turnkey solution provider shall propose 3 colour options in advance during approval stage and shall change the approved colour scheme in future at no cost.
	Safety Design and Material Execution
6.	Wall Panelling shall be made up of Factory made; 100% Modular self inter lockable metal panels (sheet thickness 0.6mm & PVC Coating 0.15mm).
7.	Control Room should be designed as per ISO 11064.
8.	To ensure proper illumination level in the control room bidder should provide lux calculation report as per ISO 11064
9.	Wall Panelling and Ceiling must be seismically tested & .
10.	Wall Panelling and Ceiling tiles must be Class A fire rated certified for surface burning characteristics.

11.	The ceiling and panelling must be RoHS certified to ensure restriction of hazardous substance in any of the materials.
12.	Wall panelling and Ceiling tiles must be a combination of perforated and non-perforated tiles to have Sound absorption coefficient (NRC)
13.	Wall Panelling Tiles: - Minimum 40% of the tiles shall have at least 10,000 micro-perforations per square meter to achieve NRC of 0.6 Sound Absorption Coefficient by diffuse field method; IS: 8225-1987 “Measurement of Sound Absorption Coefficient in Reverberation Room” (Equivalent to ISO: 354- 1985 and ASTM 423-90).
14.	UL Certificate/Undertaking on 11064 standards on Load bearing capacity of Panelling - Panelling structure shall have load carrying capacity of 300 Kg to hold any display unit on. UL Certificate/ISO 11064 Norms undertaking need to be enclosed along with the bid.
15.	<p>Partitions</p> <p>Partitions must be modular in nature.</p> <p>Straight Metal Partition</p> <p>All the properties and material of construction shall be like straight Metal panelling but the partition shall have metal tiles on either side of the frame.</p> <p>Curvilinear Metal Partition</p> <p>All the properties and material of construction shall be like Metal panelling/partition but the front tiles shall be having perfect curve as per the requirement of the Control room and shall allow easy installation of the LVS/Screens on it.</p> <p>Glass Partition</p> <p>Full glass wall partitions will be made of 12mm Toughened laminated glass with frame-less structure. The glass partition shall be supported by 200-600mm high Modular metal partition (having the same finish as that of wall cladding) from the floor. Proper structure shall be made to ensure the fixing of glass from RCC slab above false ceiling and flooring.</p> <p>Straight and vertical structural members shall not be visible. Safety film shall be applied on the glass to avoid shattering. Glass shall be fitted on anodized extrusion with tool less technology and having a provision for replacing glass with perforated sheet/acoustic tile by removing the glass.</p> <p>The nature of installation should be replaceable, expandable and flexible to cater the future expansion/technical up-gradation.</p> <p>Safety of the Command Center - From fire and safety point of view; the metal partitions must be certified for surface spread of flame and smoke generation and ROHS Certified.</p>

16.	Air Flow Design to ensure proper flow and throw of air in the Command center. This requirement is mandatory to create perfect temperature and enough air movement to stay awake and comfortable. Design must comply ISO 11064:6.
17.	All desired certificates or undertaking to be obtained from UL or Intertek or 11064 standard or any Indian Government owned Research / Testing Institute.
18.	Wall Panelling Panel should comprise of hexagonal perforations for making the cladding and partitions acoustically sound. Min 20% panels shall be perforated or as required in the control room to achieve the desired acoustic levels. Materials having adverse impact on the environment and nature shall not be accepted. Zero / minimum maintenance is the basic requirement, thus wood, painted Gypsum, etc are not acceptable. As per design panel shall comprise of hexagonal perforation for making paneling and partitions acoustically sound. Panel shall be design in such a manner that it takes care of undulation of civil walls and gives perfect flat surface finish and compile easy service & maintenance procedure.
19.	Design: The cladding panels shall be made up of combination of two sheets locked and riveted together and polystyrene shall be used as infill to achieve strength and acoustics. The front tile (PVC pre-coated metal sheet) shall be perforated/ non-perforated as per the design requirement and the back tile shall be designed in such a manner that it fits on the back portion of the front tile. Once the tiles are fitted together then these will be manually riveted. These tiles shall be bend through CNC, machine punched & laser Cut to achieve perfect accuracy. Structure Shall be made from heavy duty powder coated modular steel frame (minimum sheet thickness 1 to 1.6mm) and shall allow uninterrupted flow of wires/cable/tubes of max. dia. 25mm. Structure Shall be securely grouted from wall, roof and floor. It shall be made up of 1-1.6mm thick vertical Slotted rolled C sections (Upright) and horizontal rolled 'C' connectors. Grid of desired dimension shall be formed by Vertical and horizontal sections having 50mm pitch.
20.	Surface Finish: For Panels: Front Panel: PVC pre-coated GI sheet (sheet thickness: 0.6mm and PVC coating: 0.15mm)

	<p>Back Cover: Powder coated GI sheet. (sheet thickness: 0.6mm with powder coating:)</p> <p>Panel shall provide better thermal, electrical insulation as compared to normal GI panels. It shall be non-reflective/glare free and be eligible for food contact.</p> <p>For Structure:</p> <p>Powder coated sheet. (sheet thickness: 1.0mm to 1.6mm with powder coating)</p> <p>The metal sheet shall have possibility of being formed mechanically per the specific needs of the project.</p>
21.	<p>Material Selection:</p> <p>Available Width- 300mm to 1200mm (in multiples of 150mm).</p> <p>Available Height- 150mm to 750mm (in multiples of 150mm).</p> <p>Thickness- 10mm to 15mm for perforated tiles with acoustic fleece without back cover 25mm to 30mm for non-perforated tiles with back covers.</p> <p>PVC pre-coated sheet:</p> <p>Fire rating and Low flame spread: EN ISO 11925-2,/EN 13823 / ASTM E-84</p> <p>Acoustic test: 9301/ ISO: 140/ASTM 413, ASTM C 578.</p> <p>Powder coating</p> <p>Adhesion test: EN ISO 2409</p> <p>Salt spray test: 600 hrs.</p> <p>Resistance to humid atmosphere test: DIN 50017.</p>
22.	<p>Acoustics Design</p> <p>The ambient noise level in the control room must not exceed 45 dB(A) during the length of the working day also it should not be less than 30dB. The auditory alarms Alarm signals should be at least 10 dB(A) over the background noise of the control room in order to be audible; and less than 15 dB higher than the background to avoid startling staff and affecting speech communication (ISO 7731:1986).</p> <p>Sound transmission class (STC) value of 35dB for Wall Panelling & Partition (according to IS: 9901 (Part III) 1981, DIN 52210 Part IV- 1984, ISO:140(Part III)- 1995. Metal modular perforated plank false ceiling have Sound absorption coefficient (NRC) value 0.60 per IS:8225-1987.</p> <p>Acoustic flooring (shall reduce impact sound by 14dB (ISO 717-2)). It shall be twin layer linoleum built up from 2 mm acoustic and a 2 mm Corkment backing. Flooring shall be decorative type of approved shade, pattern, texture and design and of</p>

	approved manufacturer. Dimensions shall be as per the final approved design and site requirement. Acoustic flooring (shall reduce impact sound by 14dB (ISO 717-2)). It shall be a combination of acoustic laminate and corkment. The top finish of flooring material shall be Greenguard certified to reduce health hazardous because of interior finishes.
23.	Printed Catalogues to be furnished for all items for interiors, furniture, lighting etc.

a) Miscellaneous – SI has to work out the exact requirement as per given building layouts at Annexures.

- i. Furniture
- ii. Reception Table
- iii. Meeting Table
- iv. Security table
- v. Chairs
- vi. Metal Detector
- vii. Fire Vault
- viii. Baggage Scanner
- ix. Printer (A3,A4) Scan and copier

5.1.13. Functional & Technical Requirements for Network Laser Printer

Sr. No	Parameters	Technical Specifications
1	Resolution (black)	Up to 1200 x 1200 dpi or better
2	Resolution (color)	Up to 1200 x 1200 dpi or better
3	Paper trays, standard	3
4	Print technology	Laser
5	Display	4-line LCD (color graphics)
6	Number of print cartridges	4 (1 each black, cyan, magenta, yellow)
7	Connectivity	2 Hi-Speed USB 2.0 Host ports; 1 Hi-Speed USB 2.0 Device port; 1 Gigabit Ethernet 10/100/1000T network port; 1 Hardware Integration Pocket; 2 internal USB Host ports
8	Processor speed	Minimum 700 MHz or better
9	Paper handling input, standard	100-sheet multipurpose tray, 500-sheet input tray 2, 500-sheet heavy media input tray 3

10	Paper handling output, standard	250-sheet output bin
11	Duplex printing	Automatic (standard)
12	Hard disk	Standard, 250 GB minimum (AES 128 encryption)
13	Print speed, black (normal)	Up to 33 ppm
14	Memory	Minimum 512 or higher
15	Media sizes supported	Tray 1: A4, RA4, A5, B5 (JIS), B6 (JIS), 10 x 15 cm, A6, 16K, envelopes (B5, C5 ISO, C6, DL ISO); custom: 76 x 127 to 216 x 356 mm; Tray 2: A4, A5, B5 (JIS), B6 (JIS), 10 x 15 cm, A6, 16K; custom: 102 x 148.5 to 216 x 297 mm; Tray 3: A4, RA4, A5, B5 (JIS), 16K; custom: 148.5 x 216 to 210 x 356 mm
16	Compatible operating systems	Microsoft Windows 7 Professional(64bit), Windows 8 Pro (64 Bit), Windows 8.1, Windows 10, Server 2008 R2, Server 2012 R2, MAC OS 9.0, MAC OS X, Linux

5.1.14. Functional & Technical Requirements for Biometric Access Control System

Data Center will be equipped with Access Control- Biometric Entry/ Exit protocols for ensuring authorized access.



Figure: DC Access (biometric)- (Indicative diagram)

Item	Description
Finger Print Template	Open Standard Template (ISO based) Template should be compatible with aadhar database.
Credential Support	Fingerprint, Card and Pin
Finger Print template	10 per user
Proximity Card	300 per site

Sensor Type	Suprema/Morpho/Cogent
Card Type Support	Proximity Card
User Capacity	1000
Display Unit	3.5 inch TFT Display with touchscreen
Buzzer	Yes
Event Buffer	500
Connectivity	Ethernet and USB
Power Input	12 V DC
Operating Temperature	-5° to 35°C
Sensor Resolution	500 dpi
Timing	Fingerprint Capture: Less than 5 Sec
	Verification of captured finger: Less than 2 Sec
Fingerprint Software	Enrolment Yes
Certifications	STQC certified
Installation	All conduiting / wiring /Trays /channels /trenches /pipes etc. for completion of Job
Warranty	5 Years Comprehensive onsite OEM Warranty
Access Control Software:	
The Access Control Software should have the following Specifications:	
Compatibility with any Windows Operating System	
Compatibility with MYSQL / SQL / ORACLE	
Support for TCP/IP Communication	
Provision for Alarm Monitoring for Battery, Mains Supply, Door Opened too Long, Door Forced Opened, Unauthorized Swipe & Controller Tampering	
Support for unlimited number of Card Database & Transactions	

Specify Card Activation & Expiry Date
Support for Biometric, Pin & Smart Card Applications
Management of Dual Access Levels to a single Card
Remote Locking & Unlocking of Doors
Remote management of Controllers
Customization of Door User time for every card holder
One Client License
Two Stages of Alarm Management (Acknowledgement on Receipt & Closure on Investigation)
Access Privileges on the basis of Time & Date
Creation of holiday schedules to cover maintenance & Vacations / Holidays
Setting of Time / Date
Permission to activate any control output for a specific event such as alarm
Programmable Shunt time to control the door opening time
Area Control by using Hard Anti Pass back, Soft Anti Pass back, Timed Anti Pass back, Occupancy Limit, Multi man principle, Area Lock down, Threat level conditioning.
Alarm Management
Automatic User Log off
Cardholder Management &Enrolment
Creation & Maintenance of User Database
Assignment of Access Privileges
Shall be capable to enroll biometric fingerprint templates
STQC certified enrolment biometric device to be provided
Warranty: 5 Years Comprehensive onsite OEM Warranty form the date of Go-Live with necessary updates, upgrades and patches

5.2. ICT Infrastructure Components

5.2.1. ICT Hardware Components for Data Centre

5.2.1.1. Functional & Technical Requirements for Core Router

S.No.	Minimum Technical Requirements
1.	Architecture & Performance
2.	The Core Router should be chassis based, Should have redundant processor and redundant power supply. All the Interfaces should be provided in line cards and no interface should be on CPU card. All interface should have wire speed performance.
3.	The back-plane capacity of Router should be minimum 7Tbps & forwarding performance of 5000Mpps packets per sec of 64 bytes packet. The performance is considered with IPv4 & IPv6
4.	Interface Requirement: 20 X 1 Gig Base SFP interface and 10 X 10Gig interface (The optics should be populated from day one) and Chassis should have Atleast 4 free main slot (not daughter slots) to scale in future to support additional 10Gig interface, 40G QSFP+ & 100G SFP28/CFP2 interface as per the requirement.
5.	The Router shall support GE/FE, 10GE-LAN, 10GE-WAN, 40GE, 100GE, 100G OTN Interfaces
6.	The Router should have High Availability Features: Non Stop Routing, Graceful Restart, In Service Software Upgrade, 802.1ag, MC-LAG, BFD for IPv4 and IPv6, VRRP.
7.	Protocol: DHCP, IP Multicast, PIM SM, PIM SSM, IGMP, MLD, RP, Next generation Multicast using MPLS LSP, IS-IS, HQOS (64 K queues), LDP, MPLS, MPLS FRR, L2 VPN, L3 VPN, VPLS, Differ TE, RIP V 2, OSPF, VXLAN, BGP, NAT
8.	Router should have IPv4, IPv6 and QoS Classification. Should have 3M IPv4, 2M IPv6 routing entries, 50000 IPv4 Multicast & 8000 IPv6 Multicast routing per system.
9.	Router should support Netconf, YANG (RFC 6020), Openflow/REST API, VXLAN, Segment Routing & time synchronization Synchronous Ethernet, 1588v2 & Adaptive Clock recovery/PTP
10.	Network Management: SNMP V3, Console management access, NTP or SNTP
11.	Operating temperature of 0°C to 45°C
12.	Certification: Offered Router should be EAL 2+/NDPP/NDcPP certified under Common Criteria certified
13.	OEM shall be featured in the Gartner's Magic Quadrant of Wired and Wireless LAN Access Infrastructure or Data Center in Leaders/ Challengers category for 2017/ 2018 /2019/2020 years

5.2.1.2. Functional & Technical Requirements for Internet Router

S.No.	Minimum Technical Requirements
1.	Architecture & Performance
2.	The Core Router should be chassis based, Should have redundant processor and redundant power supply. All the Interfaces should be provided in line cards and no

	interface should be on CPU card. All interface should have wire speed performance.
3.	The back-plane capacity of Router should be minimum 7Tbps & forwarding performance of 5000Mpps packets per sec of 64 bytes packet. The performance is considered with IPv4 & IPv6
4.	Interface Requirement: 10 X 1 Gig Base SFP interface and 8 X 10Gig interface (The optics should be populated from day one) and Chassis should have Atleast 4 free main slot (not daughter slots) to scale in future to support additional 10Gig interface, 40G QSFP+ & 100G SFP28/CFP2 interface as per the requirement.
5.	The Router shall support GE/FE, 10GE-LAN, 10GE-WAN, 40GE, 100GE, 100G OTN Interfaces
6.	The Router should have High Availability Features: Non Stop Routing, Graceful Restart, In Service Software Upgrade, 802.1ag, MC-LAG, BFD for IPv4 and IPv6, VRRP.
7.	Protocol: DHCP, IP Multicast, PIM SM, PIM SSM, IGMP, MLD, RP, Next generation Multicast using MPLS LSP, IS-IS, HQOS, LDP, MPLS, MPLS FRR, L2 VPN, L3 VPN, VPLS, Differ TE, RIP V 2, OSPF, VXLAN, BGP, NAT
8.	Router should have IPv4, IPv6 and QoS Classification. Should have 3M IPv4, 2M IPv6 routing entries, 50000 IPv4 Multicast & 8000 IPv6 Multicast routing per system.
9.	Router should support Netconf, YANG (RFC 6020), Openflow, VXLAN, Segment Routing & time synchronization Synchronous Ethernet, 1588v2 & Adaptive Clock recovery
10.	Network Management: SNMP V3, Console management access, NTP or SNTP
11.	Operating temperature of 0°C to 45°C
12.	Certification: Offered Router/ Router Family should be EAL 2+/NDPP/NDcPP certified under Common Criteria certified
13.	OEM shall be featured in the Gartner's Magic Quardant of Wired and Wireless LAN Access Infrastructure or Data Center in Leaders/ Challengers catagory for 2017/2018/2019/2020 Years

5.2.1.3. Functional & Technical Requirements for Data Centre Firewall

SL. No.	Minimum Requirement
A.	Security Features
1	Integrated Security Appliance which have these features from day 1 - Firewall, VPN, IPS, Web filtering, Botnet Filtering, Gateway AV, Anti Spyware/Anti-malware, Application Control and Geo-IP protection.
2	Should support authentication using XAUTH/RADIUS, Active Directory, SSO, LDAP, Novell, Internal user database, terminal Services, Citrix

3	Should be quad core or higher processor based solution for faster processing. The firewall should support atleast 10 Security Processing Cores. The processor should not be proprietary ASIC based.
4	Vendor & OEM should support the appliance with all necessary upgrade for at least 3 years from the date of purchase installation along with 3 years security software subscription. Product Support should be (24 x 7) with Advanced replacement
5	Should scan for threats in both inbound and outbound traffic simultaneously to ensure that the network is not used to distribute malware and does not become a launch platform for attacks in case an infected machine is brought inside.
6	Should support deep packet SSL to decrypt HTTPS traffic for scanning(IPS, Gateway Antivirus/Anti-malware, Content Filtering, Application control) transparently for future requirement and then re-encrypt and send to destination if no threat found.
9	Should not buffer traffic before scanning for virus. Should have capacity to scan unlimited file size without buffering them.
10	Firewall must support inbound and outbound Antimalware/Antispyware scanning. Should identify and block command and control traffic originating from bots on the local network to IPs and domains that are identified as propagating malware or are known CnC points. Sandbox appliance should provide atleast 6 VMs and real-world throughput of 500 files per hour
11	The firewall should be integrated with sandboxing solution from the same OEM which should be appliance based and employ sandboxing engine for effective scanning. Single appliance based Sandbox should be quoted for cluster of 2 firewalls.
11	The Sandbox should have technology that detects and blocks malware that does not exhibit any malicious behavior and hides its weaponry via encryption. Should detect and block mass-market, zero-day threats and unknown malware. The technology should discover packed malware code that has been compressed to avoid detection, the technology should allow the malware to reveal itself by unpacking its compressed code in memory in a secure sandbox environment. It should see what code sequences are found within and compares it to what it has already seen. Sandbox appliance should provide atleast 6 VMs and real-world throughput of 500 files per hour.
12	The Firewall should have the capability to block/prevent from Side Channel attacks like Meltdown, Spectre, Foreshadow, Foreshadow-NG, Portsmash etc. The firewall should have single pass, low latency inspection system that performing stream-based, bi-directional traffic analysis at high speed without proxying or buffering to effectively uncover intrusion attempts and malware downloads while identifying application traffic regardless of port and protocol.

13	Should have ability to prevent potentially malicious files from entering the network. Should have support for files sent to the proposed on-premise sandbox for analysis to be held at the gateway until a verdict is Should have continuously updated database of tens of millions of threat signatures residing in the sandbox servers and referenced to augment the capabilities of the onboard signature database, providing deep packet inspection with extensive coverage of threats. Should support min 20K DPI signatures, 60 million Cloud AV signatures and 3500+ Application Signatures from day 1. determined.
B	Hardware and Interface Requirements
1	The product should have minimum of 16 x 1GbE interfaces, 4 x 1Gb SFP interfaces and 2 x 10Gig SFP+ interfaces. Appliances should have dedicated management Ethernet interface
2	Should have built-in storage of atleast 900GB, 1 console Port and 1 USB interface
3	Appliance should have hot swappable dual removable fans and should have built in dual, redundant, power supply
4	Appliance should be 1U and rack mountable. Vendor not having 1RU configuration may quote higher RU to meet the requirement.
C	Firewall Performance Requirement
1	Threat prevention (Firewall + IPS+ AVC+ Anti-Malware) throughput of 5 Gbps or higher.
2	The Firewall should have atleast 6 Gbps of IPS throughput or higher.
3	VPN throughput at least 6 Gbps or higher.
4	The Firewall should support at least 90,000 new sessions/connections per second.
5	The Firewall should support at least 5 million maximum connections and 100K maximum DPI SSL sessions/connections.
6	Should support at least 8,000 IPSec Site-to-Site VPN tunnels and support 6000 or more no of IPSec Client Remote access VPN
7	Should support at least 2000 SSL VPN users
D	Licensing and Certification
1	The devices should not have license restriction on number of users. The license should the following subscriptions from day 1 - Firewall, Gateway Anti-Virus/AntiSpyware/Anti-malware, Intrusion Prevention and Application Intelligence and Control, URL/Content Filtering and Advance Threat Prevention/Protection including advance sandboxing.
2	The OEM should be having "recommended rating" by NSS Labs for consecutive three years in the last six years. OEM should have scored minimum 90% in Exploit Block rate in the last NSS Lab for NGFW report (2019) OR Firewall architecture should be DC grade with Data and control plane are different and should be in the Gartner Challengers/ Leaders from last 5 years and the OEM minimally attain common criteria (CC) / NSS /Forrester wave or equivalent certification"

3	The OEM should have Common Criteria/NDPP/ICSA Enterprise Firewall certification.
5	The device should be IPv6 Ready (Both phase 1 and Phase2)
E	Logging and reporting
1	Should have reporting facility to generate reports on virus/malware detected over different protocols, top sources for viruses/malware, destination for viruses/malwares, top viruses/malwares etc.
2	The solution should generate the reports for the firewall, gateway level AV/Anti-Malware, IPS web filtering requested. The solution shall have readymade templets to generate reports like complete reports or attack reports, bandwidth report etc.
3	The solution should help to analyze/understand attacks over various protocols like HTTP , FTP , SMTP etc. The solution should help to analyze/understand the live application usage in the network.
4	The solution should be running its own syslog server or integrated server to collect the logs for 6months of historical reports.. If separate server and/or appliance is required for the logging & reporting , the BOM & cost should be included in the proposed solution.
5	The solution should provide Change Order Management and Work Flow which assures the correctness and compliance of policy changes by enforcing a process for configuring, comparing, validating, reviewing and approving policies prior to deployment.
6	The should should support Offline management thereby enabling scheduling of configurations and firmware updates on managed appliances to minimize service disruptions.

5.2.1.4. Functional & Technical Requirements for WAF

S.No.	Minimum Technical Requirements for Web Application Firewall
1	The device should be a hardware based appliance with support for redundant powersupply
2	The device should provide an overall throughput of min 5Gbps of application layer throughput and 500,000 concurrent connections. The device should have minimum of 4X 10/100/1000 ports & 2x10G Ports and it should support it should 4 inline bypass interfaces inbuilt for fail safe operation. The throughput should be sustained to its capacity with WAF enabled and security rules in blocking mode
3	Support for all deployment modes mentioned below: Transparent inline bridge mode(within built fail-open interfaces Transparent revers proxy mode, Reverse proxy and Passive/promiscuous mode
4	The device should have abuse detection, tracking, Profiling and should support Abuseresponse and real-time incident management
5	Device should be able inspect HTTP and HTTPS traffic on TCP port 80 &443

6	Should be able to detect attempts to abuse form inputs and establish vectors for injection and cross-site scripting attacks
7	Must protect web application against Cookie Poisoning, cookie injection command injection.
8	Must protect web application against buffer overflow and layer 7 DDOS attacks.
9	Must protect web application against parameter tampering and must have inbuilt controls to block invalid files, filtering of sensitive words in HTTP request and response.
10	Should be able to detect suspicious application errors that indicate abuse including illegal and unexpected response codes.
11	Should be able to detect when an attacker is attempting to request files with suspicious extensions, prefixes and tokens
12	Should support creation of the policies for HTTP/HTTPS headers to ensure critical infrastructure information is not exposed. Response and request headers can be stripped, mixed, or filtered.
13	Should be able to detect and prevent attackers from finding hidden directories, inbuilt security control to limit the action of crawling and scanning
14	Should be able to detect attempts to abuse non-standard HTTP/HTTPS methods such as TRACE.
15	Should be able to detect attempts to manipulate application behaviour through query parameter abuse. Solution must support behaviour analysis to detect and prevent day 0 attacks
16	Should maintain a profile of known application abusers and all of their malicious activity against the application
17	Should enable application administrators to re-identify abusive users and apply persistent responses across sessions
18	Should be able to process SSL traffic using passive decryption or using equivalent technology
19	Should enable administrators to respond to application abuse with session specific warnings, blocks abusive application and undertake additional checks for the same.
20	Block connection and return arbitrary error/custom message
21	Should support network based security controls including IP blacklist/whitelist and URL blacklist/Whitelist
22	Sends alert emails when specific incidents or incident patterns Occur
23	Enable command line interface/GUI for custom reporting
24	Should capture, log and display traffic related data to analyse for security incidents.

25	Should enable SNMP system logging and able to send alerts to a centralized EMSsolution
26	Should support auditing – Tracks changes to the system made by the administrators in the configuration interface, security monitor and report generation.
27	Should be able to send security incidents via syslog
28	Management: Should support simplified GUI and web-based configuration. Shouldsupport web-based monitoring and analysis interface. Should have real-time and historical system monitoring, Should support role based access control.
29	The solution should be leader/challengers in Gartner Magic Quadrant since last 3 years.
30	The solution must support custom security rules. Administrators should be able todefine rules for the positive and negative security model and to create correlation rules with multiple criteria. This should be possible without need to write any script/code.

5.2.1.5. Functional & Technical Requirements for AAA: (Authentication, Authorization and Accounting)

- a) AAA network security services provide the primary framework through which a network administrator can set up access control on network points of entry or network access servers, which is usually the function of a router or access server. Authentication identifies a user; authorization determines what that user can do; and accounting monitors the network usage time for billing purposes.
- b) AAA information is typically stored in an external database or remote server such as RADIUS or TACACS+. The information can also be stored locally on the access server or router. Remote security servers, such as RADIUS and TACACS+, assign users specific privileges by associating attribute-value (AV) pairs, which define the access rights with the appropriate user. All authorization methods must be defined through AAA.
- c) The RADIUS Protocol: The RADIUS protocol carries authentication, authorization and configuration information between a NAS and a RADIUS authentication server. Requests and responses carried by the RADIUS protocol are called RADIUS attributes. These attributes can be username, Service-Type, and so on. These attributes provide the information needed by a RADIUS server to authenticate users and to establish authorized network service for them. The RADIUS protocol also carries accounting information between a NAS and a RADIUS accounting server.

S.No.	Minimum Technical Requirements Authentication, Authorization and Access (AAA)
1	The Solution should support AAA, NAC and Guest Access
2	The solution should support 250 endpoints for AAA from day 1
3	The solution should support 3000 device profiling from day 1
4	The solution should be scalable and stable solution to support 10,000 endpoints for AAA in future using additional appliances
5	AAA server should have device profiling functionality for 5000 devices to enforce context aware policies.

6	Solution must be Agnostic to existing wired, wireless and VPN network in place today.
7	Shell protected by CLI providing configuration for base appliance settings.
8	Appliance must provide disk or file security/encryption.
9	Ability to mix and match virtual and hardware appliances in one deployment.
10	Platform must be deployable in out-of-band model and support for clustering with N+1 activeredundancy model.
11	Flexibility to operate all features/functions on any appliance in the cluster.
12	Server Cluster must be Upgradeable from the GUI. A single pane which upgrades all thenodes in a cluster
13	Web-based, interface that includes several productivity tools such as a configuration wizard and preconfigured policy templates.
14	Support any type of networking equipment (wired, wireless, VPN) and a variety ofauthentication methods (802.1X, MAC auth, Web auth)/RADIUS, TACASCS+
15	Ability to take advantage of a phased implementation approach by starting with one elementof access management (role based) and later incorporating added security measures (endpoint health).
16	Must incorporate a complete set of tools for reporting, analysis, and troubleshooting. Data from access transactions can be organized by customizable data elements and used to generate graphs, tables, and reports. Must correlate and organize user, authentication, and device information together.
17	Solution must have fully integrated support for Microsoft NAP allowing health and posture checks on Windows endpoints without the need to install an agent.
18	AAA server must support both functionality RADIUS server for client device authenticationand TACACS+ for network device authentication and logging from day 1.
19	The system should provide standard based external facing APIs to extend support and integration with external applications like Ticketing systems, Firewall, IDS/IPS solutions etc
20	The solution Must be an easy-to-deploy hardware platform that utilizes identity based policies to secure network access and includes an integrated set of capabilities bundled under one policy platform:
	<ul style="list-style-type: none"> Built-in guest management and device/user on-boarding
	<ul style="list-style-type: none"> Web based management interface with Dashboard
	<ul style="list-style-type: none"> Reporting and analysis with custom data filters
	<ul style="list-style-type: none"> Data repository for user, device, transaction information
	<ul style="list-style-type: none"> Rich policies using identity, device, health, or conditional elements
	<ul style="list-style-type: none"> Deployment and implementation tools.

21	The solution should support flexible licensing model based on required functionality (i.e Profile, Posture, Guest Access).
22	The solution should Correlation of user, device, and authentication information for easier troubleshooting, tracking
23	The solution should must allow for the complete separation of Authentication and Authorization sources. For example, authentication against Active Directory but authorize against Local database
24	The solution should support authentication or authorization support for LDAP, AD Standard database etc
25	Should support multiple methods for device identification and profiling
26	The solution should support endpoint audit via NESSUS or NMAP scanning
27	The solution should have policy creation tools:
	<ul style="list-style-type: none"> • Pre-configured templates
	<ul style="list-style-type: none"> • Wizard based interface
	<ul style="list-style-type: none"> • LDAP browser for quick look-up of AD attributes
	<ul style="list-style-type: none"> • Policy simulation engine for testing policy integrity
28	The solution should support incorporation of several contextual elements including identity, endpoint health, device, authentication method & types, and conditions such as location, time, day, etc.
29	The solution should support the following enforcement methods:
	<ul style="list-style-type: none"> • VLAN steering via RADIUS IETF attributes
	<ul style="list-style-type: none"> • VLAN steering and port bouncing via SNMP
	<ul style="list-style-type: none"> • Access control lists – both statically defined filter-ID based enforcement, as well as dynamically downloaded ACLs.
	<ul style="list-style-type: none"> • Roles Based Access or any other vendor-specific RADIUS attribute supported by the network device.
30	The solution should support Location Based Access
31	The solution should support Time Based Access
32	The solution should able to join multiple Active Directory domains to facilitate 802.1x PEAP authentication.
33	The solution should support complex PKI deployment where TLS authentication requires validating client certificate from multiple CA trust chain. Must also

	support AAA server certificate being signed by external CA whilst validating internal PKI signed client certificates.
34	Failure of master node should not impact the ability for backup appliances to continue servicing authentication traffic.
35	Must support several deployment modes including centralized, distributed, or mixed.
36	The Policy Management solution should integrate with developed security and operations features like firewalls, MDM/EMM, and SIEM with REST based APIs , Syslog messaging, and deliver end-to-end policy enforcement and visibility from day 1
37	The solution should have Integrated Certificate Authority (CA) provides a complete and secure BYOD support.
38	The solution should support for Single Sign On (SAML 2.0) and O-auth for social logins using sites like Facebook, Twitter, Office365, GoogleApps, LinkedIn etc. from day one
39	The solution should support captive portal customization, and even offers professional, in-house creation from day one
40	The solution should support a wide array of REST/SOAP/XML APIs and protocols that customers can use to integrate their own CRMs, helpdesks, SIEM vendors, admission systems and more from day one
41	The solution should support Cluster deployment provides High Availability (HA) solution with no touch automatic failover from day one
42	The solution should support multivendor solution for network access, supporting over RADIUS vendor dictionaries for ultimate end-user flexibility from day one
43	The solution should consolidate all Policy Manager and license features into a single appliance or cluster
44	The solution should support Profiling and MDM integration, in the base appliance, to gather endpoint attributes for policy enforcement from day one
45	The solution should support TACACS+ device administration from day one
46	The solution should support SQL as authentication source from day one
47	The solution should support HTTP enforcement (JSON, XML, HTTP payload) from day one
48	The solution should support Advanced Posture Health Classes for Windows and OSX like Disk Encryption, USB, P2P apps
49	The solution should support social Network SSO through O-Auth (like Facebook, Twitter, Office365, Google Apps, etc.)
50	The solution should have Enhanced capabilities for endpoint compliance and control
51	The solution should support Microsoft, Apple, and Linux operating systems

52	The solution should support sponsored base Guest Access
53	The solution should support Self Provisioned Guest Access
54	The solution should maintain a list of active visitor sessions
55	Guest solution has ability to make changes to a visitor account's session while it is in progress.
56	It should be certified by EAL/NDPP/NIAP or equivalent.

5.2.1.6. Functional & Technical Requirements for DLP

S. No.	Minimum Specifications
1	The solution should cover both Active and passive FTP including fully correlating transferred file data with control information and have the ability to monitor popular IM protocols (AIM, Yahoo, MSN, IRC) and properly classify tunneled IM traffic (HTTP)
2	The solution must have Identity and Role Based policy capabilities that integrate with AD/LDAP/HR database. The solution should be capable of "Segmentation of Duty" (SoD) based Enforcement of Information Security and the solution should enforce "Automatic Access Control" on Data and Information
3	The solution must be able to apply different policies to different employee groups. The solution should have a comprehensive Information Classification methodology that would be readily deployable. The solution MUST use automated policy mechanism and should have built-in Automated Policy Synthesis mechanism. The solution should be able to monitor and prevent Advanced Persistent Threats (APT)
4	The solution should have Built-in Ontologies on International PII and PCI- DSS capabilities and has the ability to add or customized new Ontologies to cater to specific Government or Defense parameters. The solution should have rule or policy-based capabilities such as assigning access rights, restricting where users can store sensitive data, and so forth
5	The solution should have Ability to detect and protect new or unseen documents, which content is similar to the data categorization, which has been taught via data categorization. The solution should have Ability to detect scanned documents, which contains sensitive data in text form

6	Support centralized administration. Ability to support network, storage and endpoint DLP from single console and the DLP should be from different than Web Security proxy solution.
7	The end point solution should inspect data leaks from all portable storage and to keep track of what data users are taking from and to their work computers on any kind of portable storage device. The end point solution must monitor and control various storage devices including USB flash 2 drives, CD/DVD, external HDD, card readers, Zip drives, digital cameras, smartphones, PDA, MP3 players, Bluetooth devices etc.,
8	End point DLP agent should support network offline mode to access a specific device when a client computer is disconnected from a network and The endpoint solution should encrypt information copied to removable media
9	The solution should be able to classify unstructured data, namely word/excel/powerpoint/pdf documents and MS Outlook emails. The solution should be able to label the documents in headers/footers with a pre-selection capability for either header or footer or both. The solutions should be able to insert metadata tags in the documents and emails which can be read by DLP Solutions
10	The solution should be able to uniquely tag each classified document. The solution should be able to track initial classification and reclassification events at both document and central logging level. The solution should trigger classification for document on Save, Save As, Print etc. and should be configurable using a management mechanism
11	The solution shall ensure the enforcement of classification and should not allow user to bypass classification option in the said documents types using MS and Open Office and MS Outlook. The solution should have capability to detect differential classification between an email and it's attachments and block the email from being sent
12	The solution should have some guidance mechanism while user selects a classification level, to inform the users what is the context of a said classification level as per organization's policy. The solution should enable the classification of Word, Excel and PowerPoint documents from within Microsoft Office.
13	The solution should be able to identify information like Aadhar, Passport numbers, credit card information for automated classification thru either inbuilt capability or should have capability to define regular expressions. The solution should suggest a classification based in content, but should allow user to change the classification if required by taking a justification for the same and recording it in logs.

14	The solution should support the ability to warn or prevent users from sending password-protected Microsoft Office documents via email. (The metadata in password-protected Office documents is encrypted, so this capability provide an alternative way to enforce policy.) The solution should provide a pre-built starter set of reports for the reporting database (in Excel) and Views and documentation to enable customers to write their own reports.
15	Proposed solution should have inbuilt Data classification module, which should have direct presence in India. The proposed solution should support Windows, iOS as well as Linux endpoints and servers.

5.2.1.7. Functional & Technical Requirements for DC Core Switch

S.No.	Minimum Technical Requirements
1	Architecture
1.1	The Core switch should have chassis or Fixed form based or the stack of same type of switches to meet the interface requirement
1.3	Shall provide distributed /Centralized /Fabric switching technology (any additional hardware required for the same shall be proposed) & should support virtualization betweenboth switches
1.4	The switch shall be 19” Rack Mountable and shall have all mounting accessories
1.5	Shall have up to 4 Tbps switching capacity and the chassis
1.6	Shall have up to 1.2 Bpps switching throughput
1.8	It shall support 40 Gb E port in future without any hardware upgrade
1.9	The switch shall have Modular operating system provides an easy to enhance and extendfeature which doesn't require whole scale changes
2	Min Interface Requirement
2.1	Switch shall be provided with min. 8 nos. of 40GbE QSFP+ ports. Min. 2 ports should bepopulated with multimode SR4 transceivers.
2.2	Should have 32 nos. of 1G/10G SFP+ Ports 8 ports should be populated with multimode SR transceivers
2.3	Should have 24 nos. of 1000 Base-T Ports Copper (RJ-45)
3	Reliability and Resiliency Features
3.1	Redundant/Load-sharing power supplies with N+N power redundancy

3.2	Redundant Fans / redundant fans within the fan tray for redundancy
3.3	Passive/Redundant backplane design with hot swappable modules or stack /virtual chassis should be provided
3.4	The Switch should have the capability to extend the control plane across multiple active switches making it a virtual switching fabric, enabling interconnected switches to perform as single Layer-2 switch and Layer-3 Switch. The Fabric should be managed by a single IP Address.
3.5	The connected servers or switches should be attached using standard LACP for automatic load balancing and high availability
3.6	The virtual switching fabric shall be established over standard 10G or better Ethernet links
3.7	Virtual Router Redundancy Protocol (VRRP) support
3.8	Bidirectional Forwarding Detection (BFD) for OSPF, BGP and VRRP
3.9	Graceful restart for OSPF, BGP
3.10	UDLD or equivalent feature to prevent loops on detecting unidirectional links
3.11	Shall support a ring protocol or MSTP feature for ring Ethernet-based topology
3.12	Shall support Virtual Extensible LAN (VXLAN), Software Defined Networking (SDN) architecture with OpenFlow/OPFLEX/OVSDB/ or EVPN & VXLAN protocol/ REST API supporting open standard platform integration.
4	Layer 2 features
4.1	Spanning Tree (IEEE 802.1d STP, 802.1w RSTP, 802.1s MSTP)
4.2	Up to 4000 port-based or IEEE 802.1Q-based VLANs
4.3	IEEE 802.3ad Link Aggregation
4.4	IEEE 802.3ab LLDP
4.5	Jumbo Frames Support
4.6	IGMPv1/v2/v3, MLDv2/MLDv2 Snooping
4.7	QoS, Traffic prioritization and shaping
4.8	Access Control Lists
4.9	IEEE 802.1X, Port Security
4.10	STP BPDU protection and Root Guard or equivalent
4.11	DHCP Snooping and IP Source Guard or equivalent

4.12	ARP attack protection
5	IPv4 & IPv6 Routing features (any software/license required to enable these features shall be provided from Day 1)
5.1	Static routing
5.2	OSPFv2, BGPv4
5.3	Equal-Cost Multipath (ECMP)
5.4	Policy Based routing
5.5	RIPng/Equivalent OSPFv3, BGP4+,
5.6	IPv6 tunnelling
5.7	PIM-SM/PIM-DM/PIM-SSM
5.8	(PIM-SMv6, PIM-DMv6, PIMSSMv6)/ MLD V1, V2 and 1 K or better multicast routes.
5.9	Should support VxLan, EVPN
5.10	Unicast Reverse Path Forwarding (uRPF) or equivalent
6	Management & maintenance
6.1	Configuration through the CLI, console, Telnet or SSHv2
6.2	Switch management logon security (RADIUS/TACACS+)
6.3	SNMP v1/v2/v3
6.4	Traffic statistics via sFlow or equivalent
6.5	Network Time Protocol
7	Software Defined Networking (SDN) Capability or REST API capability
7.1	OpenFlow protocol or EVPN -VXLAN protocol capability to enable software-defined networking
7.2	Should have segregation of data (packet forwarding) and control plane (routing decision)
8	Environment
8.1	Shall be Support for RoHS / WEEE regulations
8.2	Safety: UL / CAN / CSA-C22.2 / EN / IEC 60950-1
10	OEM qualification Criteria
10.1	The Switch should be EAL-2/NDPP/NDcPP/FIPS certified

5.2.1.8. Functional & Technical Requirements for DC Switches

S.No.	Minimum Technical Requirements
1	Architecture
1.1	The switch should have at least 48 fixed 1000/10000 SFP+ ports, 4 x QSFP+ 40GbE ports.
1.2	The Switch should support, 1 RJ-45 out-of-band management port and 1 USB 2.0 port
1.3	The switch should support dual power supply and redundant fan modules
1.4	The switch Shall support 1000 Base-SX, LX, LH
1.5	The switch Shall Support 10Gbase-SR, LR, ER
1.6	The switch should have 16Gb flash/SSD, 8GB SDRAM/DRAM/RAM
1.7	The Switch should have 9 MB packet buffer size
1.8	All the ports in the Switch should be 1U 19" Rack-Mountable
1.9	At least 1280 Gbps switching capacity
1.10	The switch shall have switching throughput up to 950 million pps
1.11	MAC Address table size of 128,000 entries
1.12	Switch should at least support 100,000 routing entries IPv4, 50,000 entries (IPv6)
2	Quality of Service (QoS)
2.1	The Switch should support Strict Priority (SP), WRR/WDRR/WFQ//SDWRR, SP+WRR/ SP+WDRR/SP+WFQ//SP+SDWRR, Configurable Buffer/Time range, Queue Shaping, CAR with 64kbps granularity. The Switch should support traffic shaping technology.
2.2	The Switch should support packet filtering at L2 (Layer 2) through L4 (Layer 4); flow classification based on source MAC address, destination MAC address, source IP (IPv4/IPv6) address, destination IP (IPv4/IPv6) address, port, protocol, and VLAN.
3	Resiliency, High availability and Optimization features
3.1	The Switch should have cut-through and no blocking architecture
3.2	The Switch should have the capability to extend the control plane across multiple active switches making it a virtual switching fabric, enabling interconnected switches to perform as single Layer-2 switch and Layer-3 Switch. The Fabric should be managed by a single IP Address.
3.3	The connected servers or switches should be attached using standard LACP for automatic load balancing and high availability.

3.4	The Switch should have Advanced modular operating system
3.5	The Switch should support Reversible airflow/variable speed fan
3.6	The Switch should have Internal redundant and hot-pluggable power supplies and dualfan trays
3.7	The Switch should support Jumbo frames on Gigabit Ethernet and 10-Gigabit ports
3.8	The Switch should support VXLAN Layer 2 and Layer 3 gateway support for up to 1ktunnels
3.9	The Switch should support Dynamic VXLAN configuration using fabric manager
3.10	The Switch should support OVSDB for dynamic VXLAN configuration
3.11	The Switch should support EVPN
3.12	The Switch should support IEEE 802.1w Rapid Convergence Spanning Tree Protocol
3.13	The Switch should support IEEE 802.1s Multiple Spanning Tree
3.14	The Switch should support Virtual Router Redundancy Protocol (VRRP)
3.15	The Switch should support Hitless patch upgrades or Min-loss upgrade
3.16	The Switch should support Bidirectional Forwarding Detection (BFD) to enables link connectivity monitoring and reduces network convergence time for OSPF, BGP, VRRP, and switch virtualization technology
3.17	The Switch should support Device Link Detection Protocol (DLDP) or Link Layer Discovery Protocol (LLDP)
3.18	The Switch should support Graceful restart for OSPF, BGP
4	Layer 2 switching
4.1	The Switch should support MAC-based VLAN
4.2	The Switch should support Address Resolution Protocol (ARP) and supports static,dynamic, and reverse ARP and ARP proxy
4.3	The Switch should support IEEE 802.3x Flow Control
4.4	The Switch should support Ethernet Link Aggregation
4.5	The Switch should support IEEE 802.3ad Link Aggregation of up to 60 groups of 32 ports and support for LACP.
4.6	The Switch should support STP (IEEE 802.1D), Rapid STP (RSTP, IEEE 802.1w), andMultiple STP (MSTP, IEEE 802.1s)

4.7	The Switch should support for 4,096 VLANs based on port, MAC address, IPv4 subnet, protocol, and guest VLAN; supports VLAN mapping
4.8	The Switch should support for IGMP Snooping, IPv6 IGMP Snooping/MLD Snooping provides Layer 2 optimization of multicast traffic
4.9	The Switch should support DHCP/DHCP Server
5	Layer 3 services from day-1 (any additional licenses required shall be included)
5.1	The Switch should support Address Resolution Protocol (ARP)
5.2	The Switch should determine the MAC address of another IP host in the same subnet; supports static ARPs; gratuitous ARP allows detection of duplicate IP addresses; proxy ARP allows normal ARP operation between subnets or when subnets are separated by a Layer 2 network
5.3	The Switch should support simplifies the management of large IP networks and supports client and server; DHCP Relay enables DHCP operation across subnets
6	Layer 3 routing from day-1 (any additional licenses required shall be included)
S.No.	Minimum Technical Requirements
6.1	The Switch should support Virtual Router Redundancy Protocol (VRRP)
6.2	The Switch should support Policy-based routing
6.3	The Switch should support Equal-Cost Multipath (ECMP)
6.4	The Switch should support static routes, OSPF, BGP
6.6	The Switch should support Static IPv6 routing
6.7	The Switch should support separate stacks for IPv4 and IPv6 to ease the transition from an IPv4-only network to an IPv6-only network design
6.9	The Switch should allow custom filters for increased performance and security; supports ACLs, IP prefix, AS paths, community lists, and aggregate policies
6.10	The Switch should enable link connectivity monitoring and reduces network convergence time for RIP, OSPF, BGP VRRP and switch virtualisation technology
6.11	The Switch should Multicast Routing PIM-DM/PIM-SM, PIM-SSM for IPv4 and IPv6
6.12	The Switch should static routing, RIPng/ equivalent OSPFv3, BGP4+ for IPv6 Multiprotocol BGP (MBGP)
6.13	The Switch should be able to shut off unused ports/ admin shutdown of unused port and utilizes variable-speed fans, reducing energy costs

7	Management
7.1	The Switch should allow users to copy switch files to and from a USB flash drive
7.2	The Switch should support Multiple configuration files and stores easily to the flashimage
7.3	The Switch should SNMPv1, v2, and v3
7.4	The Switch should Out-of-band interface
7.5	The Switch should enable traffic on a port to be simultaneously sent to a networkanalyser for monitoring
7.6	The Switch should support Remote configuration and management
7.7	The Switch should support IEEE 802.1AB Link Layer Discovery Protocol (LLDP)
7.8	The Switch should support sFlow (RFC 3176)
7.9	The Switch should leverage RADIUS to link a custom list of CLI commands to anindividual network administrator's login; an audit trail documents activity
7.10	The Switch should provide support management access through terminal interface, as well as in-band and out-of-band Ethernet ports; provides access through terminal interface, Telnet, or secure shell (SSH)
7.11	The Switch should restrict access to critical configuration commands; offers multiple privilege levels with password protection; ACLs provide Telnet and SNMP access; local and remote syslog capabilities allow logging of all access
7.12	The Switch should support ingress and egress port monitoring and trace-route and ping
7.13	The Switch should support sFlow (RFC 3176)
7.14	The Switch should support ISSU/NSSU/hitless upgrade and hot patching/hitless patching/Min-Loss upgrade while in Virtual chassis / stacking
7.15	The Switch should support NTP or SNTP and PTP
10	Security
10.1	The Switch should provide IP Layer 3 filtering based on source/destination IP address/subnet and source/destination TCP/UDP port number
10.2	The Switch should support RADIUS/TACACS+
10.3	The Switch should support Secure shell encrypt all transmitted data for secure remote CLI access over IP networks
10.4	The Switch should support IEEE 802.1X and RADIUS network logins

10.5	The Switch should support allow access only to specified MAC addresses, which can be learned or specified by the administrator
11	Software Defined Networking (SDN) Capability using Netflow /EVPN-VXLAN or equivalent
11.1	The Switch should have OPFLEX/OpenFlow/OVSDB//REST API/Netflow / EVPN-VXLAN capability to enable software-defined networking from Day one
11.2	The Switch should Allow the separation of data (packet forwarding) and control (routing decision) plane
12	EMC & Safety Compliance
12.1	The switch should have UL 60950-1; EN 60825-1 Safety of Laser Products-Part 1; CAN/CSA-C22.2 No. 60950-1/62368-1-14; ROHS Compliance Emissions : VCCI Class A; EN 55022 Class A
13	OEM qualification Criteria
13.1	The Switch or Switch Operating System should be EAL-2/NDPP/NDcPP/FIPS certified

5.2.1.9. Functional & Technical Requirements for Servers: (Blade Servers, GPU Servers. AAA servers and A.I./Training Server)

Blade Server

Feature	Specification for Blade Server
Processor	Up to two Intel® Xeon® Scalable processors, up to 28 cores per processor, min. 2.0 Ghz
Chipset	Latest compatible chipset supporting above processor
Storage Controller	Integrated PCIe 3.0 12Gb/s SAS Raid Controller with 2GB Cache to support both internal hard drives of compute sled as well as the hard disks in the storage sled supporting RAID 0, 1, 5, 6, 10, 50, 60
Memory	24 DDR4 DIMM slots RDIMMS& LR DIMMS supporting speeds up to 2666MT/s
Memory Protection	Advanced ECC with multi-bit error protection
Hard Drives	2 x 1.2TB 10K RPM SAS HDD in RAID-1 for RAID -1 for data Server should be configured with integrated RAID controller to support RAID level 0,1,5,6 on internal disks, Server should have 2 or more nos. of 2.5inch HDD bays
Ethernet ports	2 * 25GbE or better network ports for ethernet
FC ports	2 * 32Gbps or better FC ports

Remote management port	In addition to the above dedicated Remote Management should be done/ All the blades in the chassis should be remotely managed through Chassis or should have redundant management compliance.
Bus Slots	Minimum of 3 PCI expansions/Mezzanine expansions.
OS Support	Microsoft Windows Server 2016 Std. Edition, Windows Server Hyper-V, Redhat Enterprise Linux, SuSE Linux Enterprise Server
Virtualization Support	VMWARE ESX/ESXi, Microsoft Hyper-V, Citrix
Alerts	Pre Failure alerts for all active and important components and automatic calls logging. Should provide predictive failure monitoring & proactive alerts of actual or impending component failure for fan, power supply, memory, CPU, RAID, NIC, HDD
Systems Management	Smart Embedded Systems Management should be able to automate task like discovery deploy monitor and update.
	Should not be dependent on agents to for life cycle management.
	Should be able to provide Single console to manage Servers.
	Power management tool – Single interface to optimize and control every usage
	Should be able to integrate to 3rd party management tools.
Remote Management	Vendor should provide embedded features that helps to manage Servers in physical, local and remote environments, operating in-band or out-of-band, with or without a systems management software agent.
	Should include Power Management, necessary licenses should be included.
	Should support remote scripted reconfiguration tools
	Should be able to monitor all systems components (BIOS, HBA's, NICs)
Security	Power-on password, administrator password.
	The server should have Silicon based root of trust
Configuration & management	<ul style="list-style-type: none"> • Real-time out-of-band hardware performance monitoring & alerting • Agent-free monitoring, driver updates & configuration, power monitoring & capping, RAID management, external storage management, monitoring of FC, HBA & CNA & system health • Out-of-band hardware & firmware inventory • Zero-touch auto configuration to auto deploy a baseline server configuration profile • Automated hardware configuration and Operating System deployment to multiple servers • Zero-touch repository manager and self-updating firmware system • Virtual IO management / stateless computing • Support for Redfish API for simple and secure management of scalable platform hardware

Systems Management Software	The server should come with systems management software to provide update management, configuration management, patch management and virtualization management.
Benchmarks	Server family should have published benchmark (Spec_int_rate2017)
Accessories	All the necessary tools & tackles licenses, cables/ connectors for Ethernet/ Fibre/ USB/ Power etc. required for making the system operational shall be provided by the bidder.
Industrial Standard Compliance	ACPI 2.0 Compliant, PCI 2.0 or higher Compliant, WOL Support, MS Logo Certification, USB 2.0 Support.

5.2.1.10. Functional & Technical Requirements for GPU Based Rack Servers (Video Analytics & FRS Servers)

Parameter	Specifications
Chipset	Latest Intel Chipset
Form Factor	Min 1U rack mounted with sliding rails
Processor	Dual Intel® Xeon® Scalable 2 nd Gen 16 Core 2.9 GHz processors
Memory slots	24 DDR4 DIMM slots, speed up to 2933MT/s, scalable to 3TB
Memory configured	Minimum 4 Gb per physical core
Disks supported	Drive bays: Up to 6 x 2.5” SAS/SATA (HDD/SSD)
RAID Controller	12Gbps PCIe 3.0 with RAID 1, 5, 10, 50 with 2GB Cache Memory
Disks configured	2x480GB SSD
DVD writer	DVD+RW
I/O slots	3 x Gen3 slots all x16
Network ports	2x 1G Ethernet and 2x 10G SFP+
Certified for OS	Windows Server 2016, VMWare, Red Hat Enterprise Linux, SUSE Linux Enterprise Server
Power Supply	Redundant Power Supply or higher
GPU Configured	3 x full height GPU (NVIDIA T4 or latest series) 8GB to be configured on Day 1

Management integration	Support for integration with Microsoft System Center, VMware vCenter, BMC Software
Power & temperature	Real-time power meter, graphing, thresholds, alerts & capping with historical power counters. Temperature monitoring & graphing
Pre-failure alert	Should provide predictive failure monitoring & proactive alerts of actual or impending component failure, memory, HDD
Configuration Management &	<ul style="list-style-type: none"> • Real-time out-of-band hardware performance monitoring & alerting • Out-of-band hardware & firmware inventory • Zero-touch auto configuration to auto deploy a baseline server configuration profile
	<ul style="list-style-type: none"> • Automated hardware configuration and Operating System deployment to multiple servers • Zero-touch repository manager and self-updating firmware system
LCD panel/LED Panel	As per OEM Design
HTML5 support	HTML5 support for virtual console & virtual media without using Java or ActiveX plugins
Server security	As per OEM Design
	Should provide effective protection, reliable detection & rapid recovery using: <ul style="list-style-type: none"> - Signed firmware updates - Secure default passwords
Warranty	5 years On-site comprehensive warranty with 24x7x365 remote hardware support.

5.2.1.11. Functional & Technical Requirements for AAA Server

S. No.	Parameter	Specifications
1	Servers	Should support approach that combines AAA, NAC, BYOD and Guest Access by incorporating identity, health, physical/device information, and conditional elements into one set of policies.
2		Must have ability to scale to up to 5000 devices per appliance from day 1
3		Solution must be Agnostic to existing wired, wireless and VPN network in place today.

4		Shell protected by CLI or local access providing configuration for base appliance settings.
5		Appliance must provide disk or file encryption.
6		Ability to mix and match virtual and hardware appliances in one deployment.
7		Platform must be deployable in an out-of-band model and support for clustering with N+1 redundancy model.
8		Flexibility to operate all features/functions on any appliance in the cluster.
9		Functionality Web-based, interface that includes several productivity tools such as a configuration wizard and preconfigured policy templates.
10		Support any type of networking equipment (wired, wireless, VPN) and a variety of authentication methods (802.1X, MAC auth, Web auth).
11		Ability to take advantage of a phased implementation approach by starting with one element of access management (role based) and later incorporating added security measures (endpoint health).
12		Must incorporate a complete set of tools for reporting, analysis, and troubleshooting. Data from access transactions can be organized by customizable data elements and used to generate graphs, tables, and reports. Must correlate and organize user, authentication, and device information together.
14		AAA server should have device profiling functionality for 1000 concurrent devices from day 1 to enforce context aware policies.
15		It must provide functionality like Android should get different access and Iphone will get different access.
16		If any additional license would require to provide profiling functionality, it should be perpetual.
17		AAA server must support both functionality RADIUS server for client device authentication and TACACS+ for network device authentication and logging from day 1. Overlay component can be added to achieve both functionality.
18		All external facing interfaces are programmable, which means APIs are available to extend the system to support different

		authentication protocols, identity stores, health evaluation engines and port and vulnerability scanning engines.
19		<p>The solution Must be an easy-to-deploy hardware platform that utilizes identity based policies to secure network access and includes an integrated set of capabilities bundled under one policy platform:</p> <ul style="list-style-type: none"> • Built-in guest management and device/user onboarding • Web based management interface with Dashboard • Reporting and analysis with custom data filters • Data repository for user, device, transaction information • Rich policies using identity, device, health, or conditional elements • Deployment and implementation tools.
20		Must support flexible licensing model based on required functionality (i.e. Profile, Onboard, Posture, Guest Access).
21		Correlation of user, device, and authentication information for easier troubleshooting, tracking etc.
22		AAA framework must allow for the complete separation of Authentication and Authorization sources. For example, authentication against Active Directory but authorize against an external SQL database.
23		Authentication or authorization support for LDAP, AD, Kerberos, Token Server, SQL compliant database
24		Should support multiple methods for device identification and profiling such as:
		Integrated, network based, device profiler utilizing collection via SNMP, DHCP, HTTP, AD, ActiveSync
25		Endpoint audit via NESSUS or NMAP scanning
26		<p>Policy creation tools:</p> <ul style="list-style-type: none"> • Pre-configured templates • Wizard based interface • LDAP browser for quick look-up of AD attributes

		<ul style="list-style-type: none"> Policy simulation engine for testing policy integrity
27		Policy model should support incorporation of several contextual elements including identity, endpoint health, device, authentication method & types, and conditions such as location, time, day, etc.
28		Support the following enforcement methods:
29		VLAN steering via RADIUS IETF attributes and VSAs
30		VLAN steering and port bouncing via SNMP
31		Access control lists – both statically defined filter-ID based enforcement, as well as dynamically downloaded ACLs.
32		Roles or any other vendor-specific RADIUS attribute supported by the network device.
33		Agent-based enforcement – bouncing a managed interface and sending custom messages. Also, control access to different networks via whitelist and blacklist. License as per requirement.
34		Must be able to join multiple Active Directory domains to facilitate 802.1x PEAP authentication.
35		Must support complex PKI deployment where TLS authentication requires validating client certificate from multiple CA trust chain. Must also support AAA server certificate being signed by external CA whilst validating internal PKI signed client certificates.
36	Reliability / Performance	Appliances have ability to be clustered in any combination via local and remote network connections providing unlimited scale, redundancy, and access load balancing.
37		Platform must be deployable in an out-of-band model and support for clustering with N+1 redundancy model.
38		Failure of master node should not impact the ability for backup appliances to continue servicing authentication traffic.
39		Must support several deployment modes including centralized, distributed, or mixed.
40		Core product should have been available in the market for at least 4 years.
41	Guest Access	Solution must be capable of providing sponsored and self-provisioned Guest Access. License as per requirement.

42		Ability to provide free or billable Guest Access with built in payment solution that can integrate with payment solution providers.
43		Must be able to provide custom branding.
44		Ability to send automated SMS or email credentials to the Guest User.
45		Ability to set Account Details including Time Frame, Bandwidth Contract etc. Once account timeframe expires the User Account becomes inactive automatically.
46		Solution must be capable of providing Advertising Services (Play Video before Access, offer current Promotions, Advise of Health Alerts)
47		Guest solution should manage the individual guest credentials in a partitioned database and not pollute the user store with account credentials for guest users.
48		Ability to perform caching of MAC address post guest authentication to avoid the need for guest to re-authenticate during the period of their visit (3G like user experience after first authentication via captive portal).
49	Guest Access	Auto-login for self-registration workflow – no need for the guest to retrieve account credentials from email or SMS for initial login.
50		Anonymous login support with per device policy still applied.
51		Access token login support for single credential login to guest network – event management, scratch cards etc.
52		Bulk import of guest accounts with ability to trigger notification of credentials via email.
53		Bulk import of NAS devices for large scale deployments.
54		Sponsored approval workflow for guest self-registration where open SSID registration can be protected by requiring internal staff to approve the creation of guest account.
55		Prevent employees from accessing the guest network on the corporate laptop.
56		Apple Captive Network Assistant bypass for managing end to end guest workflow. For example post login welcome page display on iOS and Mac OS Lion and above devices.

57		Post login session statistics page displayed to users so they can monitor usage or quota assigned.
58		Support URL persistence so users originally requested webpage can be displayed post login.
59		Location based captive portal – display different landing page based on where guest is connecting to the network.
60		Support guest access across multi-vendor access networks.
61		Fully customizable self-registration or guest creation pages with user interface controls such as drop down, check list, radio button.
62		Authenticated self-registration for partner / joint venture account provisioning.
63		Published API's to allow 3 rd party system to manage guest accounts.

5.2.1.12. Functional & Technical Requirements for Continuous Learning Server
A.I/Training Server

Parameter	Specifications
Rack Height	4U
CPU Support	Must support 2 CPU's
Chipset	Intel C620 or better
Processors	Dual Intel® Xeon® Scalable 2nd Gen 16 Core 2.9 GHz processors
Memory	4x 32 GB RAM 2666 MT/s support up to 1500GB RAM, should have min. 16 DIMM slots
Hard Drives	4x3.84Tb SSD Should support up to eight hard disk drives (SAS, SATA, nearline SAS SSD: SAS, SATA)
GPU Configured	Should be configured with 8nos. Of Nvidia V100 / A100 32Gb GPU
GPU Support	Should support upto 10 GPU's
RAID Card	RAID Controller Card supports RAID 1, 5, 10
PCI Slots (I/O)	10 x PCIe 2.0/3.0 slots
NIC ports	2x1G & 2x10G baseT ports

Redundant Power Supply	Dual, Hot-plug, Redundant Power Supply
Management integration	Support for integration with Microsoft System Center, VMware vCenter, BMC Software
Power & temperature	Real-time power meter, thresholds, alerts & capping with historical power counters. Temperature monitoring
Pre-failure alert	Should provide predictive failure monitoring & proactive alerts of actual or impending component failure for fan, power supply, memory, HDD
Configuration & management	<ul style="list-style-type: none"> • Real-time out-of-band hardware performance monitoring & alerting
Management (continued)	<ul style="list-style-type: none"> • Automated hardware configuration and Operating System deployment to multiple servers
HTML5 support	HTML5 support for virtual console & virtual media without using Java or ActiveX plugins
Server security	As per OEM Design
OS	Windows server 2019 Standard Edition
Warranty	5 years On-site comprehensive warranty with 24x7x365 remote hardware support.

5.2.1.13. Functional & Technical Requirements for Blade Chassis

Feature	Specification
Chassis	Rack Mountable Chassis to accommodate Support for minimum 8 blade servers
Management Modules	Should support Hot Pluggable & fully Redundant Management Modules. The blade chassis should be configured with Hot swap IP based KVM Switch for Management or KVM Management should be integrated in Remote Management Controller.
Mid-plane	Should have passive mid-plane/no mid plane/ back-plane architecture
IO Connections	Hot swap and redundant cooling fans and all fans should be fully populated Dual end-to-end redundant Network connectivity for each blade

	The blade chassis should have at least 4 I/O Modules/ switch bays
OS support	Chassis should support industry standard operating systems like Microsoft Windows Server 2016 Std. Edition, Windows Server Hyper-V, Redhat Enterprise Linux, SuSE Linux Enterprise Server
Power supplies	The enclosure should be populated fully with power supplies of the highest capacity available with the vendor. Power supplies should support N+N as well as N+1 redundancy configuration, where N is greater than 1
	Power Management Features like
	i. To cap the power of individual server or a group.
	ii. Intelligently assign power to the appropriate server in the pool based on policy settings.
	iii. To show the actual power usage and thermal measurements data of servers
Accessories	The blade chassis should be configured with cables, connectors and accessories required to connect the Power distribution units to the power supplies
Ethernet Switches	The Chassis should have redundant Ethernet switches, each switch should have 4 no. of 10Gb or better uplinks.
FC Switches	The Chassis should have redundant FC switches, each switch should have 4 no. of 32Gbps or better FC uplinks to SAN
Management	The chassis should have a touch screen LCD /LEDdisplay
	System Management and deployment tools to aid configuring the Blade Servers and OS Deployment should be provided.
	The chassis should be equipped for providing MAC & WWN address across the slots or chassis instead of individual Host Bus Adapter/NIC of the Blade. The solution provided must not have any single point of failure and must be configured in failover
Warranty	5 years On-site comprehensive warranty with 24x7x365 remote hardware support.

5.2.1.14. Functional & Technical Requirements for SAN Switch

S. N.	Minimum Requirement
-------	---------------------

1	The fibre channel switch must be rack-mountable. Thereafter, all reference to the 'switch' shall pertain to the 'fibre channel switch'
2	The switch to be configured with minimum of 24 ports with 16 Gbps FC configuration backward compatible to 4/8.
3	All 24 x FC ports for device connectivity should be 4/8/16 Gbps auto- sensing Fibre Channel ports.
4	The switch must have hot-swappable redundant power supply & fan module without resetting the switch, or affecting the operations of the switch.
5	The switch must be able to support non-disruptive software upgrade.
6	The switch must be able to support state full process restart.
7	The switch must be capable of creating multiple hardware-based isolated Virtual Fabric (ANSI T11) instances. Each Virtual Fabric instance within the switch should be capable of being zoned like a typical SAN and maintains its own fabric services, zoning database, Name Servers and FSPF processes etc. for added scalability and resilience.
8	The switch must support up to 16 Virtual Fabric Instances.
9	The switch must be capable of supporting hardware-based routing between Virtual Fabric instances.
10	The switch must support graceful process restart and shutdown of a Virtual Fabric instance without impacting the operations of other Virtual Fabric instances.
11	The switch shall support hot-swappable Small Form Factor Pluggable (SFP) LC typed transceivers.
12	The switch must support hardware ACL-based Port Security, Virtual SANs (VSANs), and Port Zoning.
13	Inter-switch links must support the transport of multiple Virtual Fabrics between switches, whilst preserving the security between Virtual Fabrics.
14	The switch must support routing between Virtual Fabric instances in hardware.
15	The switch must be equipped with congestion control mechanisms such that it is able to throttle back traffic away from a congested link.
16	The switch must be capable of discovering neighbouring switches and identify the neighbouring Fibre Channel or Ethernet switches.
17	The switch should support IPv6.

5.2.1.15. Functional & Technical Requirements for Scale Out Storage

S.No.	Parameter	Technical Specifications
-------	-----------	--------------------------

1	Controllers and Architecture	<ul style="list-style-type: none"> - Storage Should be Fully Symmetric and fully distributed Architecture written for Scale-Out Storage operations. - Proposed Storage solution should be based on Appliance and not general purpose servers or software-define storage. - Scale out storage should be configured with minimum 4 controllers of the same type. - Over all storage cluster should be upgradable to min 2 x numbers of Storage controllers/Storage nodes/Drives, without any disruptions/downtime to production workflow for performance, capacity enhancement, software/firmware upgrades. - The storage cluster should support linear scalability of performance and capacity. ie for every drive bay/drive added, performance should increase by the same amount till the maximum capacity of the storage - Storage Controllers should processor have Intel processor as per OEM Design
2	Onboard Memory	The scale out storage must be configured with minimum 1 TB total , DRAM based cache/memory.
3	Operating System	Scale-Out Storage operating system/filesystem should have distributed specialized Operating System//filesystem by OEM(s), dedicated for serving data efficiently and customized for True Scale-Out Storage. Entire data should automatically balance across proposed controllers/nodes within each tier without any administrative intervention, or requirement of third-party software
4	Network Ports	The scale out storage should be offered with minimum 20 x 10Gbps SFP+ ports, and should be scalable to 2x the number of offered ports
5	Disk support	Storage cluster should have capability to support different kinds of disks tiers likes SSD, SAS, SATA/NL-SAS drives
6	Redundancy with No Single Point of Failure (SPOF)	<ul style="list-style-type: none"> - All video data should be striped across all storage controllers in the proposed storage system, so that performance of all controllers can be utilized for all read and write operations. - Redundant /Hot replaceable modules: Controllers, Hard Disk Drive and power supplies (230V AC, 50 Hz.) - The Complete multi-controller Storage System Solution should be fully redundant, configured in High Availability mode and should NOT have any Single Point of Failure (SPOF).

7	Total Storage Capacity	<ul style="list-style-type: none"> - All cameras to be recorded at highest resolution, 25FPS, H.265 video compression for 30 days at 24x7 continuous. - Scale out storage should be configured with 10 PiB usable capacity, using equal to or less than 12TB / 16TB NL-SAS/SATA HDD. . In case of RAID based offerings are offered -Additional 10% usable space should be reserved, or 2/3 number of disks should be provided, as hot spares. - Offered scale out storage should be capable of providing a throughput of greater than 8GBps at 100% write on SMB/NFS or equivalent , for handling the camera feed and other workloads. Dimensioning tool output/ performance decelerations needs to be provided on OEM letterhead for the same
8	Capacity/performance Expansion	<ul style="list-style-type: none"> - There should not be any downtime or migration activity required in the event it is needed to add additional capacity or additional performance to the storage system. - In the event of addition of storage controller/storage node to storage solution, existing data should be rebalanced across all nodes of storage controllers/storage nodes automatically. This auto balance should be done with low priority avoiding any impact to client performance. - Addition of storage controller/ storage nodes should not require any complicated configuration of new controller/node. It should be done easily, seamlessly and without having any impact to user access. - The storage file system shall not require metadata performance tuning. - The system must be able to support policy based tiering to different storage tiers with Storage sub-system.
9	Protection Levels	<ul style="list-style-type: none"> - Protection level which can protect data against simultaneous 2/3 disks/controllers/nodes failures, without data unavailability and data loss - Should have capability to change the protection level on-the-fly without impacting the workflow of VMS - Should be able to assign protection level on cluster or directory or file level.
10	Protocol Support	<ul style="list-style-type: none"> - Network protocol Support: Must provide access for a variety of operating systems (UNIX, Mac, Linux, Windows) using native OS protocols. All protocols required for the solution by the storage MUST be included without additional licenses and hardware. - Should support user security mechanisms like AD/LDAP / NIS.

11	Client Load Balancing	Storage System should have capability to load balance client connectivity across these multiple controllers so that all clients gets distributed across all existing controllers/nodes to avoid any performance hotspot.
12	Heterogenous support for end user systems	Operating system support RedHat Linux, Suse Linux, Windows Servers 2003/2008 or later , Windows XP/7 or later.
13	Management Interface software	Support the management, administration and configuration of the whole storage platform through a GUI based management interface along with CLI
14	Security	<ul style="list-style-type: none"> - The system must support encrypting data at rest. - The system must support Role Base Access Control with Integration with Active Directory/ LDAP
16	Warranty	5 years comprehensive OEM onsite warranty
17	Investment Protection	Storage System quoted by the OEM to be in the Leaders Quadrant in the latest Gartner Magic Quadrant for storage system/ OEM should be in the Top5 Global latest revenue report from IDC

Note: SI is expected to carry out the storage requirement estimation and supply as per the solution proposed, if the estimation is more than above specified

5.2.1.16. Functional & Technical Requirements for Unified Storage

Parameters	Description
Type of Storage System	<p>Storage Array (should be a purpose built appliance)should be unified storage with a single microcode / Operating system. Proposed Storage shall be the latest/enterprise generation storage from the respective OEM.</p> <p>The storage array must support block, file services and VVOL natively or by providing addon gateway/controllers in redundant configuration.</p>
Capacity	<p>Total 1 PB usable storage capacity to be offered.</p> <p>100 TB Usable using SSD Drive of size less than 4TB. Raid 5/6 can be used to provision this capacity.</p> <p>900TB Usable using NL-SAS Drive of size less than 12TB. RAID 6 must be used to provision this capacity</p> <p>The storage must be able to support atleast 300 SSD and 500 SAS/NL-SAS Disks.</p>
RAID Functionality	Storage should have RAID levels support for RAID 6

Cache Memory	Proposed storage shall have atleast Dual active-active controllers with minimum 500GB primary DRAM cache DRAM cache shall be protected with Cache destaging or battery backup. Entire Cache shall support both Read and Write IO operations dynamically. In the event of single controller failing, array shall not go to write through mode for proposed configuration.
Availability	The system shall have Fully Redundant & Hot Swappable Fans & Power Supplies. There shall have support for Non-Disruptive Microcode/firmware Update and upgrade & Non- Disruptive Parts Replacement
Licenses	Storage Array should be proposed with licenses for the entire capacity supported by the array from day1 for features such as Auto-Tiering, thin provisioning,, Point in time snapshot and restore, Sync and Async Replication for both Block and File Protocols, Data at Rest Encryption.
Encryption	The Storage array must be provided with controller based Data at Rest Encryption solution or SED based encryption to encrypt data on all drives. Solution should be supplied with embedded key management solution or external key management solution.
Ports	Storage System should be supplied with below configuration across controllers:-
	a. 8 x 16 Gbps FC Ports
	b. 4x12Gbps SAS ports for backend disk connectivity
GUI Application	The storage management software should display graphical depiction of storage hardware components with capability of tracking system and state information.
Snapshots	SAN should support minimum 500 snapshots .
Hosts	The storage shall be support current versions of Linux, Windows, VMWare etc.
Protocol Support	The storage shall support FC Protocol, iSCSI and file protocols NFSv3, NFSv4, NFSv4.1; CIFS (SMB 1), SMB 2, SMB 3.0, SMB 3.02, and SMB 3.1.1; FTP and SFTP
Storage Functionality	The storage system shall support advanced virtualization capabilities of combining storage from multiple RAID groups into a single pool and provision volumes from these pools. The Storage System shall have the ability to expand LUNS and Pools non-disruptively.
Replication Software	The Storage System shall support Synchronous & Asynchronous Replication for both Block .
Quality of Service	The Storage should have the capability to provide Quality of Service (QoS) feature to limit IOPS, , MB/sec and Response time or Throughput for test/dev hosts so that they do not use beyond permitted resources
Predictive	Storage OEM shall provide software-as-a-service cloud management

Analytics	dashboard that provides monitoring and reporting multiple storage system, VMware environment
Support	The Storage array must be proposed with 5 years of Storage OEM Warranty Services 24x7x365. Storage OEM must have an operational office in India from last 10 years.
Business Continuity	The partner must have office in India since last 10 years and must be having 100 support/services resources on direct payroll and OEM should have local support offices in India Storage software, hardware and support all should come from same and single OEM

5.2.1.17. Functional & Technical Requirements for Backup Appliance

S. No.	Purpose Built Backup Appliance Specifications
1	Proposed disk based backup appliance should be able to interface with various industry leading server platforms, operating systems and Must support LAN/SAN based D2D backup / VTL backup simultaneously via NFS v3, CIFS, FC , OST /NDMP protocols.
2	Proposed appliance should support global and inline data duplication using automated variable block length deduplication technology.
3	Proposed appliance should be offered with protocols like VTL/ OST/CIFS and NFS. All of the protocols should be available to use concurrently with global deduplication for data ingested across all of them.
4	Proposed appliance should support industry leading backup software like EMC Networker, Symantec Netbackup, Commvault and HP Data Protector etc and should Support deduplication at backup server/ host / application level so that only changed blocks travel through network to backup device.
5	Proposed appliance should be sized appropriately for backup of front end data 100 TB (50% DB and 50% File System) data as per below backup policies a. Daily Incremental Backup – retained for 4 weeks in disk based backup appliance. b. Weekly Full Backup for all data types – retained for 3 months in disk based backup appliance. c. Monthly Full Backups – Retained for 12 Months in the same disk based backup appliance. d. Yearly Full Backups - Retained for 7 years in the same disk based backup appliance. The Purpose built backup appliance should be quoted with adequate capacity with 15% YoY data growth and 3% daily change rate for entire duration of 5 years warranty. Any additional software or backup storage capacity (in addition to minimum 50 TB

	usable capacity) or any other component required as per sizing needs to be provided by the OEM & bidder during the entire warranty period of 5 years.
6	Proposed Appliance should have the capability to tier backup data in deduplicated format to an external cloud storage (on premise / public cloud).
7	Proposed appliance should have the ability to perform different backup, restore, replication jobs simultaneously and Must supports communications and data transfers through 8GB SAN, 10 Gb & 1 Gb ethernet LAN over copper and SFP+. The proposed backup appliance should be offered with min. 2 x 1Gbps NIC, 4 x 10Gbps NIC and 4 x 16Gbps FC ports and should support redundant controller for high availability of appliance in future.
8	Proposed appliance should support minimum backup throughput of 30 TB/hr while maintaining a single deduplication pool with RAID 6
10	Proposed appliance should support retention lock (WORM) feature which ensures that no data is deleted accidentally and support for point-in-time copies of a LUN or volumes with minimal performance impact.
11	Proposed disk appliance should be offered with battery backed up RAM / NVRAM for protection against data loss in power failure scenario and continuous automated file system check to ensure data integrity.
12	Proposed appliance should Support Enterprise Applications and Database Backups without integration with Backup Software, for better visibility of Backups to Application and database Owners, thus ensuring faster and direct recovery on application/database level. This integration should be available for Oracle, SAP, SAP HANA, DB2, MS SQL, Hadoop, MongoDB, Cassandra etc.
13	Proposed appliance should support bi-directional, many-to-one, one-to-many, and one-to-one replication.
14	Proposed appliance should support 128 bit AES encryption for data at rest and data-in-flight during replication. It should offer internal and external key management for encryption.
15	Proposed appliance should be offered RAID-6 with SAS/SATA/NL-SAS disk drives along with hot-spare disks in the ratio of 15:1 or better.
16	Proposed appliance should be offered with Multi-Tenancy features which provides a separate logical space for each tenant user while maintaining a global deduplication across data from all tenant users.

17	Purpose built backup appliance should offered with 24x7- 5 years onsite warranty support.
18	Proposed backup software should be available on various OS platforms like Windows, Linux, HP-UX, IBM AIX, Solaris etc. The backup server should be compatible to run on both Windows and Linux OS platforms
19	The backup software should be able to encrypt the backed up data using 256-bit AES encryption on the backup client and should not demand for additional license, any such license if needed should be quoted for the total number of backup clients asked for.
20	The backup solution should also support online LAN Free SAN based backups of databases through appropriate agents; Important Applications being Oracle, Microsoft SQL Server, Exchange, SharePoint, IBM DB2 UDB, Informix, Lotus Notes/Domino, MySQL, SAP, SAP HANA & Sybase etc.
21	Should able to dynamically break up large savesets into smaller savesets to be backed up in parallel to allow backups to complete faster for Windows, Unix and Linux clients.
22	Should have in-built calendar based scheduling system and also support check-point restart able backups for file systems. It should support various level of backups including full, incremental, differential, synthetic and virtual synthetic backups
23	The proposed backup software should have the capability to enable WORM on the backup sets from the backup software console on proposed disk backup appliance
24	The solution must support client-direct backup feature for file system, applications and databases to reduce extra hop for backup data at backup/media server to cater stringent backup window.
25	Bidder should provide 150TB capacity based licenses. SI need to provide backup solution on the offered IT Infra stack from single OEM for backup software & purpose built backup appliance.
26	Must have Agent/Modules for online backup of applications and databases such as MS SQL, Oracle, Exchange, Lotus, DB2, Informix, Sybase, Sharepoint, Meditech and SAP. Must support NAS and storage array based snapshot backup for off host zero downtime and zero load on the primary backup client with wizard based configuration.
27	Backup Solution must support multi tenancy feature for creation of distinct data zones where the end users have access without being able to view data, backups, recoveries, or modify in other data zones.

28	Backup Solution should also have configurable ReST API support for management, administration and reporting on backup infrastructure via custom applications and out of box integration with VMWare vRealize Automation for complete orchestration.
29	The proposed backup software should support restore a single VM, single file from a VM, a VMDK restore from the same management console for ease of use.
30	Proposed backup software should not need a physical proxy server for VMWare backups and should have a minimum of 16 concurrent sessions capability for the VMWARE VM machines image based backups with single virtual proxy. It should support instant access of a VM machine.
31	The proposed solution should have inbuilt feature for extensive alerting and reporting with pre-configured and customizable formats. The proposed solution must have capability to do trend analysis for capacity planning of backup environment not limiting to Backup Application/Clients, Virtual Environment, Replication etc.
32	The proposed backup software should be able to recreate backed up data from existing volumes from metadata backups. The solution should offer recovery of specific volumes for recovery from metadata in case of a disaster recovery.
33	The proposed Backup software should have the capability for Block based backups with granular recovery capability for Windows, Linux, Hyper-V, VMWARE and Exchange for faster backups on supported Disk platforms.
34	The proposed backup solution should provide search capability from a web portal to allow search for a single file from complete backup store.
35	The solution should be capable of integration with active directory infrastructure for ease of user rights management along with role based access control to regulate the level of management.
36	The solution should have the capability to manage and monitor backups at remote locations from a single backup server, where clients can backup data to a local disk backup device without the need of local media server or sending primary backup copy over the WAN.
37	The solution should have the capabilities to backup as well as archive data to cloud with cloud service providers like Azure / Amazon etc. In addition to this if data has to be moved from Cloud A to Cloud B the solution should be capable of cloud portability.
38	Proposed backup software should be in leader's quadrant of 2017 Gartner report for Enterprise Backup software and recovery solutions.
39	Software updates and patches: For the period of minimum 5 years.

40	Use of Source and Target Based De-duplication for Backups. In order to improve the backup performance and reduce the disk footprint for storing backup data, the disk-appliance solution proposed by the Bidder must support inline global de-duplication and must integrate with the backup software to facilitate client direct backups to the backup disk with source based de-duplication to reduce data transfer over IP and FC Networks.
41	Replication of the Backup Data. The backup solution at DC shall allow automated scheduled replication to remote site (DR) for facilitating Disaster Recovery copy of backup data at DC.

5.2.1.18. Functional & Technical Requirements for Aggregation Switches

S. No	Technical Specifications of L2 switch - 24 port POE+ Switch
1	Shall be 1U/2U Rack Mountable. Should have required accessories for rack mounting should have internal redundant power supply from day 1
2	Should have 24x RJ45 10/100/1000Mb POE+ auto-sensing ports, 4 x SFP+ ports. Switch should have minimum 400 watt power support for POE devices.
3	Should be able to support stacking with 40Gbps or better stack bandwidth. Cables & stacking ports to be provided from day one and should support minimum 4 switch in one stack for single IP management (stacking port should be dedicated stacking port)
4	Should be a non-blocking switch with Switch fabric capacity: 128Gbps and forwarding rate of 95 Mpps
5	Should have minimum 16000 MAC address entries, minimum 500 VLANs.
6	Switch should have Static routing and RIP feature from day one.
7	Should have LAG load balancing, double VLAN tagging.
8	Should have dual firmware images/software images on board. USB port for easy config & firmware image upload
9	Should support Time Based ACLs, MAC based ACLs and minimum 256 ACL rules from day 1.
10	Should have Flow based QoS, DiffServ, port based QoS, WRR/SDWRR, strict queue scheduling or equivalent
11	Should support UDLD, Jumbo frame 9K

12	Should support STP, MSTP, minimum 4 hardware queues per port, SP queuing or equivalent, LLDP-MED.
13	Should have 802.1x, RADIUS, TACACS+, IGMP v1/v2/v3 snooping
14	Should have RSPAN or equivalent, Private VLAN & Auto VLAN/voice VLAN or equivalent
15	Switch should be manageable through NMS on per port/switch basis. Should Support SNMP, RMON, SSH, telnet, web management, network management software.
16	Sflow/netflow, captive portal
17	Switch should have 1GB RAM for its smooth operations
18	Should operate at 220VAC ~50Hz. Switch Should support internal RPS (Redundant power supply)
19	Should be RoHS/REACH, 802.3az EEE compliance. The switch should be EAL/NDPP/NDcPP/FIPS certified

5.2.1.19. Functional & Technical Requirements for 24 Port L3 Switch

S.No.	Technical Specifications of Layer 3 switch - 24 port 1Gig Fiber Switch
1	Shall be 19" Rack Mountable. Should have required accessories for rack mounting.
2	Should have 24x 1gig Fiber SFP ports, 4 x SFP+ ports. Switch should support 1gig Rj45, 1gig LX, 1 gig SX, 10gig SX, 10gig LX. Switch Should be populated with 24 x 1gig LX transceivers and 4 x 10Gig LR.
3	Should be able to support stacking with 80Gbps stack bandwidth. Cables & stacking ports to be provided from day one and should support minimum 4 switch in one stack for single IP management
4	Should be a non-blocking switch with Switch fabric capacity: 128Gbps and forwarding rate of 95 Mpps
5	Should have minimum 16000 MAC address entries, minimum 1000 VLANs.
6	Switch should have Layer 3 features Static routing, OSPF, BGP, PBR, VRRP for both IPv4 and IPv6 feature from day one.
7	Switch should have PIM-SM/PIM-SSM/DM and VRF-lite from day one
8	Should have LAG load balancing, double VLAN tagging.
9	Should have dual firmware/software images on board. USB port for easy config & firmware image upload

10	Should support port Based ACLs, MAC based ACLs and minimum 256 ACL rules from day 1.
11	Should have Flow based QoS, DiffServ, port based QoS, WRR/WDRR, strict queue scheduling
12	Should support UDLD or equivalent, Jumbo frame 9K
13	Should support STP, MSTP, minimum 8 hardware queues per port, SP queuing or equivalent, LLDP-MED.
14	Should have 802.1x, RADIUS, TACACS+, IGMP v1/v2/v3 snooping
15	Should have RSPAN/ Mirroring, Private VLAN & Auto VLAN/voice VLAN or equivalent
16	Switch should be manageable through NMS on per port/switch basis. Should Support SNMP, RMON, SSH OR telnet, web management or network management software.
17	Sflow or Jflow or Netflow
18	Switch should have 2GB RAM for its smooth operations
19	Should operate at 220VAC ~50Hz. Switch Should have dual internal power supply.
20	Should be RoHS/REACH, 802.3az EEE compliance. The switch should be EAL/NDPP/NDcPP/FIPS certified

5.2.1.20. Functional & Technical Requirements for PoE Ruggedized Switches

S.no	Requirement
1	Shall have 2* 100/1000BaseSFP Single mode ports,10 KM Support with LC connectors, 8 No's of 10/100/1000 BaseT(X) copper ports (RJ45 connectors)
2	IPv6 Ready logo awarded
3	8 IEEE 802.3af and IEEE 802.3at PoE+ standard ports • 190 watt output
4	Advanced PoE management function like (PoE port setting, PD failure check, and PoE scheduling)
5	IEEE 1588 PTPV2(Precision Time Protocol) for precise time synchronization of networks
6	DHCP Option 82 for IP address assignment with different policies
7	Ethernet/IP, PROFINET, and Modbus/TCP protocols for device management and monitoring

8	Should have Ring support with 8 switches in One Single Ring and have recovery time of <50ms.
9	IGMP snooping and GMRP for filtering multicast traffic from industrial Ethernet protocols
10	IEEE 802.3ad, LACP for optimum bandwidth utilization
11	Bandwidth management prevents unpredictable network status
12	Lock port to restrict access to authorized MAC addresses
13	Multi-port mirroring for online debugging
14	Automatic warning by exception through email, relay output
15	Line-swap fast recovery
16	RMON for efficient network monitoring and proactive capability
17	QoS (IEEE 802.1p/1Q) and TOS/DiffServ to increase determinism
18	Configurable by web browser, USB-serial console
19	Works with Industrial network management software
20	System backup and restoration tool to enhance maintenance efficiency and reduce system downtime.
Cyber-security Features	
21	User passwords with multiple levels of security protect against unauthorized configuration Command line interface (CLI/local Access) for quickly configuring major managed functions: More than 200 command lines
22	SSH/HTTPS is used to encrypt passwords and data
23	Lock switch ports with 802.1x port-based network access control so that only authorized clients can access the port
24	Disable one or more ports to block network traffic
25	802.1Q VLAN allows you to logically partition traffic transmitted between selected switch ports VLAN Unaware: Supports priority-tagged frames to be received by specific devices
26	Secure switch ports so that only specific devices and/or MAC addresses can access the ports
27	Radius/TACACS+ allows you to manage passwords from a central location

28	SNMPv3 provides encrypted authentication and access security
PROTOCOLS	
30	IGMPv1/v2/v3, GMRP, GVRP, SNMPv1/v2c/v3, DHCP Server/Client, DHCP Option 66/67/82, BootP, TFTP, SNTP, SMTP, RARP, RMON, HTTP, HTTPS, Telnet, SSH, Syslog, EtherNet/IP, PROFINET, Modbus/TCP, SNMP Inform, LLDP, IEEE 1588, IPv6, NTP Server/Client
MIB	
31	MIB-II, Ethernet-Like MIB, P-BRIDGE MIB, Q-BRIDGE MIB, Bridge MIB, RSTP MIB, RMON MIB Group 1, 2, 3, 9
FLOW CONTROL	
32	IEEE 802.3x flow control, back pressure flow control
SWITCH PROPERTIES	
33	Priority Queues 4
34	IGMP Groups 2048
35	MAC Table Size: 8 K
36	Jumbo Frame Size: 9.6 KB
37	Packet Buffer Size: 1 Mbit
38	Max. Number of Available VLANs more than 200
39	VLAN ID Range VID 1 to 4094
40	Alarm Contact 1 relay outputs with current carrying capacity of 1 A @ 24 VDC
41	LED Indicators: PWR1, PWR2, FAULT, STATE, 10/100/1000M, MSTR/ HEAD, CPLR/TAIL
42	Digital Inputs: Digital Inputs: 1 input with the same ground, but electrically isolated from the electronics. • +13 to +30 V for state “1” • -30 to +3 V for state “0” • Max. input current: 8 mA
43	Console Port: USB-serial console Storage Port: USB storage
44	Overload Current Protection

45	Reverse Polarity Protection
46	Button: Reset button
	ENVIRONMENTAL
47	Operating Temperature: -4to 70°C
48	Humidity 15 to 95 %(non-condensing)
49	Mounting : DIN-Rail mounting, wall mounting (with optional kit)
50	Housing: Metal, IP30 protection
INPUT VOLTAGE	
51	Input Voltage: 48 VDC (46 to 57 VDC), redundant dual inputs
Standard and Certifications	
52	Safety: UL 508, EN60950-1 (LVD) EMI: FCC Part 15 Subpart B Class A, EN 61000-6-4 (Industrial) EMS: EN 61000-6-2 (Industrial), EN 61000-4-2 (ESD) Level 4, EN 61000-4-3 (RS) Level 3, EN 61000-4-4 (EFT) Level 4, EN 61000-4-5 (Surge) Level 4, EN 61000-4-6 (CS) Level 3, EN 61000-4-8 Rail Traffic: EN 50121-4 Shock: IEC 60068-2-27 Freefall: IEC 60068-2-32 Vibration: IEC 60068-2-6 NEMA-TS2
53	MTBF : More than 300,000 hrs
	OEM or their distributor should have Service /Support network in India since last 5 years OEM should furnish Test Report/Certificate against the Standards/Approval demanded under OEM Should have installation base of 1000 Industrial Switches in India since past 10 years

5.2.1.21. Functional & Technical Requirements for Online UPS - 100 KVA

Sr. No.	Specifications	Requirement
1	Capacity (in kVA)	100 Kva / 100 kW , 3-Phase Input / 3-Phase Output UPS in N+N. Each Cabinet of 60kva UPS shall be expandable upto min 120kva/120kW
2	Technology and Capability	a) True Online configuration double conversion UPS with 3-Level Inverter Technology b) Modular & Scalable UPS with hot swappable Power Module of rating of 20kW. Each module should have full rated rectifier, inverter & charger (no discrete or granule 1Ph design will be accepted) c) Hot Swappable STS Module & Control Module d) Parallel capability up to Six no. of Power Modules for Vertical redundancy & up to eight UPS units for capacity. e) Redundant System with optional redundant controller, Dual Aux Power Supply. f) Dual CAN Bus within frame & redundant CAN Bus between parallel systems to enable UPS to be removed or inserted UPS in parallel configuration without need of transferring it to bypass mode g) Green (i.e Sleep) mode of operation to improve operational efficiency (>96%) on varying & dynamic loading conditions without compromising the redundancy required in the application. h) Top & Bottom cable Entry options. i) DSP (Digital Signal Processor) / Microprocessor based control, using IGBT devices and high switching frequency PWM j) Capability of independent or common battery bank operation of the UPS when operated in Parallel Redundant System. k) Brushless DC Fans with speed control l) Energy Recycle Mode that enables testing of the unit for load testing without external load & helps in Load simulation
4	Input	
4.1	Input facility - Phases / Wires	3-Phase / 4-Wire & Gnd (R, Y, B -Phases & Neutral + Ground)

4.2	Nominal Input Voltage	380 / 400 / 415V AC
4.3	Input Voltage Range	305 - 477 V AC for 100% load
4.4	Nominal Input Frequency	50 / 60 Hz (Auto selectable)
4.5	Input Frequency Range	40-70 Hz
4.6	Input Power Factor	> 0.99 on Full resistive load Load
4.7	Input Current Harmonic Distortion (THDi)	< 3% on Full Load (with Mains Vthd less than 1%)
5	Output	
5.1	Nominal Output Voltage	380 / 400 / 415V AC (Selectable)
5.2	Output Voltage Regulation	+/- 1%
5.3	Nominal Output Frequency	50 / 60 Hz (Selectable)
5.4	Output Frequency Regulation	+/- 0.05 Hz (Free Running / Self Clocked Mode) + / - 5 % (Synchronized to Mains Mode, Selectable)
5.5	Output Frequency Slew Rate	1 Hz / s
5.6	Output Wave Form	Pure sine wave
5.7	Output Voltage Distortion (Vthd)	<= 1% (For 100% Linear / Resistive Load) <= 5% (For 100% Non-Linear / RCD Load)
5.8	Crest Factor	3 : 1 On Full Load
5.9	Unbalanced load on phases	100% unbalanced load should be allowed
5.1	Displacement angle for 100% balanced Load	120 deg +/- 2 deg

6	Transient Response / Recovery	
6.1	Transient response:	+/- 5% (Dynamic regulation for 0% to 90 % step load)
7	Transfer Time	
7.1	Transfer Time (Mode of operation)	Nil from Mains mode to Battery Mode
		Nil from Battery Mode to Mains mode
7.2	Transfer Time (Inverter to Bypass / Bypass to Inverter)	< 1 ms (Synchronized Mode)
		10 ms (Asynchronized Mode)
7.3	Automatic & Bi-directional static by-pass (In-built)	Uninterrupted transfer of load from Inverter to bypass (under overload / fault conditions) & automatic retransfer from bypass to inverter (on removal of overload / fault conditions)
8	Efficiency (At Nominal Voltage & Resistive Load up to kW rating of UPS)	
8.1	Overall Peak Efficiency	96 % (AC to AC) - Online (Double Conversion)
8.2	Overall Efficiency	95% (AC to AC) - Online (Double Conversion) on 25% Loading
8.3	Eco mode efficiency	99%
9	Overload	
9.1	Inverter Overload capacity	125% for 10 minutes; 150% for 60 seconds, > 150% for 1 sec (Mains Mode & Battery Mode)
10	Display Panel (In-built min. 8.5 inch Touch Display)	
10.1	Measurements (On 10" Touch Display)	Input: Voltage /Current/ Frequency
		Bypass: Voltage /Current/ Frequency
		Output: Voltage / frequency / Current
		Battery: Voltage / Capacity
		Load: In kVA / kW / Percentage
		Temperature: STS/Inverter/PFC

10.2	Event Logging & Statistical Data (On LCD): UPS should capture and display upto 10000 events	Events Logs (min. 8500 events) like: Over temperature / DC Bus Fail / Fan Fail / Fuse Fail / Overload / Short-circuit / Device Fail / Inverter Fail / Rectifier Fail / Bypass Fail, etc Statistical Data: No. of power failures / Transfers to Bypass / Total Running time, etc
10.3	User Programmable Parameters & Settings (On Touch Display)	Bypass: Voltage / Frequency Range
		Inverter: Voltage / Frequency / Eco Mode / Frequency converter
		Battery: Type / Banks / Chargers Current / Manual & Automatic Testing
		Mode selection : online Mode, Green Mode, ECO Mode, Energy Recycle Mode & Frequency conversion mode
		Auto Equalize charge enable/disable option with selectable interval
		Alarms: Buzzer Test / Buzzer Mute
		Date & Time Setting
		Password: User / Administrator Setting
		Information: UPS Serial No. / Firmware
		Log & Statistical Data Reset & Firmware upgrade
11	Alarms	
11.1	Audible Alarms	Mains Failure / Battery Low Alarm / UPS Overload / Fault / Short circuit
12	Battery Bank	LiB (Lithium Ion) – <u>with 10 years warranty</u>
12.1	Backup Required	30 minutes on 100kVA taking @ 0.8 power factor & considering 80% DOD
12.3	Model & Cell Type/Cell Configuration	3.7V Prismatic Type , 1 P Series Type Configuration (or as per Battery OEM)
12.4	Chemistry of Cell composition	It should be NMC or LMO type only. LiFePO4 shall not be considered
12.5	Module	51.8V 60Ah (or higher Ah), Pluggable Type with metal casing
12.6	Individual Rack Nominal Capacity in Ah	2 string of 60Ah (or higher Ah) as Single Rack capacity (similar to 42U size with 600(W) X2000(H)mm)

12.7	Cycle Life at 80% DOD at 25deg C	2500 cycles (at 80% DOD at 25degC)
12.8	Battery Management System (BMS)	2 Level BMS Design (Module CMU & Rack BMU)
12.9	Switchgear & SMPS assembly	Integrated Switchgear & SMPS assembly inbuilt with in each rack, Dual auxiliary power supply(DC & AC)
12.10	Mandatory Safety Certifications/ compliances	IEC 62619 or equivalent, UN38.3
12.11	Safety Features in LiB Cabinet	MCCB to be present in individual rack & Should have inbuilt protection for Overcurrent, short circuit, Overvoltage, under-voltage & over temperature
12.12	Communication Scheme with UPS	BMS Level/communication protocol integration & communication scheme. UPS Touch Display should show Cell level & Pack Level Voltage/temperature, State of charge (SOC), Remaining Time.
12.13	Communication Bus	CAN2.0/RS485
12.14	Charging time	90% of capacity within 4 to 4.5 hrs
12.15	Environment Operation Temperature	Charge: 0°C ~ +45°C Discharge: -20°C ~ +45°C
13.1	Drycontact/ communication Ports	Output Dry contact :6 configurable for 21 events including Battery breaker shunt trip, backfeed protection EPO activated Input Dry contact: 4,ParallelPort : 4, REPO, External battery Temperature sensor : 4 ,External switch Breaker status: 4 ,USB Port & RS232 Port ,SMART slot for more no. of Dry contacts, Integrated MODBUS/SNMP card
14	Restart / Testing Capability	
14.1	Automatic Restart	UPS should start up automatically on mains resumption after battery low shutdown
14.2	Battery Self Test	Manual / Scheduled battery test to ensure healthiness of batteries.
15	Physical	

15.1	Operating Temperature	0 to 40 deg C full load
15.2	Storage Temperature	-25 to 70 deg C
15.3	Operating Humidity	0 to 95% RH (Non-condensing)
15.4	Operating Altitude	1000 m (meters above sea level) without derating, Derating 1% for each additional 100m.
15.5	Protection Class	IP – 20
15.6	Type of Cooling	Forced Air
15.7	Noise Level	< 65 dbA at 1 meter distance
15.8	Form Factor	Free Standing Floor Mounted UPS
15.9	Dimension (w x d x h) in mm	Vendor to Furnish
15.10	Weight - in kg	Vendor to Furnish
15.11	Reliability	MTBF greater than 350000 hours
15.12	Connections - Rectifier Input / Output / Bypass Input / Battery	Breakers for input , Output, Bypass & Maintenance bypass
16	Certifications	
16.1	Manufacturer	QMS: As per ISO 9001
		EMS: As per ISO 14001
		ISO 45001/50001
		NABL type test for the same model or OEM shall have to submit report from own factory having NABL Accredited Factory calibration in India
		Proven solutions required. OEM shall have supplied and installed min. 20 sets of UPS (above 100kva or more) with Li-Ion batteries (of same Chemistry asked) in India with Hot-Swap Modular UPS Systems in last 3 years
		OEM shall have manufacturing from last 10 years or more in India for Modular UPS Systems
16.2	Product	Safety: As per IEC62040-1

		EMC: As per IEC62040-2
		Performance : As per IEC62040-3
		ESD: As per IEC61000-4-2 Level 4
		RF: As per IEC61000-4-3 Level 3
		FT/Burst: As per IEC61000-4-4 Level 4
		Surge: As per IEC61000-4-5 Level 4
		CE Declaration of Conformance

5.2.1.22. Functional & Technical Requirements for Online UPS - 300 KVA

Sr. No.	Specifications	Requirement
1	Capacity (in kVA)	300 kVA/kW, 3-Phase Input / 3-Phase Output UPS with frame capacity (width max. 600mm of frame)
2	Technology and Capability	a) True Online configuration double conversion UPS with 3-Level Inverter Technology b) Modular & Scalable UPS with hot swappable Power Module of rating of 30 to 50kW. c) Hot Swappable STS Module & controller Module d) Redundant System with hot swappable dual controllers & Dual Aux Power Supply. e) Dual CAN Bus within frame & redundant CAN Bus between parallel systems to enable UPS to be removed or inserted UPS in parallel configuration without need of transferring it to bypass mode f) Green mode of operation to improve operational efficiency (>96%) on varying & dynamic loading conditions without compromising the redundancy required in the application. g) Top & Bottom cable Entry options shall be available without addition of any extra cabinet h) DSP (Digital Signal Processor) / Microprocessor based control, using IGBT devices and high switching frequency PWM

3		i) Capability of independent or common battery bank operation of the UPS when operated in Parallel Redundant System.
		j) Brushless DC Fans with speed control
		h) Energy Recycle Mode that enables testing of the unit for load testing without external load & helps in Load simulation
		i) Inbuilt Breakers for input, output, bypass & Maintenance Bypass within the same UPS Cabinet
4	Input	
4.1	Input facility - Phases / Wires	3-Phase / 4-Wire & Gnd (R, Y, B -Phases & Neutral + Ground)
4.2	Nominal Input Voltage	380 / 400 / 415V AC
4.3	Input Voltage Range	305 - 477 V AC (on full load) 242- 477 V AC (< 70% Loading)
4.4	Nominal Input Frequency	50 / 60 Hz (Auto selectable)
4.5	Input Frequency Range	40-70 Hz
4.6	Input Power Factor	> 0.99 on Full resistive load Load
4.7	Input Current Harmonic Distortion (THDi)	< 3% on Full Load (with Mains Vthd less than 1%)
5	Output	
5.1	Nominal Output Voltage	380 / 400 / 415V AC (Selectable)
5.2	Output Voltage Regulation	+/- 1%
5.3	Nominal Output Frequency	50 / 60 Hz (Selectable)
5.4	Output Frequency Regulation	+/- 0.05 Hz (Free Running / Self Clocked Mode) +/- 5 % (Synchronized to Mains Mode, Selectable)

5.5	Output Frequency Slew Rate	1 Hz / s
5.6	Output Wave Form	Pure sine wave
5.7	Output Voltage Distortion (THDv)	<= 2% (For 100% Linear / Resistive Load)
		<= 5% (For 100% Non-Linear / RCD Load)
5.8	Crest Factor	3 : 1 On Full Load
5.9	Unbalanced load on phases	100% unbalanced load should be allowed
5.1	Displacement angle for 100% balanced Load	120 deg +/- 2 deg
6	Transient Response / Recovery	
6.1	Transient response:	+/- 5% (Dynamic regulation for 0% to 90 % step load)
7	Transfer Time	
7.1	Transfer Time	Nil from Mains mode to Battery Mode Nil from Battery Mode to Mains mode
7.2	Transfer Time (Inverter to Bypass / Bypass to Inverter)	< 1 ms (Synchronized Mode) < 10 ms (Asynchronized Mode)
7.3	Automatic & Bi-directional static by-pass (In-built)	Uninterrupted transfer of load from Inverter to bypass (under overload / fault conditions) & automatic retransfer from bypass to inverter (on removal of overload / fault conditions)
8	Efficiency (At Nominal Voltage & Resistive Load up to kW rating of UPS)	
8.1	Overall Peak Efficiency	96.5% (AC to AC) - Online (Double Conversion)
8.2	Overall Efficiency	95.5 % (AC to AC) - Online (Double Conversion) on 25% Loading
8.3	Eco mode efficiency	99%
9	Overload	

9.1	Inverter Overload capacity (Mains Mode & Battery Mode)	125% for 10 minutes 150% for 60 seconds, > 150% for 1 sec
10	Display Panel (In-built min. 8.5 inch Touch Display)	
10.1	Measurements (On Touch Display)	Input: Voltage /Current/ Frequency
		Bypass: Voltage /Current/ Frequency
		Output: Voltage / frequency / Current
		Battery: Voltage / Capacity
		Load: In kVA / kW / Percentage
		Temperature: STS/Inverter/PFC
10.2	Event Logging & Statistical Data (On Touch LCD):	Events Logs (min. 8000 events) like: Over temperature / DC Bus Fail / Fan Fail / Fuse Fail / Overload / Short-circuit / Device Fail / Inverter Fail / Rectifier Fail / Bypass Fail, etc Statistical Data: No. of power failures / Transfers to Bypass / Total Running time, etc
10.3	User Programmable Parameters & Settings (On Touch Display)	Bypass: Voltage / Frequency Range
		Inverter: Voltage / Frequency / Eco Mode / Frequency converter
		Battery: Type / Banks / Chargers Current / Manual & Automatic Testing
		Mode selection : online Mode, Green Mode, ECO Mode, Energy Recycle Mode & Frequency conversion mode
		Auto Equalize charge enable/disable option with selectable interval
		Alarms: Buzzer Test / Buzzer Mute
		Date & Time Setting
		Password: User / Administrator Setting
		Information: UPS Serial No. / Firmware
		Log & Statistical Data Reset & Firmware upgrade
11	Alarms	
	Audible Alarms	Mains Failure / Battery Low Alarm / UPS Overload / Fault / Short-circuit

12	Battery Bank	Lithium ion Battery – <u>with 10 years warranty</u>
12.1	Backup Required	30 minutes on 300kVA taking @ 0.7 power factor & considering 80% DOD
12.2	Make, Type, Model No.	Samsung/UPS OEM Make/L.G
12.3	Model & Cell Type/Cell Configuration	3.7V Prismatic Type , 1 P Series Type Configuration (or as per Battery OEM)
12.4	Chemistry of Cell composition	It should be NMC or LMO type only. LiFePO4 shall not be considered
12.5	Module	51.8V 60Ah(or higher Ah), Pluggable Type with metal casing
12.6	Individual Rack Nominal Capacity in Ah	5 x 60Ah (or higher Ah) as three Rack capacity (similar to 42U size with 600(W) X2000(H)mm)
12.7	Cycle Life at 80% DOD at 25deg C	2500 cycles (at 80% DOD at 25degC)
12.8	Battery Management System (BMS)	2 Level BMS Design (Module CMU & Rack BMU)
12.09	Switchgear & SMPS assembly	Integrated Switchgear & SMPS assembly inbuilt with in each rack, Dual auxiliary power supply(DC & AC)
12.10	Mandatory Safety Certifications/ compliances	IEC 62619 or equivalent, UN38.3
12.11	Safety Features in LiB Cabinet	MCCB to be present in individual rack & Should have inbuilt protection for Overcurrent, short circuit, Overvoltage, under-voltage & over temperature
12.12	Communication Scheme with UPS	BMS Level/communication protocol integration & communication scheme. UPS Touch Display should show Cell level & Pack Level Voltage/temperature, State of charge (SOC), Remaining Time.
12.13	Communication Bus	CAN2.0/RS485
12.14	Charging time	90% of capacity within 4 to 4.5 hrs

12.15	Environment Operation Temperature	Charge: 0°C ~ +45°C Discharge: -20°C ~ +45°C
13	Communication Interfaces	
13.1	Dry Contact / communication Ports	Output Dry contact :6 configurable for 21 events including Battery breaker shunt trip, Backfeed protection EPO activated Input Dry contact: 4, Parallel Port : 4, REPO, External battery Temperature sensor : 4 ,External switch Breaker status: 4 ,USB Port & RS232 Port ,SMART slot for more no. of Dry contacts, Integrated MODBUS/SNMP card
14	Restart / Testing Capability	
14.1	Automatic Restart	UPS should start up automatically on mains resumption after battery low shutdown
14.2	Battery Self Test	Manual / Scheduled battery test to ensure healthiness of batteries.
15	Physical	
15.1	Operating Temperature	0 to 40 deg. C full load, 0-45degC (output power derated to 85%)
15.2	Storage Temperature	-25 to 70 deg C
15.3	Operating Humidity	0 to 95% RH (Non-condensing)
15.4	Operating Altitude	1000 m (meters above sea level) without derating, Derating 1% for each additional 100m.
15.5	Protection Class	IP – 20
15.6	Type of Cooling	Forced Air
15.7	Noise Level	< 75 dbA at 1 meter distance
15.8	Form Factor	Free Standing Floor Mounted UPS
15.9	Dimension	Vendor to Furnish(w x d x h) in mm
15.10	Weight - in kg	Vendor to Furnish
15.11	Reliability	MTBF greater than 225000 hours
15.13	Connections - Rectifier Input / Output /	Integrated Breakers for Input, Bypass, Output & Maintenance Bypass.

	Bypass Input / Battery	
16	Certifications	
16.1	Manufacturer	QMS: As per ISO 9001
		EMS: As per ISO 14001
		ISO 45001/50001
		NABL type test for the same model or OEM shall have to submit report from own factory having NABL Accredited Factory calibration in India
		Proven solutions required. OEM shall have supplied and installed min. 20 sets of UPS (above 200kva or more) with Li-Ion batteries (of same Chemistry asked) in India with Hot-Swap Modular UPS Systems in last 3 years
		OEM shall have manufacturing from last 10 years or more in India for Modular UPS Systems
16.2	Product	Safety: As per IEC62040-1
		EMC: As per IEC62040-2
		Performance : As per IEC62040-3
		ESD: As per IEC61000-4-2 Level 4
		RF: As per IEC61000-4-3 Level 3
		FT/Burst: As per IEC61000-4-4 Level 4
		Surge:As per IEC61000-4-5 Level 4
		CE Declaration of Conformance

5.2.1.23. Functional & Technical Requirements for Online UPS – 1/2/3/5 KVA

S.No	Parameter	Minimum Specifications
1	OEM	ALL UPS including Field, DC and ICCS shall from the same OEM
2	Input voltage	shall be 1Ph
	Range	UPS upto 3kva - 175 to 280Vac for all 1P (Requires 60% load support @ 110Vac for UPS upto 3kva. (Input range shall be settable at site from 110 to 295Vac to match the incoming raw power)

		UPS 5kva - 50% load support @ 100Vac
3	Technology	DSP based technology
	Features	Cold Start, Auto Start & ECO mode
	Noise	below 52 db in all UPS upto 5kva
4	Output voltage	shall be 1Ph
	Voltage	for UPS upto 5kva – Single Phase 200/208/220/230/240Vac
5	Output Power Factor	
	a) for UPS upto 3kva	0.9
	b) 5kva UPS	Unity (UPS must have UNITY PF ONLY)
6	Efficiency	
	a) for below 5kva	Upto 89% for below 5kva
	b) for 5kva	Upto 95% for 5kva
7	Voltage THD	3% for Linear load & 6% for Non-linear load
8	Interface	RS 232 & USB for all rating
9	Display	LCD Display required for all UPS (Graphical type for 5kva)
10	Input Terminal	
	a) for UPS upto 3kva	Resettable
	b) for UPS 5kva	Breaker
11	Output Terminal	
	a) For upto 3kva	Indian Socket 10A(min 3nos) – for UPS below 5kva
	Programmable outlet	Min. One Programmable outlet in UPS
	b) for 5kva	Terminal for 5kva (one Programmable terminal desired in 5kva)
12	Overload	105% continue or better with warning for all rating 125% - 2 min or better
13	Charger	

	a) in UPS upto 3kva b) in UPS 5kva	Min 12A in UPS upto 3kva as to be used in remote or field Min. 6Amp inbuilt (or as higher w.r.t 10% capacity on battery Ah for UPS 5kva)
14	Battery Back-up time and VDC	
	a) For UPS upto 3kva – as per OEM	Back-up time - 60 minutes (on actual load at site, to be confirmed by SI) for all Field UPS
	b) For 5kva –	30 minutes for any indoor UPS. VDC - as per OEM but with variance from 16 nos to 22 nos at site. UPS shall also work with 12 batteries if desired at site with de-rated capacity
15	Dimension	Upto 3kva – Tower 5kva – Rack Mount 2U
16	Certification	For OEM ISO 9001, ISO 14001, ISO 45001/50001, Factory Calibration lab of manufacturer shall be NABL accredited

5.2.1.24. Functional & Technical Requirements for Online UPS - 500 VA

S.No.	Parameter	Minimum Specifications
1	OEM	ALL UPS including Field, DC and ICCS shall from the same OEM
2	Input voltage	shall be 1Ph
	Range	175 to 280Vac for all 1P (Requires 60% load support @ 110Vac for UPS (Input range shall be settable at site from 110 to 295Vac to match the incoming raw power)
3	Technology	DSP based technology
	Features	Cold Start, Auto Start & ECO mode
	Noise	below 52 db
4	Output voltage	shall be 1Ph - 200/208/220/230/240Vac
5	Output Power Factor	0.9
6	Efficiency	Upto 80%
7	Voltage THD	6% for Linear load & 10 % for Non-linear load

8	Interface	RS 232 & USB
9	Display	LCD Display
10	Input Terminal	Resettable
11	Output Terminal	Indian Socket 10A(min 3nos)
	Programmable outlet	Min. One Programmable outlet in UPS
12	Overload	105% continue or better with warning 125% - 2 min or better
13	Charger	Min 12A in UPS upto 3kva as to be used in remote or field
14	Battery Back-up time and VDC	36V - Back-up time - 60 minutes (on actual load at site, to be confirmed by SI) for all Field UPS
15	Dimension	Tower
16	Certification	For OEM ISO 9001, ISO 14001, ISO 45001/50001, Factory Calibration lab of manufacturer shall be NABL accredited

5.2.1.25. Functional & Technical Requirements for HIPS & NIPS

S.No.	Minimum Specifications
1.	Proposed solution should protect against distributed DoS attack and should have the ability to lock down a computer (prevent all communication) except with management server
2.	Should support stateful Inspection Firewall, Anti-Malware, Deep Packet Inspection with HIPS, Integrity Monitoring, Application Control and Recommended scan in single module with agentless and agent capabilities
3.	Firewall rules should filter traffic based on source and destination IP address, port, MAC address, etc. and should detect reconnaissance activities such as port scans and Solution should be capable of blocking and detecting IPv6 attacks and Product should support CVE cross-referencing when applicable for vulnerabilities.
4.	Should provide automatic recommendations against existing vulnerabilities
5.	Solution should support any pre-defined lists of critical system files for various operating systems and/or applications (web servers, DNS, etc.) and support custom rules as well
6.	Solution should have feature to take backup of infected files and restoring the same

S.No.	Minimum Specifications
7.	Host IPS should be capable of recommending rules based on vulnerabilities with the help of virtual patching and should have capabilities to schedule recommendation scan and entire features of solution should be agentless
8.	Product should support CVE cross-referencing when applicable for vulnerabilities.
9.	Host based IPS should support virtual patching both known and unknown vulnerabilities until the next scheduled maintenance window
10.	Should provide automatic recommendations against existing vulnerabilities, dynamically tuning IDS/IPS sensors (Selecting rules, configuring policies, updating policies) provide automatic recommendation of removing assigned policies if vulnerability no longer exists
11.	Solution should have Security Profiles allows Integrity Monitoring rules to be configured for groups of systems, or individual systems
12.	Should have pre and post execution machine Learning and should have Ransom ware Protection in Behavior Monitoring
13.	Demonstrate compliance with a number of regulatory requirements including PCI DSS, HIPAA, NIST, SSAE 16
14.	Management server should support Windows & Linux OS platforms
15.	Should be Common Criteria EAL 4 and FIPS 140-2 validated
16.	Machine Learning: Analyses unknown files and zero-day threats using machine learning algorithms to determine if the file is malicious
17.	Should have container security automated processes for critical security controls to protect containers and the Docker host
18.	Should automatically submit unknown files/suspicious object samples with On-Premise sandbox solution as per RFP specifications for simulation and create IOC's on real time basis as per sandboxing analysis and revert back to server security for mitigation
19.	OEM of proposed solution should have local 24x7 TAC support in India

S.No.	NIPS Minimum Technical Requirement
1	Intrusion Prevention System (IPS) should be based on purpose-built platform that has Field Programmable Gate Arrays (FPGAs). NIPS should be independent standalone and dedicated appliance based solution, NIPS should not be the part of firewall and UTM.
2	The NIPS appliance must have at least 40 Gbps inspection throughput, which includes SSL inspection. NIPS should have 2 * 40 GE QSFP+ and 8 * 10G SFP+ ports. NIPS solution should be in gartner leaders quadrant as per latest report.

S.No.	NIPS Minimum Technical Requirement
3	The NIPS must support 115,000,000 concurrent sessions and 6,50,000 new connections per second with latency should be <40 Micro.
4	The proposed IPS solution must support Adaptive Filter Configuration (AFC) and proposed IPS should support the ability to mitigate Denial of Service (DoS/DDoS) attacks such as SYN floods and proposed IPS solution must be able to provide zero-day filters that must be included in weekly signature update.
5	The IPS filter must support network action set such as Block (drop packet), Block (TCP Reset), Permit, Trust, Notify, Trace (Packet Capture), Rate Limit and Quarantine & proposed IPS solution must support signatures, protocol anomaly, vulnerabilities and traffic anomaly filtering methods to detect attacks and malicious traffic
6	The IPS filters must be categories into the following categories for easy management: - Exploits, Identity Theft/Phishing, Reconnaissance, Security Policy, Spyware, Virus, Vulnerabilities, Network Equipment, Traffic Normalization, Peer to Peer, Internet Messaging, Streaming Media
7	The proposed IPS must be able to support granular security policy enforcement based on the following methods: Per IPS device (all segments), Per physical segment uni-direction and bi-directional.
8	The proposed IPS must be able to control the known bad host such as spyware, botnet C2 server, spam and so on based on country of origin, exploit type and the reputation score.
9	The centralized management server for NIPS must be an appliance based on a hardened OS shipped by-default from factory and system shall allow the latest update to be manually, automatically or based on schedule with central management and reporting.
10	The proposed IPS solution must support fail open option to bypass NIC to bypass traffic even with the power on, in event of un-recoverable internal software error such as firmware corruption, memory errors. NIPS should able submit file to sandboxing for real time execution and sandboxing should be customized and able to support win 7, win 8, win 2008, win2012 at least.

5.2.1.26. Functional & Technical Requirement for SIEM

S.No.	Minimum Technical Specification
1	Intelligent next generation SIEM must be able to detect any anomalies, report in real time and take action as programmed having SIEM AND SOAR capabilities.
2	It must provide complete chain of custody by maintain Raw and Normalized logs for 6 Months and must deidentify logs at source itself using format preserving encryption in stateless mode to ensure log security end to end.
3	It must provide platform for orchestration and automation of response integrated for complete usage and for all devices and admins
4	Solution must be Sized for 20000 Sustained, 40000 Peak EPS with burst support for upto 50000 EPS without queuing or dropping any logs in three tiered physically segregated architecture consisting of Collection layer, log management layer and Correlation layer. SOAR Solution must support all devices as SIEM and no restriction on Admins.
5	The proposed solution must provide inline options to reduce event data at the source by filtering out unnecessary event data. Filtering must be simple string-based or regular expressions and must delete the event data before it is processed. Log Filtering needs to be available across all tier to filter out logs as wherever required.
6	Solution should have security orchestration and automated response engine bi-directionally integrated to reduce security incident MTTR (Mean Time To Respond) and automate L1/L2 security activities.
7	Proposed solution should have unified security data lake natively available to provide AI/ML based threat hunting and analytics capabilities
8	Proposed solution should support predictive analysis (data science enabled) by creating custom data models in log reporting.
9	Solution should consist Un-obfuscated parsers natively available with log connector to modify existing parser as when required by security operations team.
10	The solution should provide the dashboard and Reports for viewing application vulnerabilities, and it should provide the aggregated, correlated information from all applications in the enterprises like Application Attack types and Top Apps Attacked etc.
11	Solution must be agentless and should not require any agents to integrate with end devices
12	Logs must be retained for 6 months on centralized storage. No separate storage should be required. All logs must get auto archived on centralized storage directly from Log management layer and archived logs must be readable from archival/ central storage directly
13	For future expansion the proposed solution must provide ability to archive as when required logs upto 24 PB. It must support auto-archiving to attached remote storage (ie. NAS/DAS/ NLSAS).
14	The proposed solution should capability to provide centrally or remotely log collector installation to integrate event sources. This ensure to reduce time of implementation as well as any changes to be made later through single click push from central site.
15	Platform must be on VM's or physical servers supporting complete HA at DC and DR. All licenses must be included.
16	Platform must support MITR For threat intelligence

S.No.	Minimum Technical Specification
17	Solution must integrate with NIPS and other Network devices to capture packet data
18	Quoted Solution must have its presence in India for more than 7 years and must have atleast 3 deployments for more than 50000 EPS in Government of India organization. Atleast 3 sign-off must be attached for more than 50K EPS from Government of India organization.
19	Solution must De-Identify logs at source itself using Format preserving encryption which must be stateless in nature to secure logs end to end

5.2.2. Intelligent Integrated Infrastructure

- a) Intelligent integrated/inbuilt infrastructure, standalone system design, engineering, manufacture, assembly, testing at manufacturer's works, supply, delivery at site, unloading, handling, proper storage at site, erection, testing and commissioning at site of complete infrastructure for the proposed Data Centre to be installed.
- b) The detail specifications of the intelligent integrated/inbuilt infrastructure, standalone system shall be in adherence to TIA 942 guidelines thus shall be composed of multiple active power and cooling distribution paths, but only one path active. Shall have redundant components.
- c) The Intelligent Integrated Infrastructure essentially includes internal redundant or backup power supplies, environmental controls (e.g., precision air conditioning, fire suppression, smoke detection, Water leak detection, humidity sensor etc.), security devices etc. Critical systems like UPS and Precision Air-conditioning system will have N+N and N topology respectively.
- d) The Intelligent integrated infrastructure would provide many functionality and some of the key functionalities are Cold Contained Front Aisle & Rear Contained Hot Aisle, insulation, remote management and single point of service.
- e) The Intelligent integrated Infrastructure shall have following components:-
 - i. Precision Air conditioner with variable capacity cooling, heater and humidifier to cater IT load approximately 2X300 KVA in N+N redundancy for a total of 15 racks (including 5 network racks).
 - ii. 2 x 300 KVA UPS with P.F. up to 0.9 & efficiency 92% ~94%. There should be approximately 120 minutes battery back-up.
 - iii. Novec 1230 Gas based fire suppression system as per NFPA guidelines
 - iv. Smoke detectors, water leaks detection system, temperature & humidity sensor, door sensor, and alarm beacon.
 - v. 42 U racks of dimension 800 mm x 1000 mm.
 - vi. Monitoring system – capable for Email alerts
 - vii. Standalone rodent repellent system
 - viii. Biometric access control system, which should be control by access control panel.
 - ix. Exhaust Fan with Gravity Damper
 - x. 32A Vertical Rack mount PDU of type IEC C13 & IEC C19 combination, each rack shall have two such PDU's.
 - xi. Electrical system with essential MCB/MCCB.

Intelligent integrated infrastructure would have provision to add extra racks in future. It should be flexible, adaptable, controllable infrastructure.

5.2.2.1. Fire Proof Enclosure

The overall design of the safe should be suitable for safe storage of computer diskettes, tapes, smart cards and similar devices and other magnetic media, paper documents, etc. the safe should have adequate fire protection.

S.No.	Item	Minimum Specifications
1.	Capacity	2MX1MX3M
2.	Temperature to Withstand	1000° C for at least 1 hour
3.	Internal Temperature	30° C after exposure to high temperature For 1 hour
4.	Locking	2 IO-lever high security cylindrical / Electronic lock

5.2.2.2. Structured Cabling

To supply and installation, testing and commissioning of the following equipment but not limited to

- i. OFC Cabling (MTO Cabling) As per rack layout
- ii. Copper Cabling As per rack layout using Patch Panels and CAT 6 I/O
- iii. Fibre Runner As per rack layout
- iv. Wire basket for Copper As per rack layout
- v. The fibre Runner and wire basket shall connect all the rooms

S.No.	Parameter	Minimum Specifications
1.	Standards	ANSI TIA 568 C for all structured cabling components
2.	OEM Warranty	OEM Certification and Warranty of 15-20 years as per OEM standards
3.	Certification	UL Listed and Verified

5.2.2.3. Technical Specifications for Indoor Copper cable

S. No	Particulars	Specification
1	Type	Unshielded Twisted Pair, Category 6, TIA / EIA 568-C.2 & ISO/IEC 11801
2	Conductors	23 AWG solid bare copper
3	Insulation	High Density Polyethylene
4	Jacket	LSOH
5	Pair Separator	Cross-member (+) fluted Spline
6	Operating temperature	-10 °C to +65 °C
7	Storage Temperature	-20 °C to +80 °C

8	Frequency	Tested up to Minimum 250 MHz
9	Packing Box	305 Meters/Box
10	Cable Outer Diameter	6.3 +/- 0.4 mm
11	Bend Radius	4 * Cable Diameter
12	Impedance	100 Ohms + / - 15 ohms, 1 to 250 MHz
13	Fire Rating	IEC 60332-1, IEC 60754, IEC 61034
14	Mutual Capacitance	5.6 nF MAX /100 Mtr
15	Propagation Delay Skew	35 ns/100 Mtrs. MAX
16	Max. Tensile strength	110N
17	Performance characteristics	Performance characteristics to be provided along with bid Attenuation, Pair-to-pair and PS NEXT, ELFEXT and PSELFEXT, Return Loss, ACR and PS ACR
18	Standard Compliance	ANSI/TIA-568 C.2 category 6, ISO/IEC-11801, Class E/ IEC 61156-5: category 6
19	Application	IEEE 802.af and IEEE 802.3at for PoE
20	Certification	CPR (Class: B2ca-s1a, d1,a1)

5.2.2.4. Technical Specifications for Outdoor Copper cable

S. No	Particulars	Specification
1	Type	Unshielded Twisted Pair, Category 6 Double Jacket External Armoured Cable, TIA / EIA 568-C.2 & ISO/IEC 11801
2	Conductors	23 AWG solid bare copper
3	Insulation Material	Foam PE
4	Inner Jacket Material	FRPVC
5	Outer Jacket Material	PE (UV Stabilized)
6	Insulation Diameter	1.05 +/- 0.05mm
7	Cable Diameter	10.5 ± 0.5 mm
8	Operating temperature	-20 °C to +60 °C
9	Frequency	Tested up to Minimum 250 MHz
10	Armour	ECCS Tape
11	Armour Thickness	≥ 0.125mm
12	Impedance	100 Ohms + / - 15 ohms, 1 to 250 MHz.
13	Propagation Delay Skew	45 ns/100 Mtrs. MAX
14	Standard Compliance	ANSI/TIA-568 C.2 category 6, ISO/IEC-11801, Class E/ IEC 61156-5: category 6

5.2.2.5. Electrical System & cabling

To supply and installation, testing and commissioning of the following equipment but not limited to

- LT panels ,SUB Distribution Panel, UPS Input and Output Panel with Switch gear as per

- ii. specification
 - iii. Power Cable tray as per requirement
 - iv. Conduiting and wiring as per requirement
 - v. Floor PDU as per requirement based on Layout Drawing
 - vi. LED lighting and Motion detector as per site requirement
- All electrical components shall be design manufactured and tested in accordance with relevant IndianStandard IECSS

5.2.2.6. Cooling System

To supply and installation, testing and commissioning of the following equipment but notlimited to

- i. DX based Precision Air Conditioning(Perimeter Cooling)
- ii. DX based Row Based Cooling (Row Cooling)and Containment for Server room 3
- iii. Both Hot and cold Aisle Containment for Server room as per layout in Annexure-2&3 of RFP Vol-II for better PUE, Cooling, Power, DCIM from same OEM for better Integration

5.2.2.7. Precision Air Conditioning System

SN	Specifications
1	For CCC DC, the cumulative capacity of precision AC would around 20 TR. The PAC solution will be N+1 configuration, with the best rating as per the proposal submitted. One of the PAC units will be always passive The CCC-DC should be precision environment controlled. The temperature inside Server Farm area should be maintained at 22 degree centigrade with a precision of ± 2 degrees.
2	CCC-DC should be provided with precision air conditioning on a 24 x 7 operating basis at least meeting with Tier - II architecture requirements. The units should be able to switch the air conditioner on and off automatically and alternately for effective usage. The units should be down-flow fashion/ horizontal air-flow fashion, air-cooled conditioning system. Precision Air Conditioning systems specifically designed for stringent environmental Control with automatic monitoring and control of cooling, heating, humidification, dehumidification and air filtration function should be installed.
3	<p>The CCC-DC shall be provided with fully redundant Microprocessor based Precision Air-conditioning system. The precision unit shall be air cooled refrigerant system with N+1 configuration. Cool air feed to the CCC DC shall Horizontal Air Flow in the row type. The return air flow shall be through natural upwardly movement of hot air. Cooling shall be done by the Air-conditioning system only. Forced cooling using Fans on False floor, etc is not acceptable.</p> <p>The aisle to be contained, the CCC DC shall be provided with fully redundant Microprocessor based Precision Air-conditioning system. The precision unit shall be air cooled gas based refrigerant system with N+1 configuration on low level with low power consumption. Cool air feed to the CCC DC shall be horizontal air flow ensuring no air</p>

	<p>stratification across the face of the IT racks. The system shall be floor mounted placed next to server racks and configured for horizontal airflow with draw-through air pattern to provide uniform air distribution over the entire face of the server racks. Positions of Indoor units shall be done wisely to reduce the distance of return air path from hot aisle to hot-air in-take of cooling units. Cooling units shall be positioned as closer to the heat load, so that any kind of recirculation of air can be avoided i.e. next to the IT racks. The Bidder should work out design tonnage and air flow CFM values/ requirements for CCC DC.</p> <p>All the design parameters and head-load estimation calculations in detail need to be submitted for the CCC DC. The bidder needs to provision and include the low side works for the augmentation of during future expansion in the server room.</p>
4	<p><u>Temperature requirements</u></p> <p>The environment inside the CCC DC shall need to be continuously maintained at 22 ± 2 Centigrade. It is advised that the temperature and humidity be controlled at desired levels. The necessary alarms for variation in temperatures shall be monitored on a 24x7 basis and logged for providing reports.</p>
5	<p><u>Relative Humidity (RH) requirements</u></p> <p>Ambient RH levels shall need to be maintained at $50\% \pm 5$ non-condensing. Humidity sensors shall be deployed. The necessary alarms for variation in RH shall be monitored on a 24x7 basis and logged for providing reports.</p>
6	<p><u>Temperature & Relative Humidity Recorders</u></p> <p>Temperature and Relative Humidity Recorders shall preferably be deployed for recording events of multiple locations within the CCC DC. Records of events for about past 7 days shall be recorded and presentable whenever required by. Automatic recording of temperature and humidity using sensors located at various locations (or levels of the IT Racks) within the CCC DC is necessary through BMS system.</p>
7	<p><u>Air quality levels</u></p> <p>The CCC DC shall be kept at highest level of cleanliness to eliminate the impact of air quality on the hardware and other critical devices. The CCC DC shall be deployed with efficient air filters in PAC units to eliminate and arrest the possibility of airborne particulate matter which may cause air-flow clogging, gumming up of components, causing short-circuits, blocking the function of moving parts, causing components to overheat, etc. Air filters to provide up-to 5 Micron particulate shall be deployed.</p>
8	<p>The precision air-conditioners should be capable of maintaining a temperature range of 22 degree with a maximum of 2 degree variation on higher and lower side and relative humidity of 50% with a maximum variation of 5% on higher and lower side.</p>

9	The precision air-conditioners shall have 2 independent refrigeration circuits (each comprising 1 no scroll/rotatory compressors, refrigeration controls and condensers) and dual blowers for flexibility of operations and better redundancy.
10	The unit casing shall be in double skin construction for longer life of the unit and low noise level.
11	For close control of the CCC DC environment conditions (Temp. and RH) the controller shall have (PID) proportional integration and differential.
12	The precision unit shall be air cooled refrigerant based system to avoid chilled water in critical space.
13	The internal cooling design shall follow cold aisle and hot aisle concept. In case of aisle containment, there may not be requirement of raised floor. However, the bidder has to ensure data center efficiency, i.e., Power Utilization Effectiveness (PUE), of 1.7 or less, measured quarterly, for CCC DC IT load ranging between 30% to 100%.
14	The refrigerant used shall be environment friendly HFC, R-407-C/ equivalent in view of long term usage of the data center equipment, availability of spares and refrigerant.
15	For close control of the data center environment conditions (Temp. and RH) the controller shall have (PID) proportional integration and differential or equivalent.
16	For PAC if greater than 10TR it is recommended that the refrigeration circuit should be dual type, each circuit should have one no of scroll compressor. Refrigeration controls, condenser and dual blower
17	<p>In case of aisle containment, the following points need to be adhered to:</p> <ul style="list-style-type: none"> o Cooling Fans: Temperature controlled variable speed (30%-100%) driven by variable frequency drives. Units shall be 42 U, 600mm width & include casters and leveling feet to allow ease of installation in the row and provide a means to level the equipment with adjacent IT racks. Fans shall soft start to minimize in-rush current when starting. o Microprocessor controlled audio & visual alarms for Temp /sensors setting fault indications; Temperature/ Air pressure / Humidity sensors excessive use or functional unit failure. o System should be capable of remotely controlled /managed over TCP/IP. It should help changing set points as well as view and clear alarms remotely. o In cooling system, cooling coils should be certified in accordance with UL207 or equivalent. o Load dependent variable frequency driven compressor with proper protections. o Humidifier shall be able steam-generating type, disposable cylinder and automatic solid-state control circuit. The humidifier controller shall communicate directly to the microprocessor. Humidifier shall be capable of producing min 3 kg of steam per hour.

5.2.2.8. Safety and Security System

To supply and installation, testing and commissioning of the following equipment but not limited to

- i. Addressable Fire Detection and Alarm System
- ii. Rodent Repellent System
- iii. Gas Based fire Suppression System
- iv. Portable Fire Extinguishers

Addressable Fire Detection and Fire Alarm System

S. No	Minimum Required Specifications
1.	<p>MAIN FIRE ALARM CONTROL PANEL (FACP)</p> <p>A. The main FACP Central Console shall contain a microprocessor based Central Processing Unit (CPU). The CPU shall communicate with and control the following types of equipment used to make up the system: intelligent addressable smoke and thermal (heat) detectors, addressable modules, control circuits, and notification appliance circuits, local and remote operator terminals, printers, annunciators, and other system controlled devices.</p> <p>B. Information is critical to fire evacuation personnel, large 640- character Liquid Crystal Display (LCD) is required to present vital information to operators concerning a fire situation, fire progression, and evacuation details. Other options are single or Multichannel voice firefighter’s telephone; LED, LCD, or PC based Graphic annunciators; fire or integration networking; advanced detection products for challenging environments etc.</p>
2.	<p>Panel Components & functions</p> <p>The control panel(s) shall be a multi-processor based networked system designed specifically for fire, smoke control, extinguishing agent releasing system. The control panel shall be UL/FM/ EN listed The control panel shall include all required hardware, software and site specific system programming to provide a complete and operational system. The control panel(s) shall be designed such that interactions between any applications can be configured, and modified. The control panel(s) operational priority shall assure that life safety takes precedence among the activities coordinated by the control panel.</p> <p>The control panel shall include the following capacities:</p> <p>Support up to minimum 90 detectors & 90 devices</p> <p>Support up to minimum 180 addressable points.</p> <p>Support multiple digital dialers and modems</p> <p>The control panels shall include the following features:</p> <p>Provide electronic addressing of analog/addressable devices.</p> <p>Provide an operator interface control/display that shall annunciate command and control system functions.</p>

	<p>Provide an internal audible signal with different programmable patters to distinguish between alarm, supervisory, trouble and monitor conditions.</p> <p>Provide a discreet system control switch provided for reset, alarm silence, panel silence, drill switch, previous message switch, next message switch and details switch.</p> <p>Provide system reports that provide detailed description of the status of system parameters for corrective action or for preventative maintenance programs.</p> <p>Provide an authorized operator to perform test functions within the installed system.</p>
3.	<p>Power Supply</p> <p>System power supply(s) shall provide multiple powers limited 24 VDC output circuits as required by the panel. Upon failure of normal (AC) power, the affected portion(s) of the system shall automatically switch over to secondary power without losing any system functions. Each system power supply shall be individually supervised. Power supply trouble signals shall identify the specific supply and the nature of the trouble condition.</p> <p>All standby batteries shall be continuously monitored by the power supply. Low battery and disconnection of battery power supply conditions shall immediately annunciated as battery trouble and identify the specific power supply affected. All system power supplies shall be capable of recharging their associated batteries, from a fully discharged condition to a capacity sufficient to allow the system to perform consistent with the requirements of this section, in 48 hours maximum.</p> <p>All AC power connections shall be to the building's designated emergency electrical power circuit and shall meet the requirements of NFPA 72 - The AC power circuit shall be installed in raceway. The power circuit disconnect means shall be clearly labelled FIRE ALARM CIRCUIT CONTROL and shall have a red marking. The location of the circuit disconnect shall be labelled permanently inside the each control panel the disconnect serves.</p> <p>Power supply for all input & output devices to be driven from main Fire Alarm Panel.</p>
4.	<p>Field Mounted System Components</p>
5.	<p>Multi-sensor Photo Thermal Detector:</p> <p>The Multisensor or multitech smoke detector which will have both photoelectric as well as thermal detection elements shall have inbuilt microprocessor, and shall be capable of taking an independent alarm decision. The scattering of smoke particles shall activate the photo sensor. Each addressable smoke detector's sensitivity shall be capable of being programmed electronically from Control Panel without any extra tools. The detector should continue to give TRUE alarms even if the loop controller on the main panel fails. Alarm condition shall be based upon the combined input from the photoelectric and thermal detection elements. Each detector shall be</p>

	capable of transmitting prealarm and alarm signals in addition to the normal, trouble and need cleaning information.
6.	Addressable Detector Bases: The bases shall be easy to install and mount and shall be of standard type.
7.	Manual Stations The fire alarm station shall be of polycarbonate construction and incorporate an internal toggle switch. A locked test feature shall be provided. The station shall be finished in red with silver "PULL IN CASE OF FIRE" lettering.
8.	Intelligent Modules The personality of multifunction modules shall be programmable at site to suit conditions and may be changed at any time using a personality code downloaded from the Analog Loop Controller. The modules shall have a minimum of 1 diagnostic LEDs mounted behind a finished cover plate. The module shall be capable of storing up to 24 diagnostic codes, which can be retrieved for troubleshooting assistance. Input and output circuit wiring shall be supervised for open and ground faults.
9.	Control Relay Module: The Control Relay Module shall provide one form "C" dry relay contact to control external appliances or equipment shutdown. The control relay shall be rated for pilot duty and releasing systems. The position of the relay contact shall be confirmed by the system firmware.
10.	Isolator Module/ Bases: Provide intelligent fault isolators modules. The Isolator Module shall be capable of isolating and removing a fault from a class A data circuit while allowing the remaining data loop to continue operating.
11.	Monitor Module: The Monitor Module shall be factory set to support one (1) supervised Class B Normally-Open Active Non-Latching Monitor circuit.
12.	Sequence of Operations General - Audio Upon alarm activation of any area smoke detector, heat detector, manual pull station, sprinkler water flow, the following functions shall automatically occur: The internal audible device shall sound at the control panel or command center. The following audio messages and actions shall occur simultaneously:

	<p>An evacuation message shall be sounded on fire floors (zones) immediately above and below (adjacent to) the fire floor (zone), on the floor in fire condition. It is the intent of this message to advise occupants hearing this message that they are near danger and should leave the building via the stairs (nearest exit) immediately.</p> <p>Activate visual strobes on the fire floors (zones) immediately above and below (adjacent to) the fire floor (zone). The visual strobe shall continue to flash until the system has been reset. The visual strobe shall not stop operating when the "Alarm Silence" is pressed. An alert message shall be sounded on the remainder of building. It is the intent of this message to advise occupants to prepare for evacuation if necessary. An instructional message shall be sounded in the stairwells instructing occupants to move carefully and quickly down the stairs to exit the building and to exit to a safe floor if you encounter smoke in the stairwell.</p> <p>Activate automatic smoke control sequences.</p> <p>All automatic events programmed to the alarm point shall be executed and the associated outputs activated.</p> <p>All stairwell/exit doors shall unlock throughout the building.</p> <p>All self-closing fire/smoke doors held open shall be released.</p>
13.	Installation: All conduiting / wiring /Trays /channels /trenches /pipes etc. for completion of Job
14.	Warranty: 5 Years Comprehensive onsite OEM Warranty

Rodent Repellent System

It would consist of :-

- Controllers –Be capable of generating variable high frequency electronic signalsthat are ultrasonic in nature (20 KHz to 50 KHz) and these signals shall be transmitted to the transducers for emission all around.
- Transducers – To cover an open area of 300 Sq.ft. minimum with an averageceiling height of 10ft.

1	Operating Frequency	Above 20Khz
2	Power Consumption	15W max
3	Sound Output:	80db to 110db (at 1m)
4	Power output	800mW per transducers

Gas Based fire Suppression System

1. Gas Based Fire Suppression System (GBFSS)
 - The SI shall supply, install, test and put in operation NOVEC1230 based fire suppression system.
 - The fire suppression system shall include and not be limited to gas release control panel, CCE approved seamless cylinders, discharge valve (with solenoidor pneumatic

actuator) as the case may be, discharge pipe, non-return valve and all other accessories required to provide a complete operation system meeting applicable requirements of NFPA 2001 or ISO standards and installed in compliance with all applicable requirements of the local codes and standards.

- The system design should be based on the specifications contained herein, NFPA 2001 & in accordance with the requirements specified in the design manual of the agent.
 - The SI shall confirm compliance to the above along with their bid.
 - The system shall be properly filled and supplied by an approved OEM (Original Equipment Manufacturer)
2. Generally the key components* of the system shall be VdS or LPCB or FM/UL listed. The NOVEC 1230 gas shall:
- comply with NFPA 2001 or ISO 14520 standard
 - have the approval from US EPA (Environmental Protection Agency) for use as a total flooding fire extinguishing for the protection of occupied space:
 - Be given Underwriters' Laboratories Inc. (ULI, USA) component listing for the NOVEC 1230 gaseous agent.
 - must have zero ozone depletion potential (ODP);
 - have a short life span in the atmosphere, with atmospheric life time of less than 5 days
 - be efficient, effective and does not require excessive space and high pressure for storage
 - commercially available
 - *Key components are valves and its accessories, actuators, flexible discharge and connection hoses, check valves, pressure switch, and nozzles

3. Design Condition

- The hazard space volumes shall be protected from a common central or individual supply, the cylinder bank or individual cylinder system, with corresponding pipes and nozzle system.
- The individual zone/ system shall be dimensioned to give a complete discharge of the agent in less than 10 seconds into the affected zone.
- The software calculation shall be approved VdS or FM / UL. The discharge time shall not exceed 10 seconds. After end of discharge (10s) a homogeneous NOVEC 1230 concentration shall be built-up in the room.
- The design concentration shall follow ISO 14520 or at minimum NFPA 2001 for under floor, room and ceiling space. Unless otherwise approved, room temperature for air-conditioned space shall be taken around 20°C. For non-air conditioned space, the temperature shall be taken around ambient temperature. The system shall be designed with minimum design concentration of 4.7 % as applicable to Class-A & C fire.
- All voids within each hazard shall be discharged simultaneously. Each hazard shall have an independent system, unless otherwise specifically stated.
- The system engineering company should carry out the piping Isometric design and validate the same with a hydraulic flow calculation generated by using the agent's design software.

Appropriate fill density to be arrived at based on the same.

- The system shall be so designed that a fire condition in any one protected area
- shall actuate automatically the total flooding of clean agent in that area independently.
- The entire system shall incorporate inter-alia detection, audible and visual alarms, actuation and extinguishing.

4. Clean Agent Supply System

- The extinguishing agent shall be NOVEC 1230 with physical properties conforming to NFPA Standard 2001 or ISO 14520 standard.
- Each zone to be protected by the Total Flooding System shall be capable of being flooded independently of the other.

5. Re-Filling and Maintenance

- In case of any leakage or accidental discharge of the agent, it should be possible to re-fill the cylinders in India itself.
- The SI should indicate the source of re-filling and the time that will be taken for re-filling and replacement.188

6. Storage of Extinguishing Agent

- The agent shall be stored in liquid form at ambient temperature in high- pressure seamless cylinder containers designed for the purpose. The cylinder shall be high pressure, seamless, flat type and concave bottom.
- As per the regulations of the Chief Controller of Explosive (CCE) Nagpur, any system which has a working pressure above 19 bar will require the use of seamless cylinders that have been duly approved by the CCE, Nagpur.
- Each cylinder shall have its own built-in pressure safety relief valves and shall also be equipped with pressure gauge to indicate the pressure of its content.
- The cylinders shall be super-pressurized with dry Nitrogen to 42 Bar. The cylinder shall be capable of withstanding any temperature between -30 Deg C and 70 Deg C.
- All cylinders shall be distinctly and permanently marked with the quantity of agent contained, the empty cylinder weight, the pressurization pressure and the zones they are protecting.
- All cylinders shall be adequately mounted and supported in a manner to facilitate individual servicing or content weighing.
- Cylinders installed shall be of the same size where possible and the manifold shall be provided with non-return or check valves to prevent back flow when any cylinder is being removed for maintenance.

7. Piping and Fittings

- All piping shall be Schedule 40 seamless pipes complying with grade B and all fitting shall be of ASTM A-105.
- Discharge Nozzles
- Discharge nozzles shall be manufactured in corrosion resistant material and shall be positioned in a manner to effect a uniform concentration at the shortest time after discharge. Each nozzle shall be able to cover a height of 5m effectively.

8. Detection

- The detection part shall consist of the installation of an adequate number of smoke detectors strategically positioned for the early detection of smoke, and/or products of combustion. All detectors shall be ULI, FMRC and/or LPC or Vds approved.
- The detection of smoke by such detectors shall immediately set off an audible alarm at the control unit and visual indication of the zone where smoke has been detected.
- The detectors in each zone protected by Total Flooding System shall be wired on a DUAL RISK CIRCUIT basis. The actuation of one detector in a zone shall not be sufficient to cause the discharge of the agent. The agent shall only be actuated to discharge on activation of another adjacent detector in that zone.
- The signal from the second activated detector within the particular zone protected by the Total Flooding System shall after a time delay activate the agent release device of the Total Flooding System. The time-delay circuit shall have a delay period adjustable from zero second to 180 seconds.

9. Documentation:

- The system engineering company should prepare & submit along with the bid documents, the piping Isometric drawing and support the same with a hydraulic flow calculation generated by using the agent's design software. The calculations shall validate the fill density assumed by the SI.
- The SI shall submit copies of the datasheets of the hardware used in the system.
- The SI shall also submit copy of CCE approval letter for the cylinder proposed to be used.
- The SI shall also submit calculations to evidence the quantity of agent considered for the system.
- The successful vendor must submit, along with the supply invoice, a certificate of authenticity, for the agent from the system engineering company duly checked and verified by distributor.
- The system engineering company should provide, as part of the handing over, the As built drawings and operation & maintenance manual.

5.2.2.9. Monitoring System

To supply and installation, testing and commissioning of the following equipment but not limited to

- i. Building Management System
 - a. BMS comprises of a management system for the following:

Monitoring and control of utility system

 - Monitoring of Electrical System
 - External lighting Control
 - Under vehicle detection and scanning system
 - Fire door monitoring system and Fire pump monitoring
 - Elevator level monitoring system
 - Water sump – Motor control and monitoring
 - UPS Monitoring System
 - Integration of BAS system
 - Attendance and Access control for O&M staffs through Bio-metric system.

Safety and security system

- IP based Addressable Fire alarm panel- Alarm and Detection
- Public Address and Emergency voice communication System
- Smart card based Access Control system and Flap barrier
- RFID – Tag based vehicle barriers.(four wheelers)
- IP based Closed Circuit Surveillance including External Solvency system
- Visitor management system with photo ID and card issue at security gate
- Car calling system
- LHS cables for cable trays
- ii. Temperature and Humidity Sensor
- iii. Flow meter for Diesel unloading
- iv. Float Sensor for Diesel Monitoring at day tank level
- v. Integration with All energy meter, MCCB, ACB, Safety and Security Equipment's, Diesel monitoring, Data centre Temperature and Humidity Monitoring, UPS, PAC, Panel ON/Off/Trip status etc.

5.2.2.10. 42U Racks and PDU

Sr No	Specification	Minimum Requirement
1	General	42 U X 600mm X 1200mm (H x W x D) rack should have metal frame supporting more than 1300 kgs of static load and more than 1000 kg of dynamic load.
2		Single front door and split rear door should have the perforation of more than 75% to provide the maximum airflow eliminating the need of additional FHU in the rack.
3		Doors shall have lift of hinges for tool less field reversibility.
4		Rack should have integrated hole pattern for easy installation of top panel accessories have removable opening for cable entry and shall accommodate 2000 cat 6 cables to suffice the cabling requirements.
5		Rack should have two pair of 19-inch EIA mounting rail with U marking on front and rear of each rail for ease of installation.
6	Cable Manager	Rack should have dual purpose full height depth adjustable PDU/Cable management brackets and should be mounted in the zero U space.
7		PDU/Cable management brackets shall have button mount keyholes throughout to accommodate the tool less mounting of rack PDU's of various heights and accessories mounting holes for toolless cable mounting accessories.
8	Panel	Rack should have split side panels with single locking slam latch for quick and easy installation and maintenance, single person

		removal and installation eliminates the manpower dependencies.
9	Caster & Levelling	42 U rack frame height that allows access through standard doors on four swivel casters, rack shall have the levelling feet and shall be accessible from the top of the frame for easy adjustment.
10	Hardware Accessories / Installation ease	Rack shall have the necessary hardware accessories ((50 each M6 cage nuts and screws), Cage nut installation tool, edge protection for top panel cable entry, T30 / Phillips L key, T30 extension driver.
11		Rack shall have necessary baying brackets and the bolt down kits
12		Rack frame design should allow 2.5 inch more usable space in the rack for the proper equipment placement and ease of access.
13	Powder Coating	Rack should have the powder coated black color, RAL 7021.
14	Certification	Rack shall have EIA, UL, RoHS, REACH certified
15	Power Distribution	Rack shall have two power distribution unit, vertically mounted on the rear of the rack to power on the devices in the rack.
16	Power Distribution Unit	Monitored, Unit Level, 32Amps, 230V, 1 Phase , 7.3KW, Vertical, 30 IEC C13, 6 IEC C19, Locking Sockets , 3m power Cord with 2P+E (IP44)
17		The PDU shall have locking outlets - cable locking mechanism so that it should not require the locking cable to secure the cables connected to the PDU
18		PDU shall have Input and Breaker level current monitoring. Local high visibility LED display.
19		PDU shall have Phase (A) Monitoring (kWh, W, VA, PF, V, A) Power Measurements Compliant with ANSI C12.1 and IEC 62053-21 at 1% Accuracy Class Requirements and Circuit / Breaker Monitoring (A)
20		Circuit/Breaker Current Measurements Independently Tested and Verified at 2% Accuracy
21		The PDU shall support the mobile app for the power monitoring and should be easy to be shared in various formats

22		The PDU shall be upgrade ready so that it can be changed to monitored PDU without downtime, by simply changing the Field replaceable IMD unit.
23		PDU shall have button mounting option for easy toolless installation and reinstallation of the PDU's
24		PDU shall have colored outlets to differentiate the outlets based on the breakers.
25		The PDU should be CE certified.
26	Rack	Both rack and PDU should come with 5 years of default warranty

5.2.2.11. 9U Rack

S.No.	Minimum Specifications
1	Racks manufactured out of steel sheet punched, formed, welded and Powder coated
2	Standard for Racks configuration will be welded frame and vented top cover or better
3	Rack should have Front Toughened Glass Door with lock & Key
4	Rack should be 9U in Height, 550MM Width, 1000MM Depth
5	Provision for easy wall mounting should be there with appropriate anchor fasteners
6	Rack must be provided with 2 fan directly mounted on the roof top as an exhaust from the cabinet. Fan should be of AC 230V
7	Rack should be provided with cable management accessories. 1U Cable manager, PDU with 6 Nos. Sockets of 5 Amp
8	Manufacturer should have ISO 9001-2015 Certifications, and UL/EN and RoHS certified. Certificate needed to be submitted.

5.2.2.12. KVM Switch

S.No.	Item	Minimum Specifications
1	KVM Requirement	Keyboard, Video Display Unit and Mouse Unit (KVM) for the IT Infrastructure Management at Data Center
2	Form Factor	19" rack mountable
3	Ports	minimum 8 ports
4	Server Connections	It should support both USB and PS/2 connections.
5	Auto-Scan	It should be capable to auto scan servers
6	Rack Access	It should support local user port for rack access
7	SNMP	The KVM switch should be SNMP enabled. It should be operable from remote locations
8	OS Support	It should support multiple operating system
9	Power Supply	It should have dual power with failover and built-in surge

		protection
10	Multi-User support	It should support multi-user access and collaboration

5.2.2.13. Anti-Climb & Cantilever Poles for Mounting Camera etc.

S.N.	Parameter	Minimum Specifications
1.	Pole type	Hot Dip Galvanized after Fabrication with Silver coating of 86 micron as per IS:2629; Fabrication in accordance with IS-2713 (1980)
2.	Height	5-10 Meters, as-per-requirements for different types of cameras & Site conditions
3.	Pole Diameter	Min. 10 cm diameter pole (SI to choose larger diameter for higher height)
4.	Cantilevers	Based on the location requirement suitable size cantilevers to be considered with the pole
5.	Bottom base plate	Minimum base plate of size 300mmx300mmx15mm (or) 30cmx30cmx1.5cm
6.	Mounting facilities	To mount CCTV cameras, Switch, etc.
7.	Pipes, Tubes	All wiring must be hidden, through tubes/pipes. No wires shall be visible from outside.
8.	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 RFP.
9.	Protection	Lightning arrester at select sites as per the requirements
10.	Sign-Board	A sign board describing words such as “This area under surveillance” (in English and Hindi)

5.2.2.14. DG Set (Diesel Genset)

S.No.	Parameter	Minimum Specifications
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 foremissions. KVA rating as per the requirement.
2.	Capacity	650 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 continuous operation, Complete with level indicator, fuel inlet and outlet, air vent,
4.	Power Factor	0.8

5.	Engine	Engine should support electric auto start, water cooled, multi cylinder, maximum 1500 rpm with electronic/manual governor and electrical starting arrangement complete with battery, 4 stroke multiple cylinders/single and diesel operated conforming to BS 5514/ ISO 3046/ IS 10002
6.	Alternator	Self-exciting, self-regulating type alternator rated at 0.8 PF or better, 415 Volts, 3 Phase, 4 wires, 50 cycles/sec, 1500 RPM, conforming to IS4722/ BS 5000, Windings of 100% Copper, class H insulation, Protection as per IP 23.
7.	AMF (AutoMain Failure) Panel	AMF Panel fitted inside the enclosure, with the following meters/indicators: Incoming and outgoing voltage Current in all phases Frequency KVA and power factor Time indication for hours/ minutes of operation Fuel Level in field tank, low fuel indication Emergency Stop button Auto/Manual/Test selector switch MCCB/Circuit breaker for short-circuit and overload protection Control Fuses Earth Terminal Any other switch, instrument, relay etc. essential for Automatic functioning of DG set with AMF panel
8.	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.
9.	Output Frequency	50 HZ
10.	Tolerance	+/- 5% as defined in BSS-649-1958
11.	Indicators	Over speed /under speed/High water temperature/low lube oil etc.
12.	Intake system	Naturally Aspirated
13.	Certifications	ISO 9001/9002, relevant BS and IS standard

5.2.2.15. NOVEC 1230 Gas based Fire Suppression System

Specifications to be considered as mentioned in section 5.2.2. “Safety and Security System”

5.2.2.16. The Rodent Repellent System

Specifications to be considered as mentioned in section 5.2.2. “Safety and Security System”

5.2.2.17. Water Leak Detection System

It consists of:-

a) Water Leak Detection Panel

The water Leak detection panel consists of multiple zones. These controllers shall have MODBUS/BAC net output to be integrated with BMS system. The features areas under:-

- i. Alphanumeric LCD Display with the minimum of 3 Lines
- ii. Soft Touch Membrane Keypad
- iii. LED Indication of the events like power, Alarm & Fault
- iv. Password protected event log facility
- v. Remote monitoring via MODBUS/BAC net protocol
- vi. Configurable sensitivity adjustment
- vii. Dedicated Hooter output for local alarm

b) Water Leak Sensing Cable

- i. Water leak sensing cable shall be mechanically strong, resistant to corrosion and abrasion.
- ii. It shall be constructed with two sensing wires, an alarm signalling wire and a continuity wire constructed by fluoropolymer carrier.
- iii. It shall have end circuit to detect open circuit fault.

c) Hooter

5.2.2.18. High Sensitivity Smoke Detection System

a) High Sensitivity Smoke Detection aspiration General Description:

a. A high performance aspirating smoke detection system shall be supplied, installed and commissioned by the specialist contractor in accordance with the requirements detailed in the NFPA – 72, Aspirating Detection Systems.

b. The system has been designed to sense incipient smoke at a very early stage in all critical rooms, namely:

- i. Data Centre.
- ii. UPS & Battery Room
- iii. Technical Area
- iv. The panels shall be mounted inside the risk protected and there shall be a network of air sampling pipe work.
- v. The High Sensitivity Smoke detection consist of highly sensitive Laser-based Smoke Detectors with aspirators connected to networks of sampling pipes. The alarms are generated once the laser sensor receives smoke at a pre-determined obscuration level to activate and alert, Fire 1, Fire 2 and alert signal.

- vi. The signal is extended to the Fire Alarm monitor Modules / BMS through Volt free contacts for further investigation.
- vii. When required, it shall be possible to connect an interface card for open Protocol output to BMS system for online Monitoring with Software level integration.
- viii. When required, an optional remote Display unit shall be provided to monitor each detector, and a Programmer shall be supplied to configure the system.

b) Scope of Work

- i. This specification covers the requirements of design, supply of materials, installation, testing and commissioning of Aspirating Smoke Detection System. The system shall include all equipment's, appliances and labour necessary to install the system, complete with high sensitive LASER-based Smoke Detectors with aspirators connected to network of sampling pipes.
- ii. The SI shall also make provision in the Aspirating Smoke Detectors to trip AHU and to shut fire dampers in the event of fire through the relay contacts.

c) Codes and standards

The entire installation shall be installed to comply one or more of the following codes and standards:

- i. NFPA Standards,
- ii. British Standards, BS 5839 part :1

d) Approvals

All the equipment's shall be tested, approved, and/or listed by :

- i. LPCB (Loss Prevention Certification Board), UK
- ii. FM Approved for hazardous locations Class 1, Div 2
- iii. UL (Underwriters Laboratories Inc.), US
- iv. ULC (Underwriters Laboratories Canada), Canada
- v. Vds (Verband der Sachversicherer e.V), Germany

e) Design Requirements

- i. The System shall consist of a high sensitive LASER-based smoke detector, aspirator, and filter.
- ii. It shall have a display featuring LEDs and Reset/Isolate button. The system shall be configured by a programmer that is either integral to the system, portable or PC based.
- iii. The system shall allow programming of:
 - Multiple Smoke Threshold Alarm Levels
 - Time Delays.
 - Faults including airflow, detector, power, filter block and network as well as an indication of the urgency of the fault.
 - Configurable relay outputs for remote indication of alarm and fault Conditions.
 - It shall consist of an air sampling pipe network to transport air to the detection system, supported by calculations from a computer-based design modelling tool.

- Optional equipment may include intelligent remote displays and/or a highlevel interface with the building fire alarm system, or a dedicated System Management graphics package.

f) Performance Requirements

- Shall provide very early smoke detection and provide multiple output levels corresponding to Alert, Action, and Fire 1 & 2. These levels shall be programmable and shall be able to set sensitivities ranging from 0.025 – 20% obscuration / meter.
- Shall report any fault on the unit by using configurable fault output relays or via the graphics Software.
- Shall monitor for filter contamination.
- Shall incorporate a flow sensor in each pipe and provide staged airflow faults.

g) Materials and Equipment's

- i. The Laser detection Chamber shall be of the mass Light Scattering type and capable of detecting a wide range of smoke particle types of varying size.
- ii. A particle counting method shall be employed for the purposes of preventing large particles from affecting the true smoke reading.
- iii. Monitoring contamination of the filter (dust & dirt etc.) to notify automatically when maintenance is required.
- iv. The Laser Detection Chamber shall incorporate a separate secondary clean air feed from the filter; providing clean air barriers across critical detector optics to eliminate internal detector contamination.
- v. The detector shall not use adaptive algorithms to adjust the sensitivity from the set during commissioning. A learning tool shall be provided to ensure the best selection of appropriate alarm thresholds during the commissioning process.

h) Detector Assembly

- vi. The Detector, Filter, Aspirator and Relay Outputs shall be housed in a mounting box and shall be arranged in such a way that air is drawn continuously from the fire risk area by the Aspirator and a sample passed through the Dual Stage Filter and then to the detector.
- ii. The detector shall be LASER-based and shall have an obscuration sensitivity range of 0.025 – 20% obs/m.
- iii. The detector shall have four programmable smoke alarm thresholds across its sensitivity range with adjustable time delays for each threshold between 0 - 60 seconds.
- iv. The detector shall also incorporate the facility to transmit a fault through a relay.
- v. The detector shall have a single pipe inlet that must contain an ultrasonic flow sensor. High flow fault (urgent and non-urgent) and low flow fault (urgent and non-urgent) can be reported.
- vi. The filter must be a two-stage disposable filter cartridge. The first stage shall be capable of filtering particles in excess of 20 microns from the air sample. The second stage shall be ultra-fine, removing more than 99% of contaminant particles of 0.3 microns or larger, to provide a clean air barrier around the

detector's optics to prevent contamination and increase service life.

- vii. The aspirator shall be a purpose-designed rotary vane air pump. It shall be capable of allowing/ supporting for a single pipe run / multiple sampling pipe runs with a transport time of less than 90 seconds.
- viii. Detectors shall be capable of supporting a single pipe run of 25m with a maximum transport time of 120 seconds or as appropriate standards dictate.
- ix. The Assembly must contain relays for fire 1, Action and fault conditions. The relays shall be software programmable (latching or non-latching). The relays must be rated at 2 A at 30V DC. Remote relays shall be offered as an option and either configured to replicate those on the detector or programmed differently.
- x. The Assembly shall have built-in event and smoke logging. It shall store smoke levels, alarm conditions, operator actions and faults. The date and time of each event shall be recorded. Each detector (Zone) shall be capable of storing up to 18000 events.

i) Displays on the Detector Assembly

- i. The detector will be provided with LED indicators.
- ii. Each Detector shall provide the following features at a minimum.
- iii. Alert, Alarm, Fire 1 and Fire 2 corresponding to the alarm thresholds of the detector.
- iv. Smoke Dial display represents the level of smoke present.
- v. Fault Indicator.
- vi. Disabled indicator.
- vii. Buttons supporting the following features shall be accessible to authorized personnel.
- viii. Reset – Unlatches all latched alarm and faults.
- ix. Disable – Disables the fire relay outputs from actuating and indicates a fault.

i) Sampling Pipe

- i. The sampling pipe shall be smooth bore with an outside diameter of 25mm and internal diameter of 21mm should be used.
- ii. The pipe material should be suitable for the environment in which it is installed or should be the material as required by the specifying body.
- iii. All joints in the sampling pipe must be air tight and made by using solvent cement except at entry to the detector
- iv. The pipe shall be identified as Aspirating Smoke Detector Pipe along its entire length at regular intervals not exceeding the manufacturer's recommendation or that of local codes and standards.
- v. All pipes should be supported at not less than 1.5m centres, or that of the local codes or standards.
- vi. The far end of each trunk or branch pipe shall be fitted an end cap and drilled with a hole appropriately sized to achieve the performance as specified and as calculated by the system design.

j) Sampling Holes

- i. Sampling Holes of 2mm, or otherwise appropriately sized holes, shall not be separated by more than the maximum distance allowable for conventional detectors as specified in the local codes & standards. Intervals may vary according to calculations.
- ii. Each sampling point shall be identified in accordance with Codes or Standards.
- iii. Consideration shall be given to the manufacturer's recommendations and standards in relation to the number of Sampling Points and the distance of the Sampling Points from the ceiling and roof structure and forced ventilation systems.

k) Installation

- i. The Contractor shall install the system in accordance with the manufacturers recommendation.
- ii. Where false ceilings are available, the sampling pipe shall be installed above the ceiling and Capillary Sampling Points shall be installed on the ceiling and connected by means of a capillary tube.
- iii. The minimum internal diameter of the Capillary tube shall be 5mm, the maximum length of the capillary tube shall be 2m unless the manufacturer in consultation with the engineer have specified otherwise.
- iv. The Capillary tube shall terminate at a ceiling Sampling Point specifically approved by the Client. The performance characteristics of the sampling points shall be taken into account during the system design.
- v. Air Sampling Piping network shall be laid as per the approved pipe layout. Pipe work calculations shall be submitted with the proposed pipe layout design for approval.

l) Testing

- i. Commissioning Test
 - Commissioning of the entire installation shall be done in the presence of the owner and/or its representative.
 - All necessary instrumentation, equipment, materials and labour shall be provided by the Contractor.
 - The Contractor shall record all tests and system calibrations and a copy of these results shall be retained on site in the system Log Book.
- ii. Functional Test
 - Introduce Smoke into the Detector Assembly to provide a basic functional test
 - Introduce smoke to the least favourable Sampling Point in each Sampling Pipe. Transport time is not to exceed 120 Seconds.

m) Documentation

- i. The SI shall be authorized and trained by the manufacturer to design, install, test and maintain the Aspiration Smoke Detection system and shall be able to produce a certificate issued by the manufacturer along with the offer.
- ii. The SI shall submit computer generated software calculations for design of

aspirating pipe network, on award of the contract.

- iii. Product data and performance criteria shall be submitted by the SI.
- iv. The SI should provide, as part of handing over, the as-built drawing, operation manual and maintenance manual. The as-built drawing shall exactly match the Sampling pipe layout with the pipe software calculation.

5.2.2.19. Raised Floor

Figure: Fire Protection Layout

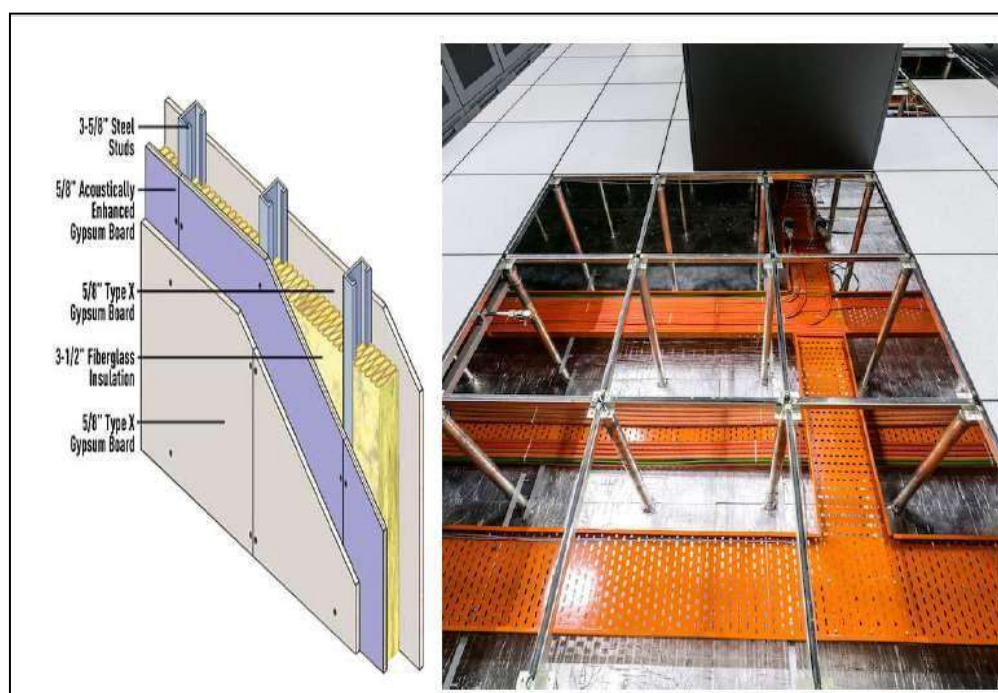
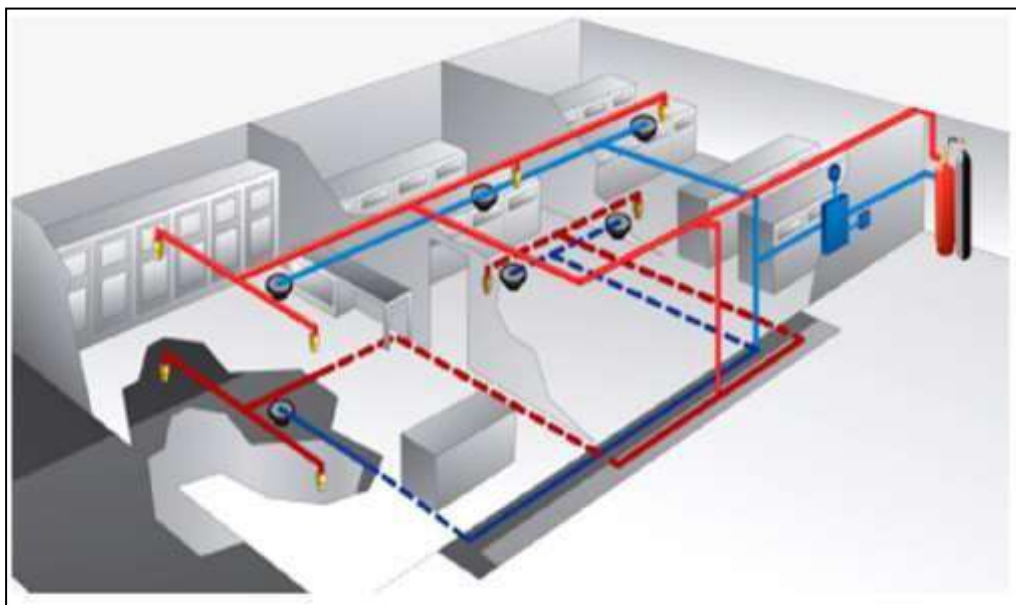


Figure: DC raised flooring

Providing and fixing Access floor systems as per EN 12825 or equivalent standards.

a) System:

- i. Access floor system to be installed at finished floor height of maximum 600 mm from the existing floor level.
- ii. The system will provide for suitable pedestal and under-structure designed to withstand various static loads and rolling loads subjected to it in an office / server / DCS / panel / rack area.
- iii. The entire Access floor system will provide for adequate fire resistance, acoustic barrier and air leakage resistance.

b) Panels:

- i. Panels will be made up of inert material Calcium sulphate. The bottom of the panel shall be of Aluminium foil to create a fire and humidity barrier and this should provide floor's electrical continuity. Panels will remain flat through and stable unaffected by humidity or fluctuation in temperature throughout its normal working life. The Panels will be UL listed/FM/DM approved.
- ii. Panels will provide for impact resistance top surfaces minimal deflection, corrosion resistance properties and shall not be combustible or aid surface spread of flame.
- iii. Panels will be insulated against heat and noise transfer.
- iv. Panels will be 600 x 600mm x 30 mm height fully interchangeable with each other within the range of a specified layout.
- v. Panels shall rest on the grid formed by the stringers which are bolted on to the pedestals.
- vi. Panels shall be finished with anti-static 0.9 mm Laminate and 0.45 mm thick plastic edge material that is self-extinguishing and will be PVC free

c) Panel Loading

- i. Concentrated point load: 450Kg per European standard EN 12825*.
- ii. Uniformly Distributed Load (UDL): 1500 Kg/M².

d) Fire Rating:

- i. The Panels will confirm to class O and Class 1 Fire Ratings tested as per CIRC 91/61 or BS 476 Part 6 & 7 (60 min).

e) Pedestals:

- i. Pedestal installed to support the panel will be suitable to achieve a finished floor height of 600mm. Pedestal design will confirm speedy assembly and removal for relocation and maintenance. Pedestal base to be permanently secured to position on the sub-floor.
- ii. Pedestal assembly will provide for easy adjustment of levelling and accurately align panels to ensure lateral restraint. Pedestals will support an axial load of 1500 Kgs, without permanent deflection and an ultimate load of 3000 Kgs. Pedestal head will be designed to avoid any rattle or squeaks.

f) Pedestal Assembly

- i. The structure is made entirely of galvanized steel consisting of hexagonal shaped, 89 mm diameter, and 1.5 mm thick base plate, with 6 shaped stiffening ribs with niches that improve adhesion and with 5 holes mechanical fastening to the ground.
- ii. The assembly will provide a range of height adjustment up to 25mm, with the help of check nuts.

g) Under structure:

- i. Under structure system consists of stringers of size 525 x 30 x 25 x 0.8 mm thick to form a grid of 600 x 600mm. These stringers are locked into the pedestal head and run both ways.
- ii. The US system will provide adequate solid, rigid and quiet support for access floor panels.
- iii. The US system will provide a minimum clear, uninterrupted height of 600 mm between the bottom of the floor and bottom of the access floor for electrical conducting and wiring.

h) Stringers:

- i. Stringer system is composed of a special frame, made of pressed galvanized steel plate and with a section 25mm wide, 30 mm high and 0.8 mm thick. The longitudinal ribs and flaps in the lower part should be designed to increase flexion resistance.
- ii. The grid formed by the pedestal and stringer assembly will receive the floor panel.

i) Floor Insulation:

- i. The floor and ceiling slabs should be heat-insulated, or coated with a heat insulating material to avoid condensation on floors below and above and to reduce the heat transfer in the server/network room area.
- ii. The insulation shall be done with 13 mm thick self-adhesive aluminium foil face nitrile rubber. The floor and ceiling shall be coated with epoxy paint.
- iii. The floor insulation should cover for true floor and true ceiling, this will not allow the thermal conductivity.
- iv. The server & other required area should be equipped with raised floor with 600mm (24 inch) height. Cavity floor shall have false flooring panels of 18 gauges steel 600 x 600 coated with APDCL Page: TSA – 2 50 micron epoxy conductive paint.
- v. Floor shall be finished with 2mm thick antistatic high pressure laminate with 2mm thick PVC trim edge all-round.
- vi. The interior of the panels shall be filled with non-combustible Cementous compound.
- vii. The raised floor distributed load should not be less than 1500 Kg/Sqm.

5.2.2.20. False Ceiling

False Ceiling at appropriate height should be installed concealing any cabling tray and electrical lighting wiring in all areas.

a) Server room

- i. False ceiling shall be provided with Armstrong Lay in (Hot dipped galvanized steel) metal ceiling system 600 x 600 x 5mm with standard perforation of 2.5 mm die (16% open space) and fleece with NRC of 70 & CAC36 to be laid on Armstrong grid system.
- ii. Armstrong Orcal Lay in metal ceiling System consisting of 600x600mm lay in tiles of pre-coated galvanised steel in 0.5 mm thickness in white colour with standard perforation of 2.5mm die & open area of 16%.
- iii. The back of the tile should have black acoustical fleece with NRC of 0.70 & CAC 36 to be laid on Armstrong grid systems with 15mm wide T - section flanges Colour white having rotary stitching on the Main Runner, 1200 mm & 600 mm Cross Tees, fixed to the structural soffit by Butterfly clip hangers, suspension wires & anchor fasteners as per the manufacturer's specification.
- iv. Suspension wires to be provided at every 600mm c/c with two no's of ties on each anchor fastener, Perimeter trim of Trulok wall angle in white colour secured to wall at 450mm maximum centres.

b) Other Areas

- i. Acoustical false ceiling of mineral fibre Board (600 x 600 x 15mm) of Armstrong (ELIT RH99) of Equipment. Laid on Grid system (Micro lock edge) with 15mm thick Tsection(White) having main runner 1200mm x 600mm, cross Tee at 295 HT.
- ii. Mineral Fibre Board modular False Ceiling in Armstrong in Board edge Fissured ANF tiles of size 600mX600mmX15mm having Noise reduction Co-efficient 0.5, light reflection over 75%, Relative Humidity 99%, fire performance class0/class1 (BS 476) 24XL - Hot Dipped Galvanized Steel Suspension System having rotary stitching on mainrunner, 1200 mm & 600 mm cross tees with 15mm wide flanges of white colour with standard perforation of 2.5mm dia. (16% open space) fleece with NRC of 0.70 & CAC 36, fixed to the structural soffit by Butterfly clip hangers, suspension wires & anchor fasteners as per the manufacturer's specification, Suspension wires to be provided at every 600mm c/c with two no's of ties on each anchor fastener, Perimeter trim of Trulok wall angle in white colour secured to wall at 450mm maximum centres.
- iii. The False Ceiling tile should be Dust free type and of Non-combustible material. Each False Ceiling tile (preferably 600mm x 600mm) should be individually removable for access to area above False Ceiling.
- iv. The false ceiling area should cover with as per layout. The contractor should propose the right quantity.

5.2.2.1. Building Management System

S. No	Minimum Specifications
1	IBMS solution should be a pre-integrated centralized management platform with a capability of managing IT as well as Non-IT equipments.
2	IBMS should be the manager of managers including SLA management and helpdesk for all equipments including IT and Non-IT.

3	Inventory management should be a part of the platform.
4	GUI should have as-is representation of the DC with real time depiction of data.
5	Correlation with impact analysis should be a part of the ibms platform.
6	IBMS should have single sign-on along with multi and concurrent session capabilities over web.
7	IBMS platform should be able to integrate the SOP's as desired.

5.2.3. ICT Software Components for Data Center

Commencement of the date of all licenses of supplied software will start from the proposed date of Acceptance Test for the Go – Live of the component in which that software is used.

5.2.3.1. Functional Enterprise Management System

Sr No	Description
FUNCTIONAL SPECIFICATIONS	
1.	For effective operations and management of IT Operations, there is a need for an industry-standard Enterprise Management System (EMS). Given the expanse and scope of the project, EMS becomes very critical for IT Operations and SLA Measurement. Some of the critical aspects that need to be considered for operations of IT setup of are: a) Network Fault Management b) Network Performance Management c) Server Performance Monitoring d) Centralized Log Management e) Centralized and Unified Dashboard f) Centralized and Customizable Service Level Reporting g) Help Desk for Incident Management
2.	The Monitoring Solution should provide Unified Architectural design offering seamless common functions including but not limited to: <ul style="list-style-type: none"> • Event and Alarm management, • Auto-discovery of the IT environment, • availability and Performance monitoring • Correlation and root cause analysis • Service Level Management, notifications • Reporting and analytics • Automation and Customization
3.	There should be a tight integration between infrastructure metrics and log to have the single consolidated console of Infrastructure & security events.

4.	Consolidate IT event management activities into a single operations bridge that allows operator quickly identify the cause of the IT incident, reduce duplication of effort and decreases the time it takes to rectify IT issues.
5.	The Operator should be able to pull up security events related to a given Configuration Item, from a single console which also has NOC events, and use the security events to triage the problem. This way the Operator gets consolidated system/network event details and security events (current and historical) from the same console and save time in troubleshooting , isolating the issue.
6.	The operator should be able to build correlation rules in a simple GUI based environment where the Operator should be able to correlate cross domain events
7.	The solution shall provide future scalability of the whole system without major architectural changes.
8.	The Solution shall be distributed, scalable, and multi-platform and open to third party integration such as Cloud, Virtualization, Database, Web Server Application Server platforms etc.
9.	All the required modules should be from same OEM and should be tightly integrated for single pane of glass view of enterprise monitoring
10.	The solution must provide single integrated dashboard to provide line of business views and drill down capabilities to navigate technical operator right from services to last infrastructure components
11.	Consolidated dashboard of the proposed EMS solution must be able to do dynamic service modelling of all business-critical production services & use near-real time Service Model for efficient cross domain event correlation.
12.	The proposed solution must provide SDK/Rest API for North bound and South Bound Integrations E.g. Forwarding specific metric data to third party database, Notifications to third party systems such as Jira, AutoDesk, Slack
13.	Proposed NMS solution must have deployment reference of monitoring & managing 2500+ network nodes in at least 3 deployments across Gov/PSU/Large Enterprise.
14.	The Solution should provide all the modules as a single monitoring engine to correlate events in real-time from Networks, Servers and Applications
15.	The solution should be virtual appliance and deployable on Linux operating systems to reduce the overall TCO

16.	The solution should run without any propriety database license for datastore - Datastore must be bundled within EMS (E.g. popular time-series no-sql, hbase based monitoring systems) to reduce the TCO
17.	The solution should provide High Availability (HA) at datacenter site
18.	The solution should have inbuilt role-based access module to enable multiple users with different groups to create dashboards specific to their department
19.	The Solution should have way to control and define permission such as read/write for set of devices rather than all the devices for the ease of use.
20.	Calculates availability for clients, servers and ANPR/access/video units for efficient SLA management
21.	Detailed system care statistics will be available through a web-based dashboard providing health metrics of ANPR Platform including Uptime and mean-time-between-failures.
TECHNICAL SPECIFICATIONS	
	Consolidated Dashboard
1.	The platform must provide complete cross-domain visibility of IT infrastructure issues
2.	The platform must consolidate monitoring events from across layers such as Network, Server, Application, Database etc.
3.	The solution should support single console for automated discovery of enterprise network components e.g. network device, servers, virtualization cloud, application and databases
4.	The solution must support custom dashboards for different role users such as Management, admin and report users
5.	The solution must allow creating custom data widget to visualize data with user preferences e.g. Refresh time, time span, background colour, unit conversion
6.	The solution must support multiple visualization methods such as gauge, grid, charts, Top N etc.
7.	The solution should provide superior view of infrastructure health across system, networks, application and other IT Infrastructure components into a consolidated, central console

8.	There should be only one dashboard/interface to collect network/server/application/log data after correlation and consolidation across the IT landscape to reduce/correlate number of metrics/alarms
Element & Network Performance Management (EMS/ NMS/ NTA)	
1.	The proposed solution platform shall provide a single integrated solution for comprehensive management of the wired/wireless access, and rich visibility into connectivity and performance assurance issues.
2.	The EMS must conduct Performance Monitoring, Performance Management Control, Performance Analysis of every network element into the system.
3.	There will be a policy driven protocol (management) to check the health of edge devices.
4.	The EMS should conduct the monitoring and management of the coordinated configuration of multiple devices
5.	The EMS must ensure FCAPS compliance: coordinated Fault Management Configuration Management, Accounting Management, Performance Management and Security Management across the associated elements in the network.
6.	The design functionality shall facilitate creation of templates used for monitoring key network resources, devices, and attributes. Default templates and best practice designs are provided for quick out-of-the-box implementation automating the work required to use OEM validated designs and best practices.
7.	The proposed solution must provide comprehensive and integrated management of IT infrastructure components to maximize the availability of IT services and SLA performance.
8.	The proposed solution must provide the complete view of the Topology and network elements. The NMS shall have the ability to include the network elements and the links in the visual/graphical map of the department. The visual maps shall display the elements in different colour depending upon the status of the element. It is preferable that green color for healthy and amber/yellow color for degraded condition and red for unhealthy condition is used.
9.	The proposed solution must have suitable system level backup mechanism for taking backup of NMS data manually as well as automatically
10.	The proposed solution must keep historical data at raw level without averaging for minimum of six month

11.	The proposed solution must provide the visual presentation of the Network Element's status and the alarms. It shall also present the complete map of the network domain with suitable icons and in suitable color like green for healthy, red for non-operational, yellow for degraded mode of operation etc.
12.	The proposed solution must provide Health Monitoring reports of the network with settable periodicity -@24 Hrs, 1 week, 1 month.
13.	The proposed solution must provide the graphical layout of the network element with modules drawn using different colors to indicate their status
14.	The proposed solution must provide calendar view which allows the operator all the schedule activities such as Reports, Inventory scans etc. It shall also allow to define scheduled report for uptime, link status etc.
15.	The proposed solution should have multiple alerting features to get the notification via email, SMS and third-party systems
16.	The proposed solution must support listening to traps and syslog events from the network devices with retention period upto 6 months.
17.	The proposed solution must support defining the data retention period to control storage
18.	The solution must support custom device template to support Generic SNMP devices
19.	The solution must provide discovery & inventory of heterogeneous physical network devices like Layer-2 & Layer-3 switches, Routers and other IP devices and do mapping of LAN & WAN connectivity with granular visibility up to individual ports level.
20.	It shall provide Real time network monitoring and Measurement of end-to-end Network performance & availability to define service levels and further improve upon them.
Fault Management	
1.	The proposed solution must should provide out of the box root cause analysis with multiple root cause algorithms inbuilt for root cause analysis. It should also have a strong event correlation engine which can correlate the events on the basis of event pairing, event sequencing etc.

2.	The Platform must include an event correlation automatically fed with events originating from managed elements, monitoring tools or data sources external to the platform. This correlation must perform: <ul style="list-style-type: none"> • Event filtering • Event suppression • Event aggregation • Event annotation
3.	The proposed solution should provide out of the box root cause analysis with multiple root cause algorithms inbuilt for root cause analysis. It should also have a strong event correlation engine which can correlate the event on the basis of event pairing, event sequencing etc.
4.	Powerful correlation capabilities to reduce number of actionable events. Topology based and event stream-based correlation should be made available.
5.	The solution must offer relevant remedy tools, graphs in context of a selected fault alarm/event
6.	The proposed monitoring solution should have capability to configure actions-based rules for set of pre-defined alarms/alerts enabling automation of set tasks.
7.	The Platform must support Event or Alarm Correlation integrations with service desk to trigger automated creation of incidents, problem management
8.	The solution should classify events based on business impact and also allow defining custom severity levels and priority metrics such as Ok, Critical, Major, Down, Info etc. with color codes
9.	The solution should allow creation of correlation or analytics rules for administrators
10.	The proposed solution must provide default event dashboard to identify, accept and assign generated alarms
Log Management	
1.	The proposed solution must provide a common classification of events irrespective of the log format
2.	The proposed solution must provide the ability to store/ retain both normalized and the original raw format of the event log as for forensic purposes for the period of 3 months and allow to extend it to further with additional hardware without any disruption to the ongoing data collection

3.	The proposed solution should provide a minimum log compression of 8:1 for ensuring log compression to reduce overall log index storage space for the raw log format
4.	The log data generated should be stored in a centralized server. The period up to which the data must be available should be customizable.
5.	The proposed solution must support logs collected from commercial and proprietary applications. For assets not natively supported, the solution should provide the collection of events through customization of connector or similar integration
6.	The proposed solution must support log collection for Directories (i.e. AD LDAP), hosted applications such as database, web server, file integrity log etc. using agents
7.	The Log receiver or log collection component must store the data locally if communication with centralized collector/receiver is unavailable.
8.	The proposed solution must support log collection from Network infrastructure (i.e. switches, routers, etc.). Please describe the level of support for this type of product.
9.	The system shall support the following log formats for log collection: Windows Event Log, Syslog, Access Log Data, Application Log data, Any Custom Log data, Text Log (flat file), JSON Data
10.	The solution should be able to collect raw logs in real-time to a Central log database from any IP device including: <ul style="list-style-type: none"> • Networking devices(router/switches/voice gateways) • Security devices (IDS/IPS, AV, Patch Mgmt., Firewall/DB Security solutions) • Operating systems(Windows 2003/2008, Unix, linux, AIX) • Virtualization Platforms(Microsoft HyperV, VMware Vcenter/VSphere 4.X, vDirector, Citrix) • Databases(Oracle/SQL/MYSQL/DB2)
11.	The collection devices should support collection of logs through Syslog, syslogNG and also provide native Windows Agents as well as Agentless (PowerShell) connectors
12.	The proposed solution must provide alerting based upon established policy
13.	The proposed solution must provide SDK and Rest API to write custom connectors and collectors to pull log and monitoring data from third party system

14.	The proposed solution must provide UI based wizard and capabilities to minimize false positives and deliver accurate results.
15.	The proposed solution must collect, index the log messages and support full text searching for forensic investigation
16.	The proposed solution must support the ability to take action upon receiving an alert. For example, the solution should support the ability to initiate a script or send an email message.
17.	The solution must provide pre-defined log correlation rules to detect suspicious behavior
18.	The solution must support real-time and scheduled alerting time-line while creating a log policy to catch specific log pattern
19.	The solution should support applying regex pattern in real-time to extract vendor specific log data for reporting and alerting purpose
20.	The system shall have the capability to drag and drop building of custom search queries & reports
21.	The system shall be capable of operating at a sustained 5000 EPS per collection instance. The system shall provide the ability to scale to higher event rates by adding multiple collection instance
Service Desk - Incident Management	
1.	The proposed helpdesk system shall provide flexibility of logging, viewing, updating and closing incident manually via web interface
2.	The proposed helpdesk solution should have achieved Pink VERIFIED certification on at least 6 available ITIL processes. Documentary proof must be provided at the time of submission.
3.	Each incident shall be able to associate multiple activity logs entries via manual update or automatic update from other enterprise management tools.
4.	The proposed helpdesk system shall be able to provide flexibility of incident assignment based on the workload, category, location etc.
5.	The proposed solution should automatically provide suggested knowledge base articles based on Incident properties with no programming
6.	The proposed solution should automatically suggest available technicians based on workload, average ticket closure time assigning tickets with no programming

7.	The proposed solution should tightly integrate with monitoring system to provide two-way integration - E.g. when system down alarm created, it should automatically create ticket and assign it to technician, in case system comes up before ticket is resolved by technician, it should automatically close the ticket to minimize human efforts
8.	The proposed system must not create more than one ticket for same recurring alarm to avoid ticket flooding from Monitoring system
9.	Each escalation policy shall allow easy definition on multiple escalation levels and notification to different personnel via web-based console with no programming
10.	The proposed helpdesk system shall be capable of assigning call requests to technical staff manually as well as automatically based on predefined rules and shall support notification and escalation over email
11.	The proposed solution should allow administrator to define ticket dispatcher workflow which automatically assign incoming tickets based on rules defined in workflow. E.g. Network fault keyword tickets gets assigned to network technician automatically within NOC team
12.	The proposed helpdesk system shall provide grouping access on different security knowledge articles for different group of users.
13.	The proposed helpdesk system shall have an updateable knowledge base for technical analysis and further help end-users to search solutions for previously solved issues
14.	The proposed solution should allow Technician to relate Incidents to Problem, Change and vice versa to have better context while working on any of ticket type
15.	The proposed helpdesk system shall support tracking of SLA (service level agreements) for call requests within the help desk through service types.
16.	The proposed helpdesk system shall integrate tightly with the Knowledge tools and CMDB and shall be accessible from the same login window
Asset Inventory Management	
1.	A configuration management database shall be established which store unique information about each type Configuration Item CI or group of CIs.
2.	The proposed solution allows scheduling periodic report to check current software and hardware inventory
3.	The proposed solution must allow attaching CI record to generated service tickets

4.	The Proposed solution should provide end to end Asset Life Cycle Management: Makes it easier to handle the complete life cycle of an asset that is, all stages/modules from procurement to disposal
5.	The Proposed solution should support maintaining AMC/Warranty Information with Alerting when about to expire also provide Asset Deletion capabilities enabled with workflow engine
6.	The Proposed solution should support Software License Metering: Helps to understand the software license compliance and the use of unauthorized software in the organization and helps to act proactively to curb illegal usage and problems associated with it.
7.	The proposed solution should provide Asset Dashboards/Reporting Graphical representation all the assets based on Category, location, aging of the asset, customer, which can be further level down to the incident record ID
8.	The proposed solution should provide out of the box purchase and contract management modules to support end to end asset life cycle
Service Level Reporting	
1.	The solution should provide reports that can prove IT service quality levels such as application response times and server resource consumption
2.	The system reports should be accessible via web browser and Reports can be published in PDF and csv format
3.	The solution must have an integrated dashboard, view of Contract Parties & current SLA delivery levels and view of Services & current SLA performance
4.	The solution must provide Reports that can be scheduled to publish automatically or they can be produced on demand
5.	The solution should be able to report in the context of the business service that the infrastructure elements support—clearly showing how the infrastructure impacts business service levels
6.	The solution should provide Business Service Management functionality to track Service quality by logically grouping Network, Server and Application components. The solution should provide correlation between Network Server and Application to identify the business impact from the specific event or alarm
7.	The solution must provide way to define key performance indicators (KPIs) within the Service Quality report.

8.	The solution must provide SLA measurement to track service quality from both Availability and Performance perspective.
----	--

5.2.3.2. Functional & Technical Specifications for Server Load Balancer

Sr No.	Minimum Technical Specification
1	<p>The Load Balancer device should be a dedicated Hardware Appliance with the following features:</p> <p>1) Should support multiple virtual network functions/instances for future scalability.</p> <p>2) The appliance shall deliver the high availability required by modern data centers. It should support Active/Passive or Active / Active HA configurations using standard VRRP protocol or equivalent.</p> <p>3) The Load Balancer shall automatically synchronize configurations between the pair and automatically failover if any fault is detected with the primary unit.</p> <p>4) The device should support upto 16 virtual instances/segmentation. Should have internal redundant Power supply with 240GB usable hard disk, 16 GB RAM .</p>
2	The Load Balancer shall support offloading of SSL connections and should deliver 10 Gbps of SSL throughput on 1024 key or better.
3	Proposed device should have minimum 4 x 10G SFP+ ports prepopulated and upto 8 x 10 SFP+ ports
4	Proposed device should support upto 8 virtual instances/segmentation.
5	The server load balancer should deliver minimum 1 Million concurrent sessions
6	The server load balancer should cater up to 20,000 SSL transactions per second on 1K key RSA and upto 16K TPS (ECDSA-SHA256)
7	Local Application Switching, Server load Balancing, HTTP,TCP Multiplexing, HTTP Pooling, HTTP Pipelining, Compression, Caching, TCP Optimization, Filter-based Load Balancing, Transparent Deployments, captive portal, Content-based Load Balancing, Persistency, HTTP Content Modifications, Band Width Management(BWM), Support for connection pooling to TCP request, Support for distributed denial-of-service (DDoS) protection
8	Should have secure access solutions for mobile PDAs, Android, Windows and iOS based smart phones and tablets with machine authentication
9	The solution should able to load balancer both TCP and UDP based applications with layer 2 to layer 7 load balancing including WebSocket and WebSocket Secure.

10	The solution should support server load balancing algorithms i.e. round robin, weighted round robin, least connection, Persistent IP, Hash IP, Hash Cookie, consistent hash IP, shortest response, proximity, SNMP, SIP session ID, hash header etc. or equivalent.
11	The solution should support Multi-level virtual service policy routing , -Static, default and backup policies for intelligent traffic distribution to backend servers
12	The solution should provide compressive support for IPv6 functions to help with ipv4-to-ipv6 transition without business disruption and must provide support for dual stack/NAT 64/ DNS 46/NAT 46/ IPv6 NAT , DNS64/46
13	The solution should support advance ACL's/Policy to protect against network based flooding attacks. Administrator should able to define ACL's/policy rules based on connections per second (CPS) and concurrent connections (CC), cookie value.
14	The solution should provide comprehensive and reliable support for high availability through standard VRRP or equivalent on Per VIP based Active-active & active standby unit redundancy mode.
15	OEM should have presence in India since last 5 years and have 24 x 7 TAC in India

5.2.3.3. Functional & Technical Requirements for Link Load Balancer

Sr.No.	Minimum Technical Specifications
1	Physical Specification
1.1	The proposed load balancer must be a purpose built dedicated hardware load balancer with harden OS and it should be a virtual load balancer
1.2	The proposed load balancer should be allow to install any generic or third party operating/application
1.1	System must of be 19-inch rack mountable 1 U form factor
1.2	System must have dedicated management port
1.3	System must have RJ-45 console port
1.4	System must have 5 x 1 G cu Interface and 4 x 10 G fiber ports
1.5	System must have dual power supply
2	Performance
2.1	System must support 20 Gbps of L7 throughput
2.2	System must support 32 million concurrent connection
2.3	System must support 450 K Layer4 connection per second
2.4	System must support 120 K 1:1 Layer7 connection per second for HTTP
3	Application delivery partition/Virtual Context
3.1	System must support 30 Application delivery partition/Virtual Context
3.2	System must support dedicated configuration file for each Virtual context
3.3	System must support resource allocation to each context including throughput, CPS, Concurrent connection,SSL throughput
3.4	System must be able to modify the resource allocation on the fly without restarting/rebooting any context
3.5	All the virtual context must be available from day-1

Sr.No.	Minimum Technical Specifications
4	DDOS
4.1	System must support protection from Fragmented packets
4.2	System must support protection from IP Option
4.3	System must support protection from Land Attack
4.4	System must support protection from Packet Deformity Layer 3
4.5	System must support protection from Packet Deformity Layer 4
4.6	System must support protection from Ping of Death
4.7	System must support protection from TCP No Flag
4.8	System must support protection from TCP Syn Fin
4.9	System must support protection from TCP Syn Frag
4.1	System must support connection limit based on source IP
4.11	System must support connection rate limit based on source IP
4.12	System must support request rate limit based on source IP
5	Load-balancing features
5.1	System must support Layer4-Layer7 load-balancing
5.2	System must support load-balancing algorithms including round-robin, least connection, service least connection, fastest reponse, hash etc
5.3	System must support active-active and active-backup link configuration for load-balancing
5.4	System must support configuration of multi-level backup link
5.5	System must support Source-NAT for SLB traffic
5.6	System must support Global Server load-balancing
5.7	System must support Next Hop Load Distribution (NHLD) for load balancing multiple links
5.8	System must support Link selection based on Source IP
5.9	System must support Link selection based on Destination IP
5.1	System must support graceful activation and disabling of links
5.11	System must support DNS caching
5.12	System must support NAT 64 - DNS 64
5.13	System must support Firewall load-balancing
5.14	System must support IDS/IPS load-balancing
5.15	System must support bandwidth restriction per source IP
6	Redundency
6.1	System must support VRRP based redundancy
6.2	System must support active-active and active-backup configuration
6.3	System must support automatic and manual configuration sync
6.4	System must support dynamic VRRP priority by traffic interface, server, nexthop and routes
6.5	System must support dedicated VRRP setting per virtual context
7	Management
7.1	System must have Web-based Graphical User Interface (GUI)
7.2	System must have Industry-standard Command Line Interface (CLI)
7.3	System must support Granular Role-based\Object-based Access Control
7.4	System must support SNMP, Syslog, email alerts, NetFlow v9 and v10 (IPFIX), sFlow
7.5	System must support REST-style XML API (aXAPI) for all functions
7.6	System must support external authentication including LDAP, TACACS+, RADIUS

Sr.No.	Minimum Technical Specifications
7.7	System must support flexibility in selecting number of CPUs for control processing

5.2.3.4. Functional & Technical Requirements for Centralized AV & Anti-Spam

The following features are required for centralized anti-virus solution, to protect all computing resources (servers, desktops, other edge level devices, etc.):

S.No.	Minimum Technical Specifications
1.	AV Solution: Should have critical components for total security on the endpoint. (Antivirus, Antimalware, Vulnerability protection, iDLP, HIPS, Firewall, Device control & Virtual Patching.)
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 are allowed to 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
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
d.	Endpoint Host based IPS should support virtual patching both known and unknown vulnerabilities until the next scheduled maintenance window. Endpoint security solution should submit unknown files to on-premise sandbox appliance for simulation. It should also support creation of IOC's on real time basis. These IOC's

S.No.	Minimum Technical Specifications
	should be distributed to rest of the servers for block, remediate and clean up threats and sandboxing should have at least 55 virtual instances, which should have OS (win7, win8, win 10, Win 2003, win 2008, win 2012) instances in sandboxing- along with customized sandboxing feature.
e.	Should support prevention against script-based attacks used to deliver malware such as ransomware. Endpoint solution should able to consume IOC's and output from sandboxing from Zero day threat solution to protect and clean zero day threat at endpoint level.
f.	Should Support Signature & Heuristic Phishing Protection
g.	Should Support Site Status Check
h.	Should Support Centralized Browser Security Policy Management
i.	Should Support Centralized Browser Security Event Logging & Reporting
17.	Management Platform Support
a.	Operating systems: Should Support Windows Server 2008, 2012, 2016
b.	Browsers: Should Support Internet latest version of leading web browsers
c.	Client Platform Support
d.	Should support Windows 8, 10 (32 & 64 bit), Mac
18.	Spam Filtering
a.	The proposed solution should Stop spam, denial-of-service attacks, and other inbound email threats using industry-leading technologies and response capabilities, leverage adaptive reputation management techniques that combine global and local sender reputation analysis to reduce email infrastructure costs by dropping up to 90% of spam at the connection level, Filter email to remove unwanted content, demonstrate regulatory compliance, and protect against intellectual property and data loss over email, Secure and protect other protocols, such as public IM communications, using the same management console as email, Obtain visibility into messaging trends and events with minimal administrative burden.
b.	The proposed solution should automatically back up all configuration and quarantine databases on the appliance at specified intervals. Administrators should be given an option to store data on the local machine or a remote server.
c.	should be able to detect spam mails in SMTP, POP3 as well as IMAP protocols
d.	The proposed solution should have inspection facility on the header and body of the mail to check for spam URI content and identify whether the mail is a spam mail or not.
e.	The proposed solution should support real time statistics of scan performance, message processed and security violations and proposed solution should support message tracking for quarantined, archived and postpone messages in message tracking logs
f.	should have options to configure white list as well black list based on IP address and validate against the same to detect whether a mail is spam mail or not
g.	Should have configurable parameter to enable HELO DNS lookup to check whether a mail is a spam or not.
h.	Should have configurable parameter to enable return email DNS lookup to check whether a mail is a spam or not.
i.	Should have provision to define banned key words and check against that key words to identify spam mails.
j.	Should have options to define mime headers and check against the same to identify spam mail.

S.No.	Minimum Technical Specifications
k.	The solution should have Global sender reputation and local sender reputation analysis to reduce email infrastructure costs by restricting unwanted connections.
l.	Solution must be scalable to incorporate the following with no installation of component on clients should need be in future:
m.	Email Security solution should able submit files to customize sandboxing for zero day protection
n.	Should have integrated data loss prevention technologies to check loss of data through mails at gateway
o.	The proposed solution should have an option to restore an solution to its original image configuration.
p.	Should have configurable spam actions for detected spam mails (e.g. tag the mail, delete the spam mail etc.).

5.2.3.5. Functional & Technical Specifications for Network Management System

Specifications to be considered as mentioned in 8.18.1” Enterprise Management System”

5.2.3.6. Functional & Technical Specifications for Centralised Helpdesk

Sr. No.	Parameters
1.	The proposed helpdesk system shall provide flexibility of logging, viewing, updating and closing incident manually via web interface
2.	The proposed helpdesk solution should have achieved PinkVERIFY certification on at least 6 available ITIL processes. Documentary proof must be provided at the time of submission.
3.	Each incident shall be able to associate multiple activity logs entries via manual update or automatic update from other enterprise management tools.
4.	The proposed helpdesk system shall be able to provide flexibility of incident assignment based on the workload, category, location etc.
5.	The proposed solution should automatically provide suggested knowledge base articles based on Incident properties with no programming
6.	The proposed solution should automatically suggest available technicians based on workload, average ticket closure time assigning tickets with no programming
7.	The proposed solution should tightly integrate with monitoring system to provide two-way integration - E.g. when system down alarm created, it should automatically create ticket and assign it to technician, in case system comes up before ticket is resolved by technician, it should automatically close the ticket to minimize human efforts

8.	The proposed system must not create more than one ticket for same recurring alarm to avoid ticket flooding from Monitoring system
9.	Each escalation policy shall allow easy definition on multiple escalation levels and notification to different personnel via web-based console with no programming
10.	The proposed helpdesk system shall be capable of assigning call requests to technical staff manually as well as automatically based on predefined rules, and shall support notification and escalation over email
11.	The proposed solution should allow administrator to define ticket dispatcher workflow which automatically assign incoming tickets based on rules defined in workflow. E.g. Network fault keyword tickets gets assigned to network technician automatically within NOC team
12.	The proposed helpdesk system shall provide grouping access on different security knowledge articles for different group of users.
13.	The proposed helpdesk system shall have an updateable knowledge base for technical analysis and further help end-users to search solutions for previously solved issues
14.	The proposed solution should allow Technician to relate Incidents to Problem, Change and vice versa to have better context while working on any of ticket type
15.	The proposed helpdesk system shall support tracking of SLA (service level agreements) for call requests within the help desk through service types.
16.	The proposed helpdesk system shall integrate tightly with the Knowledge tools and CMDB and shall be accessible from the same login window

5.2.3.7. IDAM Functional & Technical Requirements for Mailing & Messaging Solution

S.No.	Minimum Technical Specification
1.	General
a.	Network/Server edition should run on Linux /Windows.
b.	Desktop client should run on Mac, Linux and Windows.
c.	Solution should be based on open standards for minimum 1000 users.
d.	Should support advanced search and file indexing for large inboxes
e.	Ability to use custom logos in the web interface
f.	Should support e-mail, Address Book, Calendar, Task & File Server
g.	Should support real-time backup and restore
h.	Should support clustering/High-Availability
i.	Ability to access the Mail server via IMAP clients, with the option to connect over SSL/TLS
j.	Ability to access the Mail server via POP clients, with the option to connect via

	SSL/TLS
k.	Comprehensive suite of standards-based web services APIs enabling seamless integration with other applications
l.	Ability to utilize Active Directory for user authentication and/or Global Address List
m.	Admin can configure an initial password in the migration wizard and import wizard for newly provisioned accounts
n.	Should support multi-tenancy
o.	Should support e-mail Archiving & Discovery
p.	Should have rich, interactive, web-based interface for end user functions (access via HTTP or HTTPS)
q.	Ability to customize the colors and appearance of the web interface
r.	Option to check and correct spelling in a mail message, calendar appointment, or web Document
s.	Ability to share Address Books, Calendars, and Notebooks (Documents) with internal users and groups (read or write access)
t.	Ability to share Address Books, Calendars, and Notebooks (Documents) with external users via a custom password (read access)
u.	Ability to quickly categorize messages, contacts, and/or documents by attaching "Tags" with user-defined names and colors
v.	Option to quickly view attachments in HTML format
w.	Should support conversations span folders
x.	Ability to create personal folders and folder hierarchies
y.	Ability to print a message and see a print preview
z.	Ability to sort messages based on subject, date, or sender
aa.	Ability to flag/unflag messages/conversations for follow up
bb.	Ability to define filter rules and priorities for incoming messages
cc.	Ability to enable/disable a custom away message
dd.	Ability to add a custom signature to a message
ee.	Option to popup a separate window when composing a message
ff.	Ability to save in-progress messages to a Drafts folder
gg.	Ability for a user to set an automatic forwarding address and choose whether to leave a copy in the primary mailbox
hh.	Option to Reply or Reply-All while retaining the attachments from the original message
ii.	Right-clicking a message displays a menu of actions to take on that message (e.g. Mark Read, Reply, Delete)
jj.	Right-clicking an email address displays a menu of actions to take on that address (e.g. view website, add/edit contact, create filter, search for messages)
kk.	Ability to export a set of messages as a ZIP file
ll.	Ability to toggle between Reply and Reply-All while composing a reply

mm.	Users can set their default preference for viewing messages in the reading pane
nn.	Users can set the default font family, font size and font color to use when composing email messages and Documents pages
oo.	Users can share their mailbox folders and set the permission levels to manage or to view-only.
pp.	Users can insert inline images in email messages and calendar appointments
qq.	Admin can configure the maximum number of characters used in a signature
rr.	Admin can define expiration policy for individual mailbox folders
ss.	Users will receive an email message warning of quota usage based on a threshold defined by administrator
tt.	Users can attach a URL to an email message
uu.	Users can double-click on a message in message view to expand the view pane to full view
vv.	Users can define multiple email signatures to use
ww.	Users can check multiple emails in the list view to mark as read/unread/tag, delete, or to move to a different folder
xx.	When sending a message, the priority is normal, but it can be set to high or low as well
yy.	Users can get immediate notification of new mail/
zz.	Multiple messages can be selected and forwarded in one email
aaa.	Users can right click on a folder to see the number of messages and the total size of items in folder
2.	Address Book
a.	Business card view of Contacts
b.	List view of Contacts with preview pane
c.	Ability to import/export Contacts in .csv format
d.	Ability to import/export contacts in vCard (.vcf) format
e.	Ability to print a single Contact or list of Contacts and see a print preview
f.	Right-clicking a Contact displays a menu of actions to take on the Contact (e.g. compose message, search for messages)
g.	Ability to drag a Contact to a mini-calendar date to create an appointment with that Contact
h.	Ability to create multiple Address Books in a single mailbox
i.	Ability to move/copy contacts from one Address Book to another (based on access privileges)
j.	Ability to create group contact lists in their user Address Books
k.	Address book displays individual contact information in tabbed view
l.	Photos and images can be uploaded to contacts in Address Books
3.	Calendar
a.	Ability to schedule personal appointments
b.	Ability to schedule meetings and view attendees' free/busy information
c.	Ability to create recurring meetings and exceptions to recurring meetings

d.	Ability to book resources (locations, equipment, etc.) for a meeting
e.	Ability to configure a resource to auto-respond to scheduling requests based on availability
f.	Option to enable an alert popup for upcoming appointments
g.	Appointments/schedules are automatically displayed in the users current time zone
h.	Ability to set an explicit time zone for an appointment
i.	Ability to view calendars in Day, Week, Work Week, or Month views
j.	User setting for the first day of the week; value chosen impacts the Week calendar view
k.	Ability to create an appointment and/or drag an appointment's boundaries inline in calendar views
l.	Ability to quickly mark Accept/Tentative/Decline from calendar views
m.	Declined appointments display faded so that the user remains aware of their occurrence
n.	Ability to print calendars in day, week, work week, or month views and see a print preview
o.	Hovering over an appointment in calendar view displays additional appointment details
p.	Option to display a miniature calendar at all times
q.	Hovering over a date in the mini-cal displays calendar information for that date
r.	Right-clicking on the mini-cal displays a menu of actions to take on the associated date (e.g. add appointment, search for messages)
s.	Ability for a user to create multiple calendars within a single account
t.	Ability for a user to designate which calendars will be included in the user's free/busy calculations
u.	Ability to subscribe to an external calendar in i-Calendar (.ics) format
v.	Ability to publish/export a calendar in i-Calendar (.ics) format
w.	Ability for a user to view multiple calendars overlaid in the same view, which each calendar optionally represented by a different color
x.	When viewing multiple calendars, option to view that indicates the degree of conflict at each potential time slot
y.	Users can import calendar i-Calendars (.ics)
z.	Appointments can be marked as private or public.
aa.	Administrators can configure the Calendar feature to be able to create only personal appointments
bb.	Users can search for appointments within their calendars
cc.	Public calendars display in HTML read-only format
4.	Tasks
a.	Add tasks and set the start and due date, set the priority and keep track of the progress and

	percentage complete
b.	Share task lists with internal and external users and set permission levels to manage or to view- only
c.	Users can organize task lists into folders
d.	Users can sort tasks by Status or Due Date
e.	Users can set the priority of tasks to high, normal or low
f.	Individual tasks can be tagged
g.	Files can be attached to a tasks
5.	Documents
a.	Ability to create rich web Documents with WYSIWYG or HTML editing
b.	Ability to create a notebooks as a Document repository and as a mechanism for navigating through Documents
c.	Ability to create multiple notebooks in a single mailbox
d.	Ability to create a notebook that is shared by everyone within a domain
e.	Ability to insert links in Documents to other Documents or to external URLs
f.	Ability to upload Attachments as Documents
g.	Ability to embed rich content objects as independently editable items inside a web Document
h.	Ability to embed an image as an ALE object inside a web Document
i.	Ability to embed a spreadsheet as an ALE object inside a web Document
j.	Ability to print a Document and see a print preview
k.	Pages show when last modified and version
l.	Users can upload files to their mailbox and can access them from any computer
m.	Users can add email attachments to a selected folder
6.	Search
a.	Server-side indexing of mailbox content, enabling fast and efficient search from the web interface
b.	Ability for a search to include any number of conditions combined via Boolean-like expressions (AND, OR, NOT, etc.)
c.	Ability to use text commands to execute searches
d.	Advanced interface for building searches
e.	Ability to search for a specific item type (Mail, Contacts, Documents, etc.) or across item types
f.	Ability to search using a prefix plus a wildcard
g.	When using Search Builder, the search result set updates continuously as search conditions are changed
h.	Ability to save searches for subsequent one-click re-execution
i.	Ability to search for items that contain specific keywords
j.	Ability to search for items with a specific date or within a specific date range
k.	Ability to search for items that contain an attachment
l.	Ability to search for items that contain an attachment of a certain type(s)

m.	Ability to search for items that have a specific flagged/un-flagged status
n.	Ability to search for items that are in a specific folder
o.	Ability to search for items based on storage size
p.	Ability to search for items based on read/unread status
q.	Ability to search for items with specific recipients in the To /Cc fields
r.	Ability to search for items from a specific sender
s.	Ability to search for items based on subject
t.	Ability to search for items that include a specific Tag(s)
u.	Ability to search for items that were sent to or received from a specific domain
v.	Ability to search for Contacts in a Shared Address Book
w.	Ability to search for content inside attachments
x.	Can search for appointments in calendars up (up to 180 days)
y.	Administrator can disable the indexing of junk mail
7.	Domain-Level Management
a.	Ability to create and manage multiple mail domains within a single instance of Messaging Solution
b.	Ability to use different Global Address Lists for each domain
c.	Ability to use different authentication stores for each domain
d.	Ability to delegated domain-level administrators to manage users and other settings specific to a domain
e.	Ability to create domain-specific custom branding of the web interface
f.	Ability to enable a domain admin to update account quotas up to a maximum set value
g.	Ability to set quota for each domain (either unlimited or a maximum value per account)
h.	Ability to move a domain
i.	Ability to search across mailboxes from the administration console
8.	Storage
a.	Messages (including attachments) sent to multiple users are stored once to optimize storage space
b.	Ability to set quotas for mailbox size and number of Contacts
c.	View of mailboxes sortable by quota, total mailbox size, or % quota consumed
d.	Ability to define retention policies for all messages, trashed messages, and/or junk messages
e.	Ability to move a mailbox(es) from one server to another without requiring system downtime or affecting other mailboxes
f.	Ability to run a regularly scheduled process that moves older messages to a secondary storage volume
9.	System Health & Security
a.	Should have native anti-virus & anti-spam mechanism
b.	Administrator interface setting to specify spam quarantine and kill thresholds

c.	Messages that users mark as Junk / Not Junk are automatically fed into the spam training engine
d.	Administrator interface setting to define the update frequency for virus signatures
e.	Ability to enforce client authentication to the SMTP server before relaying mail (with option to require authentication over TLS)
f.	Graphical display of system activity including disk usage, message volume, and AS/AV results
g.	Ability to monitor the status of all core system servers/services in a single view
h.	Ability to block attachments based on criteria such as attachment type or size
i.	Ability to enforce that attachments be viewed as HTML, enabling risk-free attachment viewing without requiring attachment-native applications on the viewer's machine
j.	Install and manage certificates from the administration console
10.	Compatibility & Interoperability
a.	MAPI-based synchronization of mail, contacts, and calendar data between Outlook and the proposed solution server
b.	Online/offline status is automatically detected, enabling the user to work without having to specify their connection status
c.	Synchronization operations are cached and synchronized as an asynchronous process, enabling optimal Outlook performance
11.	Mobile Devices
a.	AJAX Mobile Web Browser
b.	i-Phone Email, Contact, Calendar sync
c.	Windows Mobile and other smartphone Email
d.	Email, Contact, Calendar sync
e.	Documents should be captured through mobile interface, it should fulfil following additional requirements: Application should provide rules and validations in the built-in form to avoid wrong data entry Mobile interface will also be used for Workflow based decision making applications. Application should support 3-tier architecture Application should be integrated with any domain controller system i.e. LDAP The application should merge multiple captured pages to one single page for each document type The application should perform the imaging features like Noise removal, perspective correction, enhanced image quality The application supports all the password policies. The application should provide user as well device level rights management.

5.2.3.8. Functional & Technical Requirements for Identity Access Management

S.No.	Description
1	Identity Management
1.1	The Identity and access management should be able to provide complete user lifecycle identitymanagement for all types of users.
1.2	The solution should provide identity management, governance and Identity managementportal, including entitlement certification and role management
1.3	The proposed solution should provide user provisioning and de-provisioning on all targetsystems, automatic account provisioning, removal, and approval processes throughout the user’s entire lifecycle.
1.4	The proposed solution should have customizable workflows to support the unique wayenvironment approves, alerts, and schedules these activities.
1.5	The proposed solution should provide centralized control of identities, users, roles and policiesacross on-premise and cloud applications.
1.6	The proposed solution should provide User self-service to manage attributes of their ownidentities, reset passwords and request access to resources.
1.7	The proposed solution should support Password Synchronization to reflect changes in identitymanagement systems and target applications
1.8	The proposed solution provide Privilege cleanup by examining existing system entitlements andhighlights excessive or unnecessary privileges. Delivers details such as such as how often a resource was accessed or if an entitlement causes a security policy violation.
1.9	The proposed solution should provide Identity and access governance policies usingcentralized engine that helps establish and enforce a consistent set of business and regulatory compliance policies.
1.10	The proposed solution should support Entitlements certification by providing easy to use interface through which managers or resource owners can view and certify that privileges are appropriate or should be removed, thus helping meet compliance requirements.
1.11	The proposed solution should support Role modeling analysis to efficiently sort throughextremely large volumes of user and privilege information to discover potential roles.
1.12	The system should be able to detect any changes in the target systems via the concept ofreverse synchronization and associate various actions upon detection
1.13	The solution should have ability to perform bulk jobs for example user changes, scheduled jobs
1.14	The proposed solution should offer an easy-to-use, configurable user-centric Risk Model thatidentifies areas of risk caused by users with high risk scores.
2	Single Sign on under Identity Management
2.1	The solution should have a capability which helps to prevent unauthorized users from hijackinglegitimate sessions with stolen cookies and assures that the client who initiated the session is the same client that is requesting access.

2.2	The solution should have capability to support various SSO architectures that can be used independently or mixed and match to meet various business needs such as: Agent-based policy enforcement points Centralized gateway enforcement points Support for today's open standards including SAML, OAuth, OpenID and WS-Federation
	Agent-less based approach to securely pass claims to applications without the use of proprietary APIs REST and SOAP-based Web APIs to allow applications to remotely call Single Sign-On as a Web service for authentication or authorization
2.3	The solution should provide secure single sign-on and flexible web access management to applications and Web services either on-premise, in the cloud, from a mobile device or at a partner's site.
2.4	The solution shall support SSO by passing the user's identity among heterogeneous servers securely. No additional authentication is required.
2.5	The solution should provide session assurance.
2.6	The solution should provide centralized session management to securely manage a user's online session.
3	Privilege Access Management Under Identity Management
3.1	The proposed solution should be appliance based and provide the capability to manage Password Vault, Access Management, Session Recording, Application to Application (allows dynamic password access from applications), etc. within a single hardened platform.
3.2	The proposed solution should support a process to automatically synchronize with a DR site over a WAN and provide built-in replication of the password vault aiding disaster recovery
3.3	The Proposed solution should have ability to define a zero trust, explicitly allow only access methodology.
3.4	The proposed solution should provide built in Active-Active High Availability and Load Balancing along with built-in clustering without the use of a traffic load balancer.
3.5	The Proposed solution should have ability to provide real-time data synchronization among a cluster.
3.6	The proposed solution should not require using third party software or hardware such as Operating Systems, Databases, High Availability, Load Balancers, etc.
3.7	The proposed solution should be browser independent and there shouldn't be any browser dependency to manage and record the sessions.
3.8	The proposed solution should provide highly efficient integrated video session recording with low storage requirements.

3.9	The proposed solution should provides in-line command filtering using white lists/black lists for SSH, network devices command line operations.
3.10	The proposed solution should be able to support application based session via RDP protocol in which the user can be confined, rather than requiring RDP to a full desktop.
3.11	The proposed solution should support to require an approval by designated users as a conditionof accessing the credentials for managed accounts. The Solution should also enforce users to specify reason when requesting access for a privileged account.
3.12	The proposed solution should provide tools/APIs for enabling applications that require accessto privileged accounts to access credentials programmatically, eliminating the need to "hard code" credentials into the script or application. Password should be rotated automatically.
3.13	The Proposed solution should have ability to manage target OS, Databases, Network, security devices, Virtual and cloud environments local administrator credentials through singleappliance.
3.14	The proposed solution should provide threat analytics that provides a continuous, intelligentmonitoring capability that helps enterprises detect and stop hackers and malicious insiders before they cause damage.
4	Host Based Access Control Under Identity Management
4.1	The proposed solution should provide granular access control on critical Servers to protect the access even if the servers are accessed directly from the console.
4.2	The proposed solution should support all Unix, Linux and Windows platforms and should beagent based.
4.3	The proposed solution should control and monitor privileged user access to files, folders, processes and registries, enabling accountability, incoming/outgoing TCP/IP protection, integrity monitoring and segregation of duties.
4.4	The proposed solution should restrict super-user privileges with finer level of granularity thanwhat is available in the host operating system.
4.5	The proposed solution should support authentication to Linux and Unix using Windows ADcredential and also provide User ID management (including UNIX files and NIS)
5	Authentication under Identity Management
5.1	The proposed solution should provide PKI and Risk Based authentication. It should also supportmobile OTP.
5.2	The proposed solution should have tight integration with proposed SSO solution
5.3	The proposed solution should have Pre-built rules that cover typical fraud patterns.
5.4	The proposed solution should support customization of pre-built rules or creationof new rules quickly and easily.
5.5	The proposed solution should Self-learning scoring engine based on statistical modeling
5.6	The proposed solution should have Device identification mechanism using multiple variabledevice fingerprinting

5.7	The risk based engine should also use geo location criteria
5.8	The proposed solution should have policy-based system to flag and manage cases of suspicious activity.
5.9	The proposed solution should Integrate data from multiple channels.
5.10	The proposed solution should learn end user behavior and suggests step-up authentication when there is a deviation from normal behavior.
5.11	The proposed solution should support out of band authentication via SMS, Email and Voice including mobile push.

5.2.3.1. Functional & Technical Requirements for SSLi

Sr.No.	SSLi Specifications
1	Physical Specification
1.1	System must be 19-inch rack mountable 1 U form factor
1.2	System must have dedicated management port
1.3	System must have RJ-45 console port
1.4	System must have 5 x 1 G cu Interface , 4 x 10 G fibre ports
1.5	System must be a purpose built appliance and must not be the part of IPS, Proxy, DLP and Load-balancer
2	Performance
2.1	System must support 20 Gbps of L7 throughput
2.2	System must support 125 K Connection SSLi traffic
2.3	System must support 4 K SSLi CPS on RSA 2 K Key and 3 K SSLi CPS on ECDHE cipher
2.4	System must support 7 Gbps of bulk SSL throughput
2.5	System must support 1.5 Gbps outbound SSL interception
3	Application delivery partition/Virtual Context
3.1	System must support 30 Application delivery partition/Virtual Context
3.2	System must support dedicated configuration file for each Virtual context
3.3	System must support resource allocation to each context including throughput, CPS, Concurrent connection, SSL throughput
3.4	System must be able to modify the resource allocation on the fly without restarting/rebooting any context
3.5	All the virtual context must be available from day-1
4	DDOS
4.1	System must support protection from Fragmented packets
4.2	System must support protection from IP Option
4.3	System must support protection from Land Attack
4.4	System must support protection from Packet Deformity Layer 3
4.5	System must support protection from Packet Deformity Layer 4
4.6	System must support protection from Ping of Death
4.7	System must support protection from TCP No Flag
4.8	System must support protection from TCP Syn Fin
4.9	System must support protection from TCP Syn Frag
4.1	System must support connection limit based on source IP
4.11	System must support connection rate limit based on source IP
4.12	System must support request rate limit based on source IP
5	Traffic redirection features
5.1	System must support load-balancing of multiple security devices
5.2	System must support Explicit proxy functionality with proxy chaining

Sr.No.	SSLi Specifications
5.3	System must support traffic redirection based any L2-L7 parameters
6	SSL Insight features
6.1	System must Outbound SSL interception
6.2	System must support L2 and L3 mode of deployment
6.3	System must support ICAP integration with DLP and AV
6.4	System must support modification of headers
6.5	System must support before proxy interception (between Client and Proxy)
6.6	System must support SSL interception bypass based on source and/or destination IP
6.7	System must support SSL interception bypass based SNI values
6.8	System must support SSL interception bypass based URL category
6.9	System must support bump in a wire deployment mode
6.10	System must support interception of SSH traffic
6.11	System must support sending decrypted feed to upto 4 off path devices
6.12	System must support dynamic SSL interception for SSL traffic on any tcp port
6.13	System must support URL blacklisting and whitelisting
6.14	System must support TCL based scripts for custom rules
7	Redundancy
7.1	System must support VRRP based redundancy
7.2	System must support active-active and active-backup configuration
7.3	System must support automatic and manual configuration sync
7.4	System must support dynamic VRRP priority by traffic interface, server, nexthop and routes
7.5	System must support scale-out configuration upto 8 devices to support higher throughput
7.6	System must support dedicated VRRP setting per virtual context
8	Management
8.1	System must have Web-based Graphical User Interface (GUI)
8.2	System must have Industry-standard Command Line Interface (CLI)
8.3	System must support Granular Role-based\Object-based Access Control
8.4	System must support SNMP, Syslog, email alerts, NetFlow v9 and v10 (IPFIX), sFlow
8.5	System must support REST-style XML API (aXAPI) for all functions
8.6	System must support external authentication including LDAP, TACACS+, RADIUS

5.2.3.2. Functional & Technical Requirements for Enterprise Database

S.No.	Description
1.	Database License should be un-restricted and perpetual, to prevent any noncompliance in an event of customization & integration.
2.	Databases shall support multi-hardware platform.
3.	RDBMS should support Unicode with Indian Language support
4.	RDBMS should have spatial capability and should be capable of storing vector (2D, 3D), rasterdata as well as the metadata.
5.	Database shall provide standard SQL Tool for accessing the database. The tool should be able to monitor, maintain and manage the database instance, objects, and packages.
6.	Database shall have built-in backup and recovery tool, which can support the

	online backup.
7.	RDBMS should support of seamless data transformation from on premise to public cloud and from public cloud to on premise.
8.	DB should have in built mechanism to balance the data across the available database files
9.	RDBMS should provide database clustering support for high availability
10.	Should be an enterprise class database with the ability to support connection pooling, load sharing and load balancing when the load on the application increases.
11.	Database shall have built-in DR solution to replicate the changes happening in the database across DR site with an option to run real time or near real-time reports from the DR site.
12.	RDBMS should have mechanism to recover from a disaster with no loss of data”
13.	Database shall provide native functionality to store and retrieve XML, Images and Text datatypes.
14.	Database shall provide native functionality to store XML, within the database and support search, query functionalities.
15.	RDBMS should support spatial data types.
16.	Database shall have Active-Passive or Active-Active failover clustering with objectives of scalability and high availability.
17.	Database shall provide control data access down to the row-level so that multiple users with varying access privileges can share the data within the same physical database.
18.	Database shall be having built-in provision to Administer database / database clusters, Monitor performance, Maintain database, Backup and recovery, Recovery management, Disaster recovery management.
19.	Database shall be having native auditing capabilities for the database.
20.	Database shall be having built-in provision to Administer database / database clusters, Monitor performance, Maintain database, Backup and recovery, Recovery management, Disaster recovery management.
21.	Availability of recovery/restart facilities of the DBMS.
22.	Automated recovery/restart features provided that do not require programmer involvement or system reruns.
23.	RDBMS should be able to recover after the DB restart and should have a consistent data for the application
24.	RDBMS should have the ability to manage recovery/restart facilities to reduce system overhead.
25.	Provides extra utilities to back up the databases by faster means than record by record retrieval.
26.	The database should provide controls over who, when, where and how applications, data and databases can be accessed.
27.	RDBMS should be possible to prevent privileged IT users such as DBAs and administrators from accessing and modifying the data.

28.	Should provide adequate auditing trail facility. Audit trail should also be maintained at database level for any changes made in database and it should be ensured that these audit trails cannot be manipulated by anyone including super users and DBAs.
29.	System should have the ability record all system level changes for audit purpose.
30.	Solution should offer spatial analytic functions for data mining applications, such as binning, spatial correlation, co-location mining, spatial clustering, and location prospecting

5.2.3.3. Functional & Technical Requirements for Directory Services

S.No.	Description
1.	Should be compliant with LDAP v3
2.	Support for integrated LDAP compliant directory services to record information for users and system resources
3.	Should provide authentication mechanism across different client devices / PCs
4.	Should provide support for Group policies and software restriction policies
5.	Should support security features, such as Kerberos, Smart Cards, Public Key Infrastructure (PKI), etc.
6.	Should provide support for X.500 naming standards

5.3. Data Centre and Disaster Recovery Centre

SI has to implement City Data Centre to cater the requirements of Data compute, storage and for city analytics purpose.

- a) PSCL shall provide the location to house the compute and storage infrastructure at the Data Centre facility being built in the premises of the Command and Control Centre.
- b) The DR for the data centre shall be on an Active-Passive mode on Cloud on empaneled service providers by MeITY and audited by STQC.
- c) Various ICT equipment to be provisioned and maintained by SI at the Data Centre is given below.
- d) Only the minimum specifications for the active and passive ICT and Non-ICT components are specified.
- e) SI may propose Data Centre Virtualization solution for price discovery and use all Bihar smart cities as virtual cloud to share the storage between the cities.
- f) SI shall peruse the same provide the BOM / BOQ required to meet the performance requirements as per the proposed business needs. SI may also suggest additional components as per the solution requirements.
- g) The information between the Smart DC and the DR cloud shall be synchronized over the network such that that the smart city solutions are high available on the network.
- h) Operational and Uptime Requirements for Data Centre.

- i) Minimum Tier Rating for Data Centre: **Tier 3**
 - i. Availability Target (24Hr operation): 99.741%
 - ii. Maximum Downtime Tolerated per Day: 4 minutes
 - iii. Maximum Downtime Tolerated per Week: 27 minutes
 - iv. Maximum Downtime Tolerated per Month: 1 hours 54 minutes
 - v. Maximum Downtime Tolerated per Quarter: 5 hours 42 minutes
 - vi. Maximum Downtime Tolerated per Year: 22 hours 43 minutes
- j) Operational Compliance Requirements for SI operations:
 - i. PCI-DSS
 - ii. ISO 27001
 - iii. ISO 20000
 - iv. Cyber Security Framework for Smart City (MoUHA)

Note: Operational Compliance applicable for Data Centre, ICC and NOCs

5.3.1. Disaster Recovery and DR Cloud

- a) SI shall also be responsible for providing Cloud service for storing all applications at DR [minimum 50% production capacity, RTO – 30 mins, RPO – 30 mins] which will be implemented under PSCL Smart City project for the project duration. Performance SLA will be applicable while operations from DR site.
- b) All applications need to have high performance clustering (redundancy) within the Data Centre with automatic fail-over, and redundant data storage in active passive or active-active configuration as per the high availability targets. The data replication should be continuous among all the servers and shared storage should not be used. All mission critical systems must be active-active configurations. Active-passive configurations may be permissible for supporting applications.
- c) The proposed Cloud Service Provider (CSP) must be an empanelled cloud service provider by Meity (Ministry of Electronics and Information Technology for Public cloud, Virtual Private Cloud and Community Government Cloud).
- d) The Cloud Data Centre Facility must be within India and must be Tier III or above. The DR site within India should be at least 250 Km away from the PSCL Data Center and in a different seismic zone.
- e) SI also need to ensure that the CSPs facilities/services are certified to be compliant to the following standards:
 - a. ISO 27001 – Data Center and the cloud services should be certified for the latest version of the standards
 - b. ISO/IEC 27017:2015 – Code of practice for information security controls based on ISO/IEC 27002 for cloud services and Information technology
- f) The cloud service provider must have billing model of pay-per-consume where it will charge for amount of computing resources being consumed by application rather than for the allocated resources. SI shall provide the rate chart of the cloud services to PSCL.
- g) Cloud services should be accessible via Internet, Point to Point / MPLS, Leased Lines, OFC WAN etc. SI must provide private connectivity between PSCL's network and Cloud Data Centre Facilities.
- h) SI shall be fully responsible for upgrades, technological refreshes, security patches,

bug fixes and other operational aspects of the infrastructure that is in the scope or purview of SI.

- i) SI shall provide interoperability support with regards to available APIs, data portability etc. for PSCL to utilize in case of Change of cloud service provider, migration back to Local Data Centre, burst to a different cloud service provider for a short duration or availing backup services from an alternate Cloud service provider.
- j) SI is required to prepare and submit along with their technical proposal, the details of methodologies and computations for sizing and capacity of storage, compute, backup, network and security resources.
- k) PSCL shall retain ownership of all virtual machines, templates, clones, and scripts/applications created for PSCL’s applications. PSCL shall retain the right to request (or should be able to retrieve) full copies of these virtual machines at any time.
- l) In no circumstances, the data accumulated and processed by Command Control and Communication Centre should be compromised. Hence, provisions will be made to keep all the data stored in this platform highly secured with required multi layered security access control and authorization framework. Further the platform shall provide an open standards based Integration Bus with API Management, providing full API lifecycle management with governance and security features.
- m) Additional Parameters
 - i. SI should configure, schedule and manage backups of all the data including but not limited to files, folders, images, system state, databases and enterprise applications.
 - ii. Encryption of all backup files and data and management of encryption keys as a service that can be enabled for Government Departments that require such a service.
 - iii. SI should offer dashboard to provide visibility into service via dashboard.
 - iv. SI shall not delete any data at the end of the agreement (for a maximum of 45 days beyond the expiry of the Agreement) without the approval of the PSCL.

A High Level Design (HLD) for cloud deployment should be suggested by the SI. SI can suggest security stack & deployment method according to their recommendations;

5.3.2. Preparation of Disaster Recovery Operational Plan

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

- a) Business as usual: the primary site is functioning as required, procedures for ensuring consistency of data availability at secondary site.
- b) Disaster: Declaration of disaster, making the DR site live for production, ensuring availability of users to the secondary site.

- c) Operations from DR site: Ensuring secondary site is addressing the functionality as desired
- d) Configure proposed solution for usage

5.3.3. Functional & Technical Requirement for DR Management

S.No.	Features
1	The proposed solution must offer a workflow based management& monitoring and reporting capability for the real time monitoring of a DR solution parameters like RPO (at DB level), RTO, replication status and should provide alerts(including SMS and e-mail alerts)on any deviations. The proposed solution should be able to conduct DR Drills from a centralized location
2	The proposed solution should provide a single dashboard to track DR Readiness status of all the applications under DR
3	The proposed solution should be capable of reporting important health parameters like disk space, password changes, file addition/deletion etc. to ensure DR readiness
4	The proposed solution should have inbuilt ready to use library of recovery automationaction for heterogeneous databases and replication environment. This must significantly reduce custom development of scripts and speedy deployment of DR solutions
5	The proposed solution should facilitate workflow based switchover and switchback for DR drills for standard applications based on industry best practices
6	The proposed solution should facilitate workflows for bringing up the applications and all the components it depends on at DR while it is up at primary site without pausing/stopping the replication

5.3.4. Periodic Disaster Recovery Plan

The service provider shall be responsible for–

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

5.4. Mobile App

With rapidly increasing levels of mobile penetration and continuous improvement in bandwidth, and requirements of accessibility and citizen convenience, it has been envisaged to offer information dissemination to stakeholders over mobile devices. There shall be a strong interfaces, technologies, applications etc. for mobile devices.

App’s architecture must provide for a robust mobile backend layer, providing for listed functionalities like push/pull notifications, storage of images, geolocation, advanced analytics etc. with standard Active-Active clustering on high availability mode. SI can consider a public cloud based deployment for such mobile backend layer, as per modern architecture standards. In order to maximize citizen convenience and bring about

business process improvements, the successful SI shall continuously innovate, upgrade and incorporate such new technologies that emerge new avenues.

Functional and Technical Requirements :

S.No.	Description
1	Mobile app should mirror the portal and be adapted for optimum viewing on multiple operating systems and device sizes. However the actual application layout design for both mobile and web is the responsibility of SI.
2	Mobile app must be based on latest HTML 5 and above.
3	Mobile app shall be hybrid on Android, iOS and Windows platform.
4	Mobile app should be in Hindi & English and capable to take the load of all concurrent users at peak time. SI has to evaluate and make the app's functioning smooth for peak load.
5	Mobile app should be capable of showcasing enriched infographics to its stakeholders.
6	Mobile app shall be designed in such a manner that it shall address the following key issues: <ul style="list-style-type: none"> ▪ Caching: Caching unnecessary data on a device that has limited resources ▪ Communication: Failing to protect sensitive data over any carrier ▪ Data Access: Failing to implement data-access mechanisms that work with intermittent connectivity
7	Mobile app shall be integrated with main core solution proposed. There shall be facility to PUSH through and PULL through mechanism to get and receive information using SMS service.
8	Mobile app shall provide critical data such as user identification and location information including latitude, longitude and altitude.
9	The mobile app shall have the ability to take and transmit, pictures and videos in real time along with geo-tags from the device.
10	Mobile app should have capability of - <ul style="list-style-type: none"> ▪ Image compression, B/w conversion from color images ▪ Auto cropping, Auto orientation, perspective correction, geo capture ▪ Image capture setting (camera resolution, image type)
11	Mobile app shall have the ability to post bulletins and resources on another mobile app through API's.
12	Platform will provide a report generating tool, which can be used to generate customized reports at any level.
13	Platform should allow for a graphical interface to view the summary data in MIS reports. This would include trend graphs, graphs indicating how much of the target has been met etc.

5.5. Network Backbone and Internet Connectivity

Overview

- a) Pan city network backbone and internet 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 reliable, secure and supports the required SLA parameters of Latency, Jitter, Packet Loss and Performance. City wide network is essentially intended to provide high-speed network connectivity for supporting all existing and future smart solutions. The project objectives broadly are as follows:

- To provide inexpensive and pervasive connectivity all across the city
- To boost digital inclusion among departments and citizens
- To provide 24*7 uninterrupted connectivity across the city
- 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
- To enable the government to have advanced communication products/platforms and better security and surveillance systems

The IP High Level Design is recommended to be built on a hierarchical model with a N+1 redundancy. The main design methodology is to focus on essential functional layers where hardware of different traffic handling capacity can be plugged in and out as the city grows. The different design blocks that create the network high level architecture are:

- Core
- Distribution/Aggregation
- Access

A typical Network Architecture is shown in **Figure** below:-

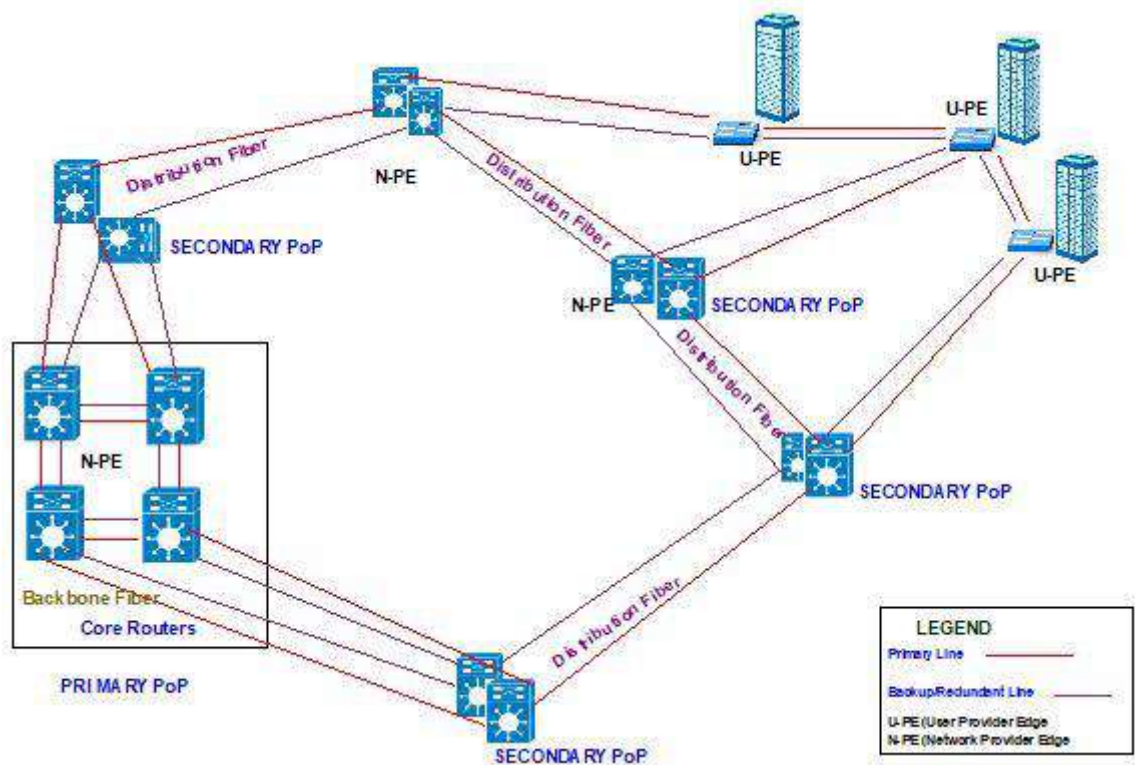


Figure 5: Design of Distribution and Access Network

The Access nodes provide different UNI (User-Network Interface) options as well as performing service multiplexing, subscriber security considerations and any or all the other functionality required for triple play service delivery and support. Another important consideration is that for Multi Dwelling Units (MDU) (Either commercial or residential buildings), the Access switch (U-PE) will reside in the Tertiary-PoP. The media choices for Access are either copper access, such as Category 6 unshielded twisted pair, or fiber. A pair of Access U-PEs devices in every PoP shall be used to terminate and support services like Video Surveillance, Traffic Management etc.

The Core layer would initially support 100Gbps network to support up to 200 Gbps eventually. For Distribution/Aggregation layer initially it would support 50 Gbps and later 100 Gbps and for the Access layer it would be 10 Gbps initially and 50Gbps at a later stage. The Core backbone, Aggregation zone backbone and the Access layer backbone with Ring topology all would be 96 core OFC. Each Core zone could contain many Distribution sites connected in a full mesh/ring topology. There will be at least one Distribution site per Primary and Secondary PoP.

Each Distribution link towards the Core will initially provide 50 Gbps of bandwidth in a redundant manner therefore the whole bandwidth on a Distribution node will be 100 Gbps. Similarly for the whole Distribution site total bandwidth handling capacity will be 200 Gbps i.e. 100 Gbps per Distribution Node. At a Primary-PoP the Distribution site equipment will be co-located with the Core equipment in order to serve the city blocks in the vicinity. Access nodes have high speed fiber point-to-point links towards the Distribution layer supporting bandwidths from 10 Gbps or higher. They have low speed fiber, copper or wireless links towards customer CPEs supporting bandwidths from 1 Gbps to 10 Gbps.

Assumptions

Minimum expected bandwidth for Services(single entity) such as Internet BW, IP TV BW, VAS, Video game etc. would be around 800 Mbps.

Each residential or commercial entity shall be connected using a 1 Gigabit physical interface.

Each residential unit will have only one Home Access Gateway(HAG).

Each commercial, business or utility will be provided with at least one Customer Premises Equipment (CPE). Additional CPE devices can be provided on demand to meet redundancy or high availability requirements

The HAG or CPE shall be the demarcation point between the customer and the OAN provider.

The Access switches of the OAN provider will be placed in the Main Telecom Rooms of

the residential, commercial or utility buildings.

Access switches will be also placed in the PoPs to meet the requirements of some of the public services.

The Primary PoP will have core equipment. Secondary PoPs will have Aggregation equipment and Tertiary PoPs will have Access equipment to provide connectivity's.

The proposed smart city solution will involve city wide network coverage across various locations in PSCL. PSCL smart city will offer various smart services to its citizens. To provide these services in an uninterrupted and effective manner a robust network is required to be deployed. Network needs to be planned to meet the all the network requirements for currently services envisaged, scalability and future requirement. PSCL intends to provide connectivity at locations like; municipal offices, Bus depots, traffic junctions, parks, fire brigade, police stations, urban health centers, schools etc. SI would be required to create a single network i.e. city wide network for the smooth functioning of all solutions. Successful bidder is required to integrate city wide network with Data center (DC), Disaster recovery (DR) and Command Control & Communication Center (ICCC).

PSCL intends to procure Leased Circuits & Internet Bandwidth for the city wide network under the PSCL smart city Project. The successful bidder is required to terminate the desired Leased circuits and Internet Bandwidth at the locations to be identified by SI in consultation with PSCL.

A Service Level Agreement will be signed with the successful bidder. As bidder, will be responsible for smooth functioning of the entire network connectivity, availability of sufficient quantities of all the critical components will be taken care of by the bidder to maintain the guaranteed uptime. Bidders are requested to take into consideration the equipment's required at each location for providing connectivity while quoting for the tender.

Full Duplex Bandwidth as Per Schedule of Requirement has to be provisioned and implemented by the Service Provider. Service Provider has to keep provision of giving burstable Bandwidth & the rates will be as per finalized rates. Service Provider has to arrange fiber & other last mile equipment accordingly including media convertors wherever required.

5.5.1. Scope of work

The detailed scope of work for SI for providing of pan city network backbone is given below:

a) Bandwidth Provisioning

SI shall implement the solution in and procure & provision the network bandwidth as per details given below. SI shall be responsible for upgrading its infrastructure, including the last mile, to meet the requirements of the PSCL, at no additional cost to the PSCL. The network & bandwidth should meet following requirements:

- i. PSCL may order an increase/decrease/termination/withdrawal in bandwidth, which bidder shall take into account.

- ii. The network should be capable of providing Bandwidth on Demand for planned as well as for unplanned activities.
- iii. SI should provide the bandwidth for intranet & internet.

Internet Bandwidth at ICCC, Data Center and all field locations

- i. PSCL is procuring bulk internet bandwidth for the requirement of various locations throughout the city. SI is required to terminate these links at the desired locations defined as per the price bid format of this RFP.
- ii. Redundancy
- iii. As a measure of redundancy remote locations, ICCC, DC & between DC & DR site connected through Leased Circuits should have redundancy in place to meet necessary SLA requirements.
- iv. Location-wise Bandwidth requirements should be planned by SI
- v. Rate Contract
- vi. PSCL is procuring leased circuits to be delivered at various locations spread across the PSCL city.
- vii. Looking at the scalability and future requirement discovery of prices shall be valid for the period of contract duration under the Rate Contract as per price bid.
- viii. It has been observed that there is a considerable price reduction in cost of domestic and Internet bandwidth during last few years. Hence, PSCL will review the prices at end of every year and SI is required to match the prevailing market prices as per TRAI regulations.
- ix. Adding new location – whenever a new location is decided to be added by the PSCL, an order will be placed with SI at the contracted price. SI shall carry out site-survey at new location for feasibility of location over wired connectivity. SI would be required to implement and commission the location within 2 weeks from the date of work order.

5.5.2. General Specifications

The areas covered under Bidder's scope are as follows:

IT Data Center complete in all respect (UTP / STP CAT 6A, 10G and 10G fiber (Single Mode OM3 OM4 fiber)

All cabling will be Intelligent Cabling Solution for Facility and for Rack to Rack connectivity MTP 40G Solution.

Backbone between Spine and Leaf switches (Single Mode OM3 fiber) and Spine Switches to Leaf Switches in Hub rooms for sitting area (Multi Mode OM3 fiber).

The server racks and storages may have any of the three possible interconnects Structured cabling involves supply, installation, testing and commissioning of all Jack panels, Network/Server Racks, Laying of cables (FTP/Fiber), Terminations at both end and other passive components.

Cable laying will be through metal raceways, PVC conduits, overhead ladder / tray and other relevant activities.

Laying of FTP Cable in raceways includes proper bunching and tagging for Data/ Voice Cable including color coding.

Preliminary continuity Testing & Ferruling at both end for the each cable, unique identity by proper Tagging.

Termination, Installation, Fixing of 24 Port Jack Panels including proper Dressing of Cables Fixing & Casio labeling of Jack Panels.

Installation & proper routing of Patch Cords in Racks, Jack Panels and wire/ cable manager with tagging of Mounting Cords.

Installation of Network rack with proper cable management, Ladder Fixing, fixing of panels including control panels, fixing of Vertical Wire Manager, Horizontal Wire Manager etc.

Penta-Scanner Testing of laid FTP Cables for the performance testing of Installed Cabling System with EIA/TIA specified parameters like Resistance, Delay, Attenuation, Wiremap, Return Loss, PSNEXT, PSELFEXT, ACR etc.

Documentation of the Installed Network with the as built Diagram and labeling details of the I/O's and Jack Panels and Penta-Scanning Results of Nodes
Fiber termination and Management System and Fiber routing also has to be included in the scope.

The bidder shall give the break-up prices of each component being used in the scope of structured cabling.

Though the approximate no. of ports per facility is given below, the bidder may add points they feel necessary for any particular facility after obtaining necessary approval.

All horizontal cabling should emanate from Jack panels on the distribution switch and be routed to outlets nominated through ceiling space, risers, skirting duct and workstation partition duct etc.

The cables must be laid in an aggregated manner to reduce the cabling space requirement.

Cables should be installed in a workman like manner, parallel to walls, floors and ceilings, as applicable.

The Manufacturers cable form should be maintained at all times. No distortion due to kinks, sharp bends or excessive hauling tension should be allowed to occur during installation.

Care should be taken to prevent other trades damaging the cable by walking or storing heavy objects on them whilst laying out and installation.

Cables should be run in a manner eliminating any possibility of strain on the cable

itself or on the terminations.

Cables entering or exiting trays, conduits, centenary wires and other fixed support should have a small gooseneck or slack provided and should be fixed at both ends to prevent the possibility of cable stress.

Cables should be concealed except where nominated otherwise, and should run in neat lines.

Cables should have no joints or splices, all foil should necessarily be grounded at all terminations.

Cables should be kept at a minimum distance of 150mm from items liable to become hot or cold. The distance should be consistent with the maximum or minimum temperature possible and the cable type. Cables should at no point make direct contact with such items.

Cables should not be directly embedded in plaster, concrete, mortar or other finishes unless they are in conduit and capable of being fully withdrawn and replaced after the building is finished without damage to finishes.

Bending radius should not be less than the manufacturer's recommendation and in any case should be not less than eight times the overall cable diameter.

Cabling will run in separate shafts and ducts from the electrical ducts so as to avoid any interference.

Cable should either have a nylon sheath or should be enclosed in a conduit if running underground.

Under no circumstance hand labeling of the cables will be accepted. No hand punching shall be allowed without proper tools. Labeling and Punching should be done as per TIA/EIA standards.

All copper conductors must be tested for continuity and pair integrity as well as EMI interference.

Any cable that does not meet TIA/EIA specifications should be repaired or replaced at the Vendor's expense.

The termination of connectors should be RJ-45 Single Information Outlets with faceplates, shutter and Surface box.

The Fibre Couplers and Connectors generally would be LC type.

There should be Professional Cable Management and tools available on site e.g. FTP Cable Termination tools.

Each outlet shall be tested for satisfactory operation based on certification parameters valid for the entire warranty period of 20 years or more as applicable. All

outlets in the Facility be clearly marked, labeled & documented for future reference.

Maintenance of the LAN Passive components shall be done by the Agency. Provision of additional Passive nodes whenever required shall need to be provided based on requests. The bidder must quote per termination charges in various slabs.

Cable layout plan should be submitted as part of the technical bid.

5.5.3. Technical Specifications

a) Leased circuit:

- i. The bandwidth must be provisioned on Optical Fiber Media. No other last mile media type is acceptable.
- ii. Latency from point A to point B should not exceed 20 ms.
- iii. The bandwidth supplied should be symmetric, dedicated 1:1 with 100% throughput.
- iv. Up time guarantee must be 99.5 %
- v. SI must deliver this bandwidth on a fiber optic cable network at the respective locations.
- vi. All costs to connect the links to last mile node of SCADA has to be borne by SI. PSCL will not pay or reimburse any last mile of extra work cost.
- vii. SI has to use the IP addressing schema provided by the SCADA.

b) Internet Bandwidth

- i. The bandwidth must be provisioned on Optic Fiber media only. No other last mile media type is acceptable.
- ii. PSCL is procuring bulk internet bandwidth (as per the Price bid) for the requirement of various locations throughout the city. However, successful SI is required to terminate these links at the desired locations.
- iii. Latency to Google, Yahoo and NIXI peering should not exceed 200 ms.
- iv. The bandwidth should be dedicated 1:1 with 100% throughput.
- v. Up time guarantee must be 99.7%
- vi. Provider must have minimum two sources of Internet Gateway bandwidth input.
- vii. SI must deliver this bandwidth on Gigabit Ethernet optically or electrically which will be taken as input.
- viii. SI must deliver the required bandwidth on a fiber optic cable network at the desired locations.
- ix. All costs to connect the link to the last mile node has to be borne by SI. PSCL will not pay or reimburse any last mile of extra work cost.
- x. Detailed IIM Specification are given in Annexure

5.6. Public Address (PA) System

Overview

- a) The Public Address System (PA) shall be capable of addressing citizens at specific locations from the ICC.

- b) The proposed system shall contain an IP-based announcing control connected to the ICC.
- c) Public Address system shall be used at intersections, public places, market places or those critical locations as identified by PSCL to make important announcements for the public.
- d) The system shall contain an IP based amplifier and uses PoE power which shall drive the speakers. The system shall also contain the control software which shall be used to control/ monitor all the components of the system which include Controller, Calling Station & keypad, Amplifier (Mixing & Booster).
- e) It shall be able to broadcast messages across all PA systems or specific announcement could be made to a particular location supporting single zone / multi zone operations.
- f) The system shall also deliver pre-recorded messages to the loud speakers attached to them from CD/DVD Players & Pen drives for public announcements.
- g) The system shall contain an IP-based amplifier and uses PoE power that could drive the speakers. The system shall also contain the control software that could be used to control/monitor all the components of the system that includes Controller, Calling Station & keypad, Amplifier (Mixing & Booster).
- h) PA system's master controller shall have function keys for selecting the single location, group of locations or all locations, simple operation on broadcasting to any terminal or separated zones.
- i) PA system's master controller should facilitate multiple MIC inputs and audio inputs.

Scope of Work

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

- a) SI shall install IP based Public Address System as part of the information dissemination system at 50 locations (tentative) in the city. These systems shall be deployed at identified junction to make public interest announcements.
- b) The system deployed shall be IP based and have the capability to be managed and controlled from the ICC
- c) SI, in consultation with PSCL can propose alternate locations apart from the locations mentioned in this RFP for installing the PA system where their effectiveness in communicating information about traffic conditions in PSCL will be maximized.
- d) PSCL shall review and approve the proposed locations. SI shall install the PA system on the approved locations.
- e) Should have the capability to control individual PAS i.e. to make an announcement at select location (1:1) and all locations (1: many) simultaneously.
- f) The PAS should also support both, Live and Recorded inputs and have minimum following capability
 - i. Speaker: Minimum 2 speakers, To be used for Public Address System
 - ii. Connectivity: IP Based
 - iii. Access Control: Access control mechanism would be also required to establish so that the usage is regulated.

- iv. Integration : With VMS and Command and Control Centre
- v. Construction: Cast Iron Foundation and M.S. Pole, Sturdy Body forequipment
- vi. Battery: Internal Battery with different charging options(Solar/Mains)
- vii. Power: Automatic on/off operation
- viii. Casing IP-55 rated for housing

5.7. Emergency Call Box (ECB) System

Overview

A high quality digital transceiver, to be placed at strategic locations determined by the PSCL. Key is to make it easily accessible by public. The unit shall have a button which when pressed, shall connect to the ICCV over the existing network infrastructure setup for ITMS project. These are to be placed only at a select locations such as CCTV field of view to avoid misuse and vandalism of the call box.

Scope of Work

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

- a) SI shall also install Emergency Call Box/Panic buttons at 50 locations (the final no. might vary based on field survey by SI) in the city. These systems shall be deployed at identified junction for ease of access by citizens of PSCL city.
- b) SI, in consultation with PSCL can propose alternate locations apart from the locations mentioned in this RFP for installing ECB system where their effectiveness in communicating information about traffic conditions in PSCL will be maximized.
- c) PSCL shall review and approve the proposed locations. SI shall install ECB system on the approved locations.
- d) ECB should have minimum following capabilities:
 - i. Construction: Cast Iron/Steel Foundation, Sturdy Body for equipment
 - ii. Call Button: Watertight Push Button, Visual Feedback for button press
 - iii. Speaker: To be used for Public Address System
 - iv. Connectivity: GSM/RF/PSTN/Ethernet as per solution offered
 - v. Sensors: For tempering/ vandalism
 - vi. Battery: Internal / External Battery with different charging options (Solar/Mains) with minimum backup of 60 Minutes.
 - vii. Power: Automatic on/off operation
 - viii. Casing: IP-55 rated for housing

5.8. Variable Message Sign boards

Overview

- a) Central Control Software shall allow controlling multiple VMSB from one console.
- b) Capable of programming to display all types of Message/ advertisement having alphanumeric character in English and Hindi and combination of text with pictograms signs. The system should have feature to manage video / still content

for VMSB display.

- c) The system shall have capability to divide VMSB screen into multi parts to display diverse form of information like video, text, still images, advertisements, weather info, city info etc.
- d) The system shall also provide airtime management and billing system for paid content management
- e) Capable of controlling and displaying messages on VMSB boards as individual/group.
- f) Capable of controlling and displaying multiple font types with flexible size and picture sizes suitable as per the size of the VMSB.
- g) Capable of controlling brightness & contrast through software.
- h) Capable to continuously monitor the operation of the Variable Message sign board, implemented control commands and communicate information to the Traffic Monitoring Centre via communication network.
- i) Real time log facility – log file documenting the actual sequence of display to be available at central control system.
- j) Multilevel event log with time & date stamp.
- k) Access to system only after the authentication and acceptance of authentication based on hardware dongle with its log.
- l) Location of each VMSB will be plotted on GIS Map with their functioning status which can be automatically updated.
- m) Report generation facility for individual/group/all VMSBs with date and time which includes summary of messages, dynamic changes, fault/repair report and system accessed logs, link breakage logs, down time reports or any other customized report.
- n) Configurable scheduler on date/day of week basis for transmitting pre-programmed message to any VMSB unit.
- o) Various users shall access the system using single sign on and shall be role based. Different roles which could be defined (to be finalized at the stage of SRS) could be Administrator, Supervisor, Officer, Operator, etc.
- p) Apart from role based access, the system shall also be able to define access based on location.
- q) Rights to different modules / Sub-Modules / Functionalities shall be role based and proper log report should be maintained by the system for such access
- r) Components of the architecture must provide redundancy and ensure that there are no single points of failure in the key project components. To take care of remote failure, the systems need to be configured to mask and recover with minimum outage.
- s) The architecture must adopt an end-to-end security model that protects data and the infrastructure from malicious attacks, theft, natural disasters 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 Antivirus mechanism. There shall 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 shall be properly stored & archived for future analysis and forensics whenever desired.

- t) 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.
- u) System shall use open standards and protocols to the extent possible
- v) Facility to export reports to excel and PDF formats.
- w) Remote Monitoring
 - i. All VMSB shall be connected/configured to Traffic Monitoring system for remote monitoring through network for two way communication between VMSB and control Room to check system failure, power failure & link breakage.
 - ii. Remote Diagnostics to allow identifying reason of failure up to the level of failed individual LED.

Scope of Work

The broad scope of work to be covered under this component shall include the following, but is not limited to:

- a) Variable Message Sign Board (VMSB referred herein) shall be installed at identified strategic locations. The location of VMSB shall be on the key junctions (mostly on the sides without obstructing the traffic) and other strategic locations with large foot fall. The VMSB software application will allow user to publish specific messages for managing traffic and also general informative messages.
- b) VMSB shall enable PSCL/Police to communicate effectively with citizens and also improve response while dealing with exigency situations. These shall also be used to regulate the traffic situations across the city by communicating right messages at the right time.

These displays can also be used for advertisement purposes. Approximately 20% to 30% of the total running time will be utilized by PSCL in day-to-day scenario (i.e. normal, non-emergency situations) for its own discretion whereas the remaining time can be used for advertisement purpose. However during emergency or disaster situations, VMSB would be required to play messages issued by ICCC all the time till normal situation is restored.

System Requirements

- a) The system should be capable to display warnings, traffic advice, route guidance and emergency messages to motorists from the ICCC in real time.
- b) The system should also be capable to display warnings, traffic advice, route guidance

- and emergency messages to motorist by using local PC/Laptops.
- c) The VMSB should display text and graphic messages using Light Emitting Diode(LED) arrays.
 - d) The System should be able to display failure status of any LED at ICC.
 - e) The System should support Display characters in true type fonts and adjustable based on the Operating system requirement.
 - f) The VMSB workstation at the ICC should communicate with the VMS controller through the network. It should send out command data to the variable message sign controller and to confirm normal operation of the signboard. In return, the VMS workstation should receive status data from the VMS controller.
 - g) VMSB controllers should continuously monitor the operation of the VMS via the provided communication network.
 - h) Operating status of the variable message sign should be checked periodically from the ICC.
 - i) It shall be capable of setting an individual VMSB or group of VMSB's to display either one of the pre-set messages or symbols entered into the computer via the control computer keyboard or by another means.
 - j) It shall be capable of being programmed to display an individual message to a VMSB or a group of VMSB's at a pre-set date and time.
 - k) A sequence of a minimum of 10 messages/pictures/ pre-decided sign or group of signs shall be possible to assign for individual VMS or group of VMS's.
 - l) It shall also store information about the time log of message displayed on each VMS. The information stored shall contain the identification number of the VMS, content of the message, date and time at which displayed message/picture starts and ends.
 - m) The central control computer shall perform regular tests (pre-set basis) for each individual VMS. Data communication shall be provided with sufficient security check to avoid unauthorized access.

5.9. Variable Message Sign Board application

- a) Central Control and Communication Software should allow controlling multiple VMS from one console.
- b) Capable of programming to display all types of Message/ advertisement having alphanumeric character in English, Hindi, and combination of text with pictograms signs. The system should have feature to manage video / still content for VMS display.
- c) The system should have capability to divide VMS screen into multi-parts to display diverse form of information like video, text, still images, advertisements, weather info, city info etc. The system should also provide airtime management and billing system for paid content management
- d) Capable of controlling and displaying messages on VMS boards as individual/ group.
- e) Capable of controlling and displaying multiple font types with flexible size and picture sizes suitable as per the size of the VMS.
- f) Capable of controlling brightness & contrast through software.

- g) Capable to continuously monitor the operation of the Variable Message sign board, implemented control commands and communicate information to the ICCC via communication network.
- h) Real time log facility – log file documenting the actual sequence of display to be available at central control system.
- i) Multilevel event log with time & date stamp.
- j) Access to system only after the authentication and acceptance of authentication based on hardware dongle with its log.
- k) Location of each VMS will be plotted on GIS Map with their functioning status which can be automatically updated.
- l) Report generation facility for individual/group/all VMSs with date and time which includes summary of messages, dynamic changes, fault/repair report and system accessed logs, link breakage logs, down time reports or any other customized report.
- m) Configurable scheduler on date/day of week basis for transmitting pre-programmed message to any VMS unit.
- n) Various users should access the system using single sign on and should be role based. Different roles which could be defined (to be finalized at the stage of SRS) could be Administrator, Supervisor, Officer, Operator, etc.
- o) Apart from role based access, the system should also be able to define access based on location.
- p) Rights to different modules / Sub-Modules / Functionalities should be role based and proper log report should be maintained by the system for such access
- q) Components of the architecture must provide redundancy and ensure that there are no single points of failure in the key project components. To take care of remote failure, the systems need to be configured to mask and recover with minimum outage.
- r) The architecture must adopt an end-to-end security model that protects data and the infrastructure from malicious attacks, theft, natural disasters 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.
- s) 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.
- t) System shall use open standards and protocols to the extent possible
- u) Solution shall be integrated with the environmental monitoring system for automatically displaying information from environmental sensors.
- v) Facility to export reports to excel and PDF formats.

5.9.1. Remote Monitoring

All VMSB shall be connected / configured to ICCC for remote monitoring through network for two way communication between VMS and control Room to check system failure, power failure & link breakage.

- a. Remote Diagnostics to allow identifying failure up to the level of failed individual LED.
 - i. Minimum 3.0m length X 1.5m height X 0.2m depth. (3000mm x 1500mm X 200mm approx.)
 - ii. Colour LED: Full Colour, class designation C2 as per IRC/EN 12966 standard
 - iii. Luminance Class/Ratio: L3 as per IRC/EN 12966 standards.
 - iv. Luminance Control & auto Dimming
 - v. Should be automatically provide different luminance levels but shall also be controllable from the traffic centre using software.
 - vi. Auto dimming capability to adjust to ambient light level (sensor based automatic control)
- b. Photoelectric sensor shall be positioned at the sign front and sign rear to measure ambient light. Capable of being continually exposed to direct sunlight without impairment of performance.
 - i. Contrast Ratio: R3 as per IRC/EN 12966 standard
 - ii. Beam Width: B6+ as per IRC/EN 12966 standards.
 - iii. Pixel Pitch: 12mm or better
- c. Picture Display
 - i. At least 300mm as per IRC/EN 12966 standards
 - ii. Full Matrix: Number of lines & characters adjustable, active area: 2.88m X 1.2m at-least
 - iii. Synchronized Dot to Dot display.
 - iv. Capable of displaying real time message generated by ICCC.
 - v. Special frontal design to avoid reflection.
 - vi. Display shall be UV resistant
 - vii. Viewing Angle: B6+ as per IRC/EN 12966 standard- Viewing angle shall ensure message readability for motorists in all lanes of the approach road
 - viii. Viewing Distance: Suitable for readability from 150 Mtrs. or more at the character size of 240mm, from moving vehicles.
- d. Self-Test
 - i. VMSB shall have self-test diagnostic feature to test for correct operation.
 - ii. Display driver boards shall test the status of all display cells in the sign even when diodes are not illuminated.
 - iii. All periodic self-test results shall be relayed to the ICCC in real time to update the status of the VMS

5.10. Environmental Management System

Functional Requirement of EMS

S.No.	Description
1.	Shall be ruggedized enough to be deployed in open air areas on streets and park
2.	Environmental Sensor station shall be housed in a compact environmentally rated outdoor enclosure. It shall be an integrated module which shall monitor overall ambient air, noise quality, weather etc.
3.	Mounting of the environmental sensor module shall be co-located on streetlight pole or shall be installed on a tripod/standalone pole.
4.	Environmental sensor station shall monitor following parameters and include the following integrated sensors inside one station: <ul style="list-style-type: none"> ▪ Carbon Monoxide (CO) sensor ▪ Ozone (O3) sensor ▪ Nitrogen Dioxide (NO2) sensor ▪ Sulphur Dioxide (SO2) sensor ▪ Carbon Dioxide (CO2) sensor ▪ Particulate/SPM Profile (PM10, PM2.5, and TSP) sensor ▪ Temperature sensor ▪ Relative Humidity sensor ▪ Wind Speed sensor ▪ Wind Direction sensor ▪ Rainfall sensor ▪ Barometric Pressure sensor; and ▪ Noise sensor.
5.	Solution shall display trends of environmental parameters based on user specific time periods.
6.	Data shall be collected in a software platform that allows third party software applications to read that data.
7.	Solution shall display real time and historical data in chart and table views for dashboard view of the Client.
8.	Alarms shall be generated for events where the environmental parameters breaches the safe or normal levels.
9.	The sensor management platform shall allow the configuration of the sensor to the network and also location details etc.
10	<ul style="list-style-type: none"> ▪ It shall comprise of an Industrial PC running latest version OS and compatible software. ▪ Data logging with central Monitoring System will be through GPRS/TCP-IP from all the AAQMS and MMS system and shall have an ability to program and log channels at different intervals and shall have a capability of averaging and displaying real time data and averaged data over a period of 1 min, 10 min, 30 min, 1 hr, 4 hr, 8, hr, 24 hr and so on. ▪ Real time or averaged data can be viewed quickly and easily through a remote interface on the central computer. ▪ System shall be able to perform nested calculations vector averaging and rolling averages. ▪ It shall have a feature for viewing instantaneous and historical data in the form of tables and graphs either locally or from a remote client.

S.No.	Description
	<ul style="list-style-type: none"> Data retrieval from CMS via USB and DVD shall be possible. Generation of reports for pollution load, wind rose etc. Alarm annunciation of analyzer/sensor in abnormal conditions.
11	<ul style="list-style-type: none"> The environment sensors shall be integrated with the command control system to capture and display/ provide feed. The data it collects is location-marked. Various environment sensors shall sense the prevailing environment conditions and send the data to the integrated control system where real time data resides and the same shall be made available to various other departments and applications for decision making. Information shall be relayed to signage – large, clear, digital-display screens which let citizens know regarding the prevalent environmental conditions. Further environmental sensors recorded data shall be used by Mobile application to enable user for alarm management and notification of environmental details on real time basis.

Technical Requirement of Environment Management Sensors

S.No.	Description
1.	Carbon Monoxide (CO) Sensor <ul style="list-style-type: none"> CO sensor shall measure the carbon monoxide in ambient air Range of CO sensor shall be between 0 to 1000 PPM Resolution of CO sensor shall be 0.001 PPM or better Lower detectable limit of CO sensor shall be 0.040 PPM or better Precision of CO sensor shall be less than 3% of reading or better Linearity of CO sensor shall be less than 1% of full scale or better Response time of CO sensor shall be less than 60 seconds Operating temperature of CO sensor shall be 0°C to 60°C Operating pressure of CO sensor shall be $\pm 10\%$.
2.	Ozone (O3) Sensor <ul style="list-style-type: none"> O3 Sensor shall measure the ozone in ambient air O3 Sensor shall have a range of at least 0-1000 PPB Resolution of O3 sensor shall be 0.001 PPM or better Lower detectable limit of O3 sensor shall be 0.001 PPM or better Precision of O3 sensor shall be less than 2% of reading or better Linearity of O3 sensor shall be less than 1% of full scale Response time of O3 sensor shall be less than 60 seconds Operating temperature of O3 sensor shall be 0°C to 60°C Operating pressure of O3 sensor shall be $\pm 10\%$
3.	Nitrogen Dioxide (NO2) Sensor <ul style="list-style-type: none"> NO2 Sensor shall measure the Nitrogen dioxide in ambient air NO2 Sensor shall have a range of at least 0-10 PPM Resolution of NO2 sensor shall be 0.001 PPM or better Lower detectable limit of NO2 sensor shall be 0.001 PPM or better Precision of NO2 sensor shall be less than 3% of reading or better Linearity of NO2 sensor shall be less than 1% of full scale Response time of NO2 sensor shall be less than 60 seconds Operating temperature of NO2 sensor shall be 0°C to 60°C Operating pressure of NO2 sensor shall be $\pm 10\%$

S.No.	Description
4.	Sulfur Dioxide (SO₂) Sensor <ul style="list-style-type: none"> SO₂ Sensor shall measure the Sulfur dioxide in ambient air SO₂ Sensor shall have a range of at least 0-20 PPM Resolution of SO₂ sensor shall be 0.001 PPM or better Lower detectable limit of SO₂ sensor shall be 0.009 PPM or better Precision of SO₂ sensor shall be less than 3% of reading or better Linearity of SO₂ sensor shall be less than 1% of full scale Response time of SO₂ sensor shall be less than 60 seconds Operating temperature of SO₂ sensor shall be 0°C to 60°C Operating pressure of SO₂ sensor shall be ±10%
5.	Carbon Dioxide (CO₂) Sensor <ul style="list-style-type: none"> CO₂ Sensor shall measure the carbon dioxide in ambient air CO₂ Sensor shall have a range of at least 0-5000 PPM Resolution of CO₂ sensor shall be 1 PPM or better Lower detectable limit of CO₂ sensor shall be 10 PPM or better Precision of CO₂ sensor shall be less than 3% of reading or better Linearity of CO₂ sensor shall be less than 2% of full scale Response time of CO₂ sensor shall be less than 60 seconds Operating temperature of CO₂ sensor shall be 0°C to 60°C Operating pressure of CO₂ sensor shall be ±10%
6.	Particulate Profile Sensor <ul style="list-style-type: none"> Particulate profile sensor shall provide simultaneous and continuous measurement of PM₁₀, PM_{2.5}, SPM and TSP (measurement of nuisance dust) in ambient air Range of PM_{2.5} shall be 0 to 230 micro gms / cu.m or better Range of PM₁₀ shall be 0 to 450 micro gms / cu.m or better Lower detectable limit of particulate profile sensor shall be less than 1 µg/m³ Accuracy of particulate profile sensor shall be <± (5 µg/m³ + 15% of reading) Flow rate shall be 1.0 LPM or better Operating temperature of the sensor shall be 0°C to 60°C Operating pressure of the sensor shall be ±10%
7.	Temperature Sensor <ul style="list-style-type: none"> Temperature sensor shall have the capability to display temperature in °Celsius Temperature range shall be -10° to +80°C Sensor accuracy shall be ±0.3°C (±0.5°F) or better Update interval shall be 10 to 12 seconds
8.	Relative Humidity Sensor <ul style="list-style-type: none"> Range of relative humidity sensor shall be 1 to 100% RH Resolution and units of relative humidity sensor shall be 1% or better Accuracy of the sensor shall be ±2% or better Update interval shall be less than 60 seconds Drift shall be less than 0.25% per year
9.	Wind Speed Sensor <ul style="list-style-type: none"> Wind speed sensor shall have the capability of displaying wind speed in km/h or knots Range of sensor shall be 0-60 m/s Accuracy of wind speed sensor shall be ±5% or better Update interval shall be less than 60 seconds
10.	Wind Direction Sensor

S.No.	Description
	<ul style="list-style-type: none"> Range of the wind direction sensor shall be 0° to 360° Display resolution shall be 16 points (22.5°) on compass rose, 1° in numeric display Accuracy shall be ±3% or better TR 6.70 Update interval shall be 2.5 to 3 seconds
11.	Rainfall Sensor <ul style="list-style-type: none"> Rainfall sensor shall the capability of displaying level of rainfall in inches and millimeter Daily Rainfall range shall be 0 to 99.99" (0 to 999.8 mm) Monthly/yearly/total rainfall range shall be 0 to 199" (0 to 6553 mm) Accuracy for rain rates shall be up to 4"/hr (100 mm/hr) or ±4% of total Update interval shall be less than 60 seconds 0.02" or (0.5mm) of rainfall shall be considered as a storm event with 24 hours without further accumulation shall end the storm event
12.	Barometric Pressure Sensor <ul style="list-style-type: none"> Barometric pressure sensor shall have the capability of displaying barometric pressure in Hg, mm Hg and hPa or mb Range of barometric pressure sensor shall be 540 hPa or mb to 1100 hPa or mb Elevation range of the barometric pressure sensor shall be -600 m to 4570 m Uncorrected reading accuracy shall be ±1.0 hPa or mb at room temperature or better Equation source of the sensor shall be Smithsonian Meteorological tables Equation accuracy shall be ±0.01" Hg (±0.3 mm Hg, ±0.3 hPa or mb) or better Elevation accuracy shall be ±10' (3m) to meet equation accuracy specification or better. Overall accuracy shall be ±0.03" Hg (±0.8 mm Hg, ±1.0 hPa or mb) or better. TR 6.85 Update interval shall be less than 60 seconds
13.	Noise Sensors <ul style="list-style-type: none"> Noise sensor shall detect the intensity of the ambient sound in a particular area Noise Sensors shall be installed for the outdoor applications Noise sensor shall be able to identify the areas of high sound intensity ranging from 30 dBA to 120 dBA Noise sensor shall have resolution of 0.1 dBA
14.	Integration with ICCS solution, VMSB, Portal and Mobile applications
15.	Conditions-Ruggedized enough to be deployed in open air areas on streets and park

5.11. Trenching using HDD/ Optical Fibre Cable

5.11.1. Specification of Permanently Lubricated HDPE Pipe

HDPE pipe shall be suitable for underground fibre optic cable installation by blowing as well as conventional pulling and should be free from the risk/damage caused by Rodents. The HDPE pipe shall be suitable for laying in trenches through RCC ducts.

Construction(Two layer)

The HDPE pipe shall have two concentric layers viz. outer layer and inner layer. The outer layer shall be made of HDPE material and the inner layer of solid permanent lubricant. These concentric layers shall be co-extruded and distinctively visible in cross-section under normal lighting conditions and generally conform to IS-9938. The

color of HDPE pipe shall be uniform throughout. In the finished HDPE pipe, the co-extruded inner layer of solid permanent lubricant shall be continuous and integral part with HDPE outer layer and preferably be white in color. The inner layer of solid permanent lubricant shall not come out during storage, usage and throughout the life of the pipe. The pipe shall be supplied in a continuous length of 1000 meter in coil form, suitable for transportation, installation and handling purposes.

Standards

The HDPE pipe shall conform to the following standard and the technical specifications described as under:-

- A. IS: 4984 - Specification for HDPE pipe.
- B. IS: 2530 - Method for tests for polyethylene moulding materials and compounds.
- C. IS: 9938 - Recommended colours for PVC insulation for LF wires and cables.
- D. TEC-spec no - HDPE pipe for use as duct for G/CDS-08/01 optical fibre cable.
- E. IS: 7328 - HDPE material for moulding and extrusion.
- F. ASTM D 1693 - Test method for environmental stress cracking of ethylene plastics.
- G. ASTMD 1505 - Test method for density.
- H. ASTMD 3895 - Method for Oxidation Induction test.

Material

The raw material used for the HDPE pipe shall meet the following requirements:-

- (i) the anti-oxidant establishes, colour master batch and other additive used shall be physiologically harmless and shall be used only to minimum extent necessary to meet the specification.
- (ii) Usage of any additives used separately or together should not impair the long-term physical and chemical properties of the HDPE pipe.
- (iii) Suitable Ultra-Violet stabilizers may be used for manufacture of the HDPE pipe to protect against UV degradation when stored in open for a minimum period of 8 months.
- (iv) The base HDPE resin used for manufacturing outer layer of pipe shall conform to any grade of IS-7328 or to any equivalent standard meeting the following requirement when tested as per standards referred in Clause 1.3.1 below.

Density 940 to 958 kg/m³ at 27o C

Melt Flow Rate 0.12 - 1.1g/10 minutes at 190oC & 5kg load

- (v) In case of HDPE pipe of two concentric layer construction, the friction reducing, polymeric material to be used as the inner layer lubrication material shall be integral with HDPE layer. The lubricant materials shall have no toxic or dramatic hazards for safe handling.

Tests on Material of HDPE pipe

- (i) Melt Flow Index and Density: The base HDPE resin material shall be tested for its melt flow index as per IS:2530 and density as per standard ASTM D 1505.

- (ii) Oxidant Induction Test: The oxidation induction test on base HDPE resin shall be conducted as per ASTM D 3895 and the oxidation induction time shall be ≥ 30 minutes.

Dimensions of HDPE Pipe with co-extruded copper wire shall be as under:

a) Outside diameter	:	50 mm +0.4 mm - 0.0 mm
b) Wall thickness	:	3.5 mm + 0.2 mm
c) Standard length	:	1000 + 100 metres
d) Copper Wire Diameter	:	1.22 mm +/- 0.02
e) Copper Wire Resistance	:	< 15.0 Ohms/Km. at 27 deg. C.
f) Web Strength	:	> 300 Kgs/10 cm
g) Web Thickness	:	> 1.5 mm
h) Thickness of Permanent Lubricant Layer	:	> 0.4 mm

Permanent Lubricated (Per Lub) HDPE Pipes should be sourced from the manufacturer with ISO 9000 accredited manufacturing facility. Per Lub HDPE Pipes should be sourced from the manufacturer having valid Type Approval Certificate from DOT as per the latest TEC Specs and its amendments thereof.

Accessories

The following accessories are required for jointing the pipe and shall be supplied along with the pipe. The manufactures shall provide complete design details, procedure for method of installation and type of the material used for the accessories.

- (i) Plastic coupler: The coupler shall be used to join two HDPE pipes. The coupling shall be able to provide a durable water tight joint between two pipes without deteriorating the strength of the pipes. The strength of coupler shall match the primary strength of the HDPE pipe. It should be push fit type. Threaded coupler is not acceptable. The jointing shall meet the air pressure test of 15 kg/cm² for a minimum period of 2 hours without any leakage.
- (ii) End plug: This shall be used for sealing the ends of empty pipe, prior to installation of FO cable and shall be fitted immediately after laying of the HDPE pipe, to prevent entry of any unwanted elements such as dirt, water, moisture, insects/rodents etc.
- (iii) Cable sealing plug: This is used to hold the cable and prevent entry of any unwanted elements, as specified above.
- (iv) End cap: This cap is made of hard rubber, shall be fitted with both ends of HDPE pipe to prevent the entry of any unwanted elements such as dirt, water, moisture, insects/rodents during transportation and storage.

OSP Fiber Optic Cable

The optical fiber proposed is an all Dielectric Gel-Free lightweight Single Mode as well as Multi-mode Fiber Optic cables designed for duct installation for backbone and access respectively. FOC shall provide full-spectrum availability for optical transmission systems operating over the entire wavelength range from 1260 nm to 1625 nm.

5.11.2. Technical Specifications of Single Mode Optical Fibre Cable

Cable Construction

Strength Member

The duct placement cables shall have a non-metallic central strength member covered by a suitable coating. The cable shall be designed with sufficient strength members to meet installation and service conditions so that the fibres are not subject to excessive strain.

Colour Coding

Loose tubes shall be individually coloured for ease of identification. Individual fibres shall also be colour coded. Fibre colours shall be as follows:-

Blue, orange, green, brown, grey, white, red, black, yellow, violet, pink, turquoise.

The tube colouring shall follow the same colour code. Fillers shall be of natural colour to fill up the cable core.

Cable Sheath Layers

The cable core shall be covered with a seamless black sheath mask of U.V. stabilised weather resistant polyethylene incorporating a moisture barrier (swellable components). The outer sheath excluding moisture barrier shall have a minimum thickness of 0.5 mm. The cable sheath shall be printed in yellow with a suitable legend to be agreed between the Contractor and the SALCAB Project Manager. The sheathing method including control measurements shall be fully described. In particular the cable diameter measurement, high voltage testing, printing and take-up on drum shall be described.

Table 5: Fiber Mechanical Characteristics

Fibre count	48	96
Fibre count in tube	4	12
Min. bending radius during installation (mm)	240	240
— installed (mm) Tensile load		
— Short term(N)	120	120
— Long term(N)	1500	1500
Crush load(N/10cm)	600	600
Applicable Temp. range — Operation	1000	1000
— Installation		
	-40~+70	-40~+70
	-20~+60	-20~+60

Table 6 : Fiber Parameters and Values

Parameters		Values
Mode Field Diameter	- range	9.2 +/- 0.4 μ m
	- deviation	+/- 10%
Attenuation	1285-1330nm1550nm	< / = 0.36 dB/km< / = 0.22dB/km
Attenuation Uniformity	Point or Step Defect Extended variations	< 0.1dB < 0.1dB
Temperature variation of attenuation from 0 Degree Celsius to 65 Degree Celsius	1300nm 1550 nm	< 0.05dB/km < 0.05dB/km
Dispersion	1285-1330 nm 1270-1340 nm 1550 nm	< 3.5 ps/nm.km < 6.0 ps/nm.km < 18 ps/nm.km
Mode cut off wavelength (of a primary coated fibre as Rec. G.652)		< / = 1260 nm
Reference surface diameter		125 +/- 0.7 μ m
Core / Cladding concentricity		< 0.6 μ m
Class non circularity (%)	Core Reference surface	<6 <2
Coating diameter		242 +/- 5 μ m
Proof test (%)		>1.0
Macro bend test (dB) 60mm diameter mandrel, 100 turns, loss increase at 1550nm		< 0.2

Splice Loss

The maximum acceptable splice loss is 0.15dB at 1500nm. The average splice loss taken in one direction on each route shall not exceed 0.1 dB at 1500nm.

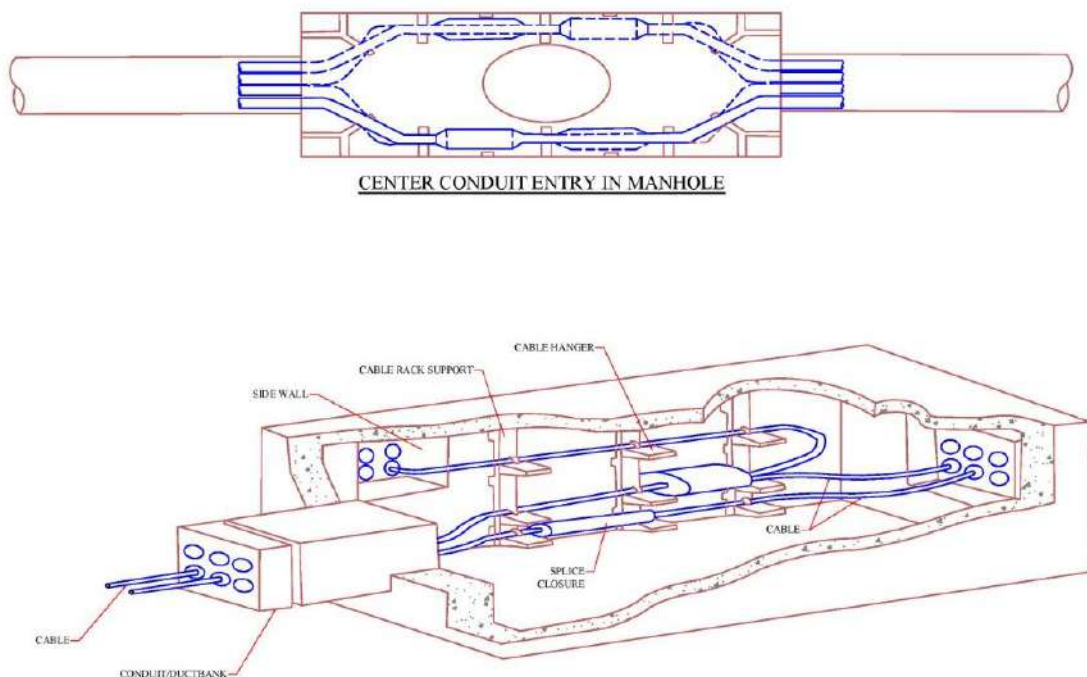
Splice/Joint closures and Manholes

Fiber joint closures or Splice closures are required to join sequential cable and fiber lengths together, or provide a function for distribution of smaller drop cables. The splice closures would be located based on the length of the fiber being supplied and the No. of cuts being envisaged during the span of next 20 yrs. Manholes provide accessible space in an outside plant pathway system for the pulling, placing, and splicing (Mid Span) of cables. Manholes are also used to segment the pathway system into lengths compatible with standard reel lengths for outside plant cable and to conform to maximum pathway lengths as defined in the TIA/EIA standards. Manholes would be placed at every 500 m distance.

Manholes should be constructed in such a way that they are capable of supporting the heaviest anticipated street traffic weight, even though all manholes should be located under the pavement. Include reasonable measures such as cable glands, rodent protection foams etc. for the purpose of water proofing and protection from pests. Provide sufficient cable supports or cable racks to be able to manage the maximum designed capacity of OFC.

Typical Manhole dimensions 1600(L)x1250(W)x1000(D)

Figure 6 : Typical Manhole Dimensions



Scope of Integration

MSI has to integrate all the existing and upcoming solutions available in city with respect to use cases through API and other method for seamless integration and the effective decision management perspective as mentioned below but not limited to:

- Smart Lighting
- ICT Enabled Solid Waste Management
- Intelligent Transportation System
- E-Challan System
- Public Bike Sharing
- Smart Education
- Smart Health Management System
- e-Municipality
- Smart Road Network
- eBuses Live Tracking and Monitoring System
- eToilet Monitoring System
- Environment Management System
- ICT component of eLibrary System
- ICT component of Smart Bus Stop System
- ICT component of Smart Parking System
- Any other upcoming solutions

District level ICCCs will be integrated with Patna ICCC for sharing the City Dashboard and major analytics. The Software for Integration would be centrally provided at PSCL and the same software would be utilized by the District level ICCCs. The MSIs of the District level ICCCs would coordinate with the MSI for Patna Smart City for proper utilization and implementation of the Software at their locations and also for seamless integration of all the ICCCs

6. SOW and Functional Requirement For Integrated Traffic Management System (ITMS) Components:

6.1. Adaptive Traffic Control System (ATCS)

6.1.1. Key Components of Adaptive Traffic Control System (ATCS)

6.1.1.1. Traffic Signal Controller

- i. The Traffic Signal Controller equipment is a 32 bit or 64 bit microcontroller with solidstate traffic signal lamp switching module with the ability to program any combination of traffic signal stages, phases and junction groups. The controller will ideally have a conflict monitoring facility to ensure that conflicting, dangerous are pre-flagged at the programming stage and these are disallowed even during manualoverride phase.
- ii. The Traffic Signal Controller will be adaptive so that it can be controlled through the central traffic control Centre as an individual junction or as part of group of

traffic junctions along a corridor or a region. The signal controller design must be flexible for the junction could be easily configured to be part of any corridor or group definition and could be changed through central command controller easily

- iii. Site specific configuration data shall be stored in a non-volatile memory device (FLASH memory) easily programmable at the site through keypad or laptop. A minimum of 512KB flash memory and 128KB RAM shall be provided. Volatile memory shall not be used for storing the junction specific plans or signal timings.
- iv. All timings generated within a traffic signal controller shall be digitally derived from a crystal clock which shall be accurate to plus or minus 100 milliseconds.
- v. The controller shall provide a real time clock (RTC) with battery backup that set and update the time, date and day of the week from the GPS. The RTC shall have minimum of 10 years battery backup with maximum time tolerance of +/- 2 sec per day.
- vi. The controller shall have the facility to update the RTC time from ATCS server, GPS and through manual entry.
- vii. The traffic signal system including controller shall have provision audio output tones and should be disabled friendly for.
- viii. The controller shall be capable of communicating with the ATCS server through Ethernet on a managed leased line network or any other appropriate stable communication network.

Traffic Signal Controller Operating Parameters

- i. Phases- The controller shall have facility to configure 32 Phases either for vehicular movement, filter green, indicative green, pedestrian movement or a combination thereof.
- ii. 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 timeout when operated with a vehicular phase.
- iii. The pedestrian phase signal shall be configured for flashing red or flashing green aspect during pedestrian clearance.
- iv. It shall be possible to configure any phase to the given lamp numbers at the site.
- v. Stages – The controller shall have facility to configure 32 Stages.
- vi. Cycle Plans – The controller shall have facility to configure 24 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 32 cycle-switching per day in fixed mode of operation.
- vii. Day Plans – The controller shall have facility to configure each day of the week with different day plans. 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 day plans.
- viii. Special Day Plans – The controller shall have facility to configure a minimum of 20 days as special days in a calendar year.

- ix. Starting Amber – During power up the controller shall initially execute the Flashing Amber / Flashing Red plan for a time period of 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.
- x. 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.
- xi. 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 pre-empt the Minimum Green once the stage start commencing execution.
- xii. 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 safety measure. The controller shall have programmability of 3 Seconds to 10 Seconds for All Red signal.
- xiii. Signal lamps monitoring – The controller shall have inbuilt circuitry to monitor the lamp status
- xiv. 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.
- xv. Cable less Synchronization – It shall be possible to synchronize the traffic signal controllers installed in a corridor in the following modes of operation, without physically linking them and without communication network. GPS enabled RTC shall be the reference for the cable less synchronization.
- xvi. Fixed Time mode with fixed offsets
- xvii. Vehicle Actuated mode with fixed offsets

Input and Output facilities

- i. Lamp Switching: The controller shall have maximum 64 individual output for signal lamp switching, configurable from 16 to 32 lamps. The signal lamps shall be operating on appropriate DC/AC voltage of applicable rating.
- ii. Detector Interface: A minimum of 16 vehicle detector inputs shall be available in the controller. All detector inputs shall be optically isolated and provided with LED indication for detection of vehicle.
- iii. Communication Interface: The traffic signal controller shall support Ethernet interface to communicate with the ATCS server
- iv. Power Saving: The traffic signal controller shall have a facility to regulate the intensity of signal lamps during different ambient light conditions thereby saving energy.
- v. Real-time Clock (RTC): The GPS receiver for updating time, date and day of the week information of the traffic signal controller should be an integral part of the traffic signal controller.

- vi. The traffic signal controller shall update the date, time and day of the week automatically from GPS during power ON and at scheduled intervals.
- vii. Manual entry for date, time and day of week shall be provisioned for setting the traffic signal controller RTC (Real Time Clock).
- viii. It shall be possible to set the RTC from the Central Server when networked
- ix. Keypad (optional): The traffic signal controller shall have a custom made keypad or should have provision for plan upload and download using PC/laptop/Central Server
- x. Operator Display (optional): The traffic signal controller shall optionally have a LED backlit Liquid Crystal Display (LCD) as the operator interface.

6.1.1.2. Countdown Timer:

It shall be installed at each traffic junction under ITMS & City Surveillance System Project.

- i. Count Down Timer to be configured in Vehicular Mode.
- ii. The Vehicular countdown timer should be dual
- iii. Color,; Red for Stop or STP and Green color for Go
- iv. There should be alternate Red and Balance phase time for STOP or STP in Flashing
- v. Alternate Green and Balance Phase Time for Go in Flashing

Technical requirement of Countdown Timer

S.No.	Description
1	CPU: Micro Controller
2	Mechanical Specifications
3	Structural Material Polycarbonate strengthened against UV rays
4	Body Color: Light Grey/Black
5	Dimensions: 360mm x 370mm x 220mm
6	Display Specification:
7	Lamp Diameter : 300mm
8	Digit Height: 150 -165mm
9	Display Type Dual Coloured (Red & Green)
10	No. of Digit 3
11	LED Specifications
12	LED Diameter : 5mm LED Viewing Angle 30° LED Wave Length 630-640nm (Red), 505nm - 520nm (Blue-Green) LED Dice Material AlInGaP (Red), InGaP (Blue-Green) LED Warranty period 5 years
13	Poles for Traffic Signals : Material: GI Class 'B' pipe
14	Paint: Pole painted with two coats of zinc chromate primer and two coats of golden yellow Asian apostolate paint or otherwise as required by architect and in addition bituminous painting for the bottom 1.5 m portion of pole.
15	No's of cores: 7 and 14 core 1.5 sq. mm.; 3 Core 2.5 sq. mm.
16	Materials: PVC insulated and PVC sheathed armoured cable with copper conductor of suitable size.

17	Certification: ISI Marked Standards: Indian Electricity Act and Rules IS:1554 - PVC insulated electric cables (heavy duty)
----	--

Communication Network

- i. Function of the Communication network is for remote monitoring of the intersection and its management. Real time data (like RTC time, stage timing, mode, events, etc.) from the traffic signal controller is required to be sent to the Central Computer in ICC. Central Computer running the ATCS application shall calculate and send optimum signal timings to all intersections in the corridor. SI shall clearly specify the bandwidth requirements and the type of network recommended for the ATCS.
- ii. The contractor shall specify the networking hardware requirements at the ICC and remote intersections for establishing the communication network.

Technical requirement of Field Junction Box

S.No.	Parameter	Minimum Specifications
1.	Size	Suitable size as per site requirements to house the field equipment
2.	Cabinet Material	Powder coated CRCA sheet/ Stainless steel
3.	Material Thickness	Min 1.2mm
4.	Number of Locks	Two
5.	Protection	IP55
6.	Mounting	On Camera Pole / Ground mounted on concrete base
7.	Form Factor	Rack Mount/DIN Rail
8.	Other Features	Rain Canopy, Cable entry with glands and Fans/any other accessories as required for operation of equipment's within junction box.

i. Junction Boxes

The junction box shall be fitted in secure locations (not easily accessible to the general public) and shall be fitted with a standard cabinet lock. Roadside cabinets shall be secured with anti-tamper fixings in addition to the standard cabinet lock.

- Each Junction box shall be fitted with sufficient screw type terminals to terminate all pairs used and unused. The terminal blocks shall be certified for use with the box.
- Each box shall be equipped with certified cable glands/plug and with earthing bar.

Cable continuity shall be through junction box dedicated terminals

6.1.2. ATCS application software requirement

Objective of the ATCS is 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 will be based up on assessments carried out by the ATCS application software running on a Central

S.No.	Description
1.	Identify the critical junction of a corridor or a region based on maximum traffic demand and saturation.
2.	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.
3.	Stage optimization to the best level of service shall be carried out based on the traffic demand.
4.	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.
5.	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.
6.	The system shall have provision to configure priority for upstream signals as default. The ATCS software shall continuously check the traffic demand for upstream and downstream traffic and automatically assign the priority route to the higher demand direction.
7.	Develop appropriate stage timing plans for each approach of every intersection under the ATCS, based on real time demand
8.	Propose timing plans to every intersection under the ATCS in every Cycle
9.	Verify the effectiveness of the proposed timing plans in every cycle
10.	Identify Priority routes
11.	Synchronize traffic in the Priority routes
12.	Manage and maintain communication with traffic signal controllers under ATCS
13.	Maintain database for time plan execution and system performance
14.	Maintain error logs and system logs
15.	Generate Reports on request
16.	Graphically present signal plan execution and traffic flow at the intersection on desktop
17.	Graphically present time-space diagram for selected corridors on desktop
18.	Graphically present network status on desktop
19.	Make available the network status and report viewing on Web
20.	The ATCS shall generate standard and customer ports for planning and analysis
21.	It shall be possible to interface the ATCS with popular microscopic traffic flow simulation software for pre and post implementation analysis and study of the proposed ATCS control strategy
22.	Shall have the ability to predict, forecast and smartly manage the traffic pattern across the signals over the next few minutes, hours or 3-5 days and just in the current real time.

23.	Shall provide a decision support tool for assessing strategies to minimize congestion, delays and emergency response time to events via simulation and planning tools linked with real time traffic data fusion and control of traffic signaling infrastructure on ground.
24.	Shall collect continuously information about current observed traffic conditions from a variety of data sources and of different kind (traffic states, signal states, vehicle trajectories, incidents, road works, etc.).
25.	Shall infer a coherent and comprehensive observed traffic state (speeds, vehicular densities, and presence of queues) on all network elements, from abovementioned observations, including vehicle trajectories, through a number of map matching, data validation, harmonization and fusion processes).
26.	Shall extend the measurements made on only a number of elements both on the rest of the unmonitored network, and over time, thus obtaining an estimation of the traffic state of the complete network and the evolution of this traffic state in the future.
27.	Shall forecast the traffic state with respect to current incidents and traffic management strategies (e.g. traffic signal control or variable message signs), improving the decision making capabilities of the operators even before problems occur.
28.	Shall calculate customizable Key Performance Indicators (KPI) to quickly assess the results
29.	Shall provide calculated traffic flows estimation and forecast, queues and delays to Urban Control and Adaptive Signal Control Systems, allowing for proactive Traffic Management and Control
30.	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)
31.	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”
32.	Shall create a traffic data warehouse for all historic traffic information gathered from the hardware installed on the road network.
33.	Shall operate in real time that is continuously updating the estimates on the state of the network and the travel times on the basis of data collected continuously over time.
34.	Shall operate the traffic lights with the adaptive traffic controls, based on the current and forecasted traffic demand and the current incidents, thus optimizing the green waves continuously throughout the network
35.	Enable a smart public transport priority respecting the delays for all road users at once with the adaptive signal controller
36.	Reports: Intersection based reports 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).

	<p>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.</p> <p>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.</p> <p>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.</p> <p>Mode switching report – The report shall give details of the mode switching taken place on a day.</p> <p>Event Report - The report shall show events generated by the controller with date and time of event.</p>
	<p>Power on & down: The report shall show time when the master is switched on, and last working time of the master controller.</p> <p>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.</p> <p>Plan Change – The report shall show the time of change of plan either through keypad or remotely through a PC or Server.</p> <p>RTC Failure – The report shall show the time when RTC battery level goes below the threshold value.</p> <p>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.</p> <p>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.</p> <p>Lamp Status Report – The report shall show lamp failure report with date and time of failure, color of the lamp and associated phase.</p> <p>Loop Failure Report – The report shall show the date and time of detector failure with detector number and associated phase.</p> <p>Conflict – The report shall show the conflict between lamps (RED, AMBER, GREEN) in the same phase or conflict between lamps with other phase.</p> <p>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</p> <p>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.</p>
37.	<p>Graphical User Interface - The application software shall have the following Graphical User Interface (GUI) for user friendliness.</p> <p>User login – Operator authentication shall be verified at this screen with login name and password</p>

	<p>Network Status Display – This online display shall indicate with appropriate color coding on site map whether an intersection under the ATCS is online or off. On double clicking the intersection a link shall be activated for the traffic flow display for the intersection.</p> <p>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.</p> <p>Saturation Snapshot – This display shall show the current saturation levels of all intersections in a corridor.</p> <p>Reports Printing / Viewing – This link shall allow selection, viewing and printing of different reports available under ATCS</p> <p>Time-Space Diagram – The time-space diagram shall display the current stages being executed at every intersection in a corridor with immediate previous history.</p> <p>Junctions shall be plotted proportional to their distance on Y-axis and time elapsed for the stage in seconds on X-axis.</p> <p>Junction names shall be identified with each plot.</p> <p>Facility shall be available to plot the time-space diagram from history.</p>
38.	<p>Currently running stage and completed stages shall be identified with different colors. Stages identified for synchronization shall be shown in a different color.</p> <p>Speed lines shall be plotted for stages identified for synchronization to the nearest intersection in both directions.</p> <p>It should be possible to freeze and resume online plotting of Time-Space diagram.</p> <p>The system shall have other graphical interfaces for configuring the ATCS, as appropriate.</p>

6.1.3. Detailed Specifications for Vehicle Detector Sensor

Sr. No	Description
1.	The vehicle detector should Forward firing technology multilane radar/video based technology with 4D object tracking with HD resolution. The sensor should be capable of working in fog, rain and without any requirement of cleaning and can provide precise information on counting , classification queue length for at least 175 meters for all stopped and moving vehicles..
2.	The sensor should have a detection range of 3m to 175 meters.
3.	The vehicle detector should have had a wide field of view of 40 degrees, and at the same time a range of up to 180m
4.	Vehicle detector should be multilane and should Detect up to 126 individual objects, and measure their position and speed
5.	The sensor should have radar/video based 4D object tracking and should measure (X, Y, Z) Cartesian coordinates or polar coordinates range, azimuth and elevation angle, as well as the speed vector simultaneously for up to 126 objects
6.	The radar/video based 4D with HD technology used should provide high-resolution capability in scenarios where many vehicles are closely spaced, i.e. in many lanes, dense traffic, traffic jams, stop and-go situations.
7.	One single sensor should allow up to 16 virtual loops and should have very high detection performance compared to video detectors.

8.	Vehicle detector should detect moving and stopped traffic i.e. Should detect vehicles, nomatter if stopped or moving. Up to 150km/h: no matter what traffic direction.
9.	Vehicle detector should not be affected by dirt, smog, sunlight, wind or sandstorms.
10.	IP67, from 0 °C to + 60 °C.
11.	The Vehicle detector should maintain high accuracy by means of built-in self-calibrationfunctions throughout the entire design life.
12.	It should have flexibility of installation on the roadside, at the corner of an intersection, at the median of a highway or on a gantry, with best results, not like side-firing technology, needingset-back from the road and having high occlusion risk
13.	It should have flexibility of installation on the roadside, at the corner of an intersection, at the median of a highway or on a gantry, with best results, not like side-firing technology, needingset-back from the road and having high occlusion risk
14.	The sensor should have wide field of view -20° to+20° Azimuth and the long range (175m) toallow the user to define at least 16, up So that vehicles are tracked over a longer period when they drive in the field of view to avoid occlusion.

6.2. Automatic Number Plate Recognition (ANPR) System

Overview

The ANPR System shall enable monitoring of vehicles at entry/exit locations. The system shall support real-time detection of vehicles at the deployed locations, recording each vehicle, reading its number plate, database look up 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. System should have following functional requirements:

Vehicle Detection and Video Capture Module

- The System should automatically detect a vehicle in the camera view using video detection and activate license plate recognition
- The System shall automatically detect the license plate in the captured video feed in real-time.
- The system shall perform OCR (optical character recognition) of the license plate characters (English alpha-numeric characters in standard fonts).
- The System shall store JPEG image of vehicle and license plate and enter the license plate number into DBMS like MySQL, PostgreSQL etc. database along with date timestamp and site location details.
- System should be able to detect and recognize the English alpha numeric License plate in standard fonts and formats of all four wheelers including cars, HCV, and LCV.
- The system shall be robust to variation in License Plates in terms of font, size, contrast and color and should work with good accuracy
- The system shall be robust to variation in License Plates in terms of font, size, contrast

and color and should work with good accuracy.

Vehicle Detection by Color

- The system shall detect the color of all vehicles on best effort basis, in the camera view during daytime and label them as per the predefined list of configured system colors. The system will store the color information of each vehicle along with the license plate information for each transaction in the database.
- The system shall have options to search historical records for post event analysis by the vehicle color or the vehicle color with license plate and date time combinations.

Hot listing and Alert Generation

- The system should have option to input certain license plates according to the hot listed categories like “Wanted”, “Suspicious”, “Stolen”, etc. by authorized personnel.
- 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.

Vehicle Status Alarm Module

- 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).
- The Instantaneous and automatic generation of alarms. In case of identity of vehicle in any category which is define by user.

Vehicle Log Module

- The system shall enable easy and quick retrieval of snapshots, video and other data for post incident analysis and investigations.
- The system should be able to generate suitable MIS reports that will provide meaningful data to concerned authorities and facilitate optimum utilization of resources. These reports shall include.
- Report of vehicle flow at each of the installed locations for Last Day, Last Week and Last Month.
- Report of vehicles in the detected categories at each of the installed locations for Last Day, Last Week and Last Month.
- Report of Vehicle Status change in different Vehicle Categories.
- 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.
- 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.

- 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).

Vehicle Category Editor

- The system should have option to input certain license plates according to category like "Wanted", "Suspicious", "Stolen", and "Expired" etc. by Authorized personnel.
- The system should have an option to add new category by authorized personnel.
- 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".
- System should have option to specify maximum time to retain vehicle records in specific categories.

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 look up 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. System should have following functional requirements:

Scope of Work

- a. System should have following components and capable of doing following:
 - i. Ability to have IR illuminators to provide illumination for night-time scenario.
 - ii. Ability to provide the live feed of the camera at the integrated command control center or as per user requirement.
 - iii. Ability to provide video clips of the transaction from the ANPR lane cameras as evidence.
 - iv. Ability to detect the color of all vehicles in the camera view during daytime. The system can store the color information of each vehicle along with the license plate information for each transaction in the database.
 - v. Ability to search historical records for post event analysis by the vehicle color or the vehicle color with license plate and date time combinations.
 - vi. Ability to input certain license plates according to the hot listed categories like "Wanted", "Suspicious", "Stolen", etc. by authorized personnel.
 - vii. Ability 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.
 - viii. Ability to generate automatic alarm to alert the control room on successful recognition of the number plate based on pre-defined rules.
 - ix. Ability to easy and quick retrieval of snapshots, video and other data for post incident analysis and investigations.
 - x. Ability to generate MIS reports to concerned authorities and facilitate optimum utilization of resources. These reports shall include but not limited to:

- Report of vehicle flow at each of the installed locations for Last Day, Last Weekend Last Month.
 - Report of vehicles in the detected categories at each of the installed locations for Last Day, Last Week and Last Month.
 - Report of Vehicle Status change in different Vehicle Categories.
- xi. Ability to search the information based on parameters defined.
 - xii. Ability to auto generate reports and send to stakeholders.
 - xiii. Ability to define system access based on rule.
 - xiv. ANPR System should function in centralized architecture on GPU based servers in Data Center.
 - xv. Operating system: The system must be based on open platform and should run on LINUX/Windows Operating system.
 - xvi. The system should be capable of generating a video & minimum 5 snapshot 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).
 - xvii. The system should perform ANPR on all the vehicles passing the site and send alert to the ICCV on detection of any Hot-listed.
 - xviii. With the detected number plate text, picture should also be sent of hot listed vehicle. It is highly likely to misread similar alphabets like 7/1/L or 8/B.
 - xix. The system should have ANPR/ OCR to address the Alpha numerical character of irregular font sizes.
 - xx. Vehicle number detection is to be made possible on the ANPR cameras.
 - xxi. The complete tracking of the vehicle is to be made possible on the GIS map to locate any suspicious / identified vehicle.
 - xxii. The identified or suspicious vehicle may be flagged by any police personnel or sensed by ANPR or through other analytics like vehicle tracking based on color & shape of the vehicle.

6.3. Traffic Violations and Enforcement System

Scope of Work

The following to be automatically detected by the system by using appropriate Non-Intrusive sensors technology:

The system should be capable to detect red light status by taking the signal feed from the traffic signal controller or video evidence shall be created for Red light violation / analytics method using RLVD / Overview focused at the red light. Over all solution should be able to provide features and capable to fulfil the following requirements:

The camera should also be capable with Automatic Number Plate Recognition (ANPR) technology and used for evidence snap generation.

- RedLight Violation Detection (RLVD)

- Speed Violation Detection (SVD)
- No Helmet Violation detection (NHVD)
- Free Left violation detection (FLVD)
- Triple riding violation detection (TRVD)
- Vehicle Wrong Direction detection (VWDD)

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:

- Type of Violation
- Date, time, Site Name and Location of the Infraction
- Registration Number of the vehicle through ANPR
- Camera system for each vehicle identified for infraction

Red Light Violation System

- a) System should have the facility to provide the live feed of the camera at the central command centre. System should generate Alarms at control room software if any signal is found not turning RED within a specific duration of time. The following Traffic violations to be automatically detected by the system by using appropriate technology. The Evidence camera should also be used for evidence snap generation minimum for Red Light Violation, Stop Line Violation, Wrong left turn violation, Wrong direction driving violation.
- 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 Type of Violation, Date, time, Site Name and Location of the Infraction, Registration Number of the vehicle through ANPR Camera system for each vehicle identified for infraction.
- c) 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 : When it violates the stop line and When it violates the red signal.
- d) The system must 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 encrypted. 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.
- e) 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.

Speed Violation Detection System :

- a. The nonintrusive system shall be capable of measuring speed of vehicles and capture over speed vehicles. The Speed measurement should support multiple methods for calculation of speed – either Average or Instantaneous Speed Measurement methods.
- b. The system shall have the provision of setting different speed thresholds for different class of vehicles.
- c. The speed violations system should be installed on mid-blocks or designated areas as identified during design stage.

Wrong Direction Vehicle Movement

- a. The non-intrusive system should be installed at critical junctions to capture the wrong direction vehicle movement. The system should identify and capture multiple IVD. The e- Challan standard procedure should be triggered.
- b. Recording & display information : The recording and display of information should be detailed on the snapshot of the infracting vehicle as follows:
 - i. Computer generated unique ID of each violation
 - ii. Date (DD/MM/YYYY)
 - iii. Time (HH:MM:SS)
 - iv. Equipment ID
 - v. Location ID
 - vi. Carriageway or direction of violating vehicle
 - vii. Type of Violation (Signal/Stop Line)
 - viii. Lane Number of violating vehicle
 - ix. Time into Red/Green/Amber
 - x. Registration Number of violating vehicle
- c. Detection of triple riding on two wheelers. The system should be capable of detection of 2 wheeler driver with triple riding / pillion riding
- c. Detection of No Helmet on two wheelers. The system should be capable of detection of 2 wheeler driver not wearing helmet

RLVD Application

- a) 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 programme should allow for viewing, sorting,

- transfer& printing of violation data.
- 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.
 - c) Violation retrieval could be sorted by date, time, location and vehicle registration number and the data structure should be compatible with PSCL Police database structure. It should also be possible to carry out recursive search and wild card search.
 - d) 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).
 - e) The application software should be integrated with the e-Challan/Vahan 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 MSI.
 - f) 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.
 - g) 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 as per requirement.
- The system should be capable of generating a video & minimum 3 snapshot 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).
 - Digital Network Camera: As per specified in Surveillance Camera Section.

6.4. Automated e-Challan System

Modules for e-Challan Software

- i. Photo Collection
- ii. Violation booking
- iii. e-challan Generation
- iv. Postal dispatches
- v. Postal Statement
- vi. Postal returns and return info feeding
- vii. Data entry in vehicle Registration. remarks database
- viii. Provision to enter comment Sold out vehicles/Fake vehicles /Fake addressed
- ix. Vehicles/Theft Vehicles/Authorized complaints/Multiple owners)
- x. Identification of Police Stations, Junctions, Courts, Police Staff for the Traffic dept
- xi. MV Act cases
- xii. ID ,Address& contact details fields addition

- xiii. Action dropouts as per Court decisions
- xiv. Report Generation
- xv. Online Pending Challan Verification
- xvi. Online Violation photo view facilities
- xvii. Upgrading the E-challan Software
- xviii. Online Uploading photos by the Police in Control room

6.5. Traffic Accident Reporting System (TARS)

- a) TARS solution should provide:
 - a. Accident reporting system
 - b. Accident recording system
 - c. Analysis of accidents
 - d. Dissemination of data
- b) Solution shall provide accident database that will support collecting high quality information on all aspects of road traffic collisions and incorporate best practices of RoadAccident Investigation.
- c) Solution shall support authorities in quickly and accurately reconstructing collisions and analysing the data to develop standards to prevent future collisions or mitigate injuries.
- d) Solution shall support information gathering and dissemination as per various stakeholder requirements for accident data, namely, PSCL, police, decision makers etc.
- e) Information to be captured shall include, but not limited to:
 - a. how the accident happened,
 - b. detailed information about the vehicle(s) involved
 - c. type and extent of human impact
 - d. human factors involved (inebriation, etc.)
 - e. nature of any injuries,
 - f. type and extent of property damage,
 - g. socio-economic data of the people involved,
 - h. primary & secondary causes of the accident
 - i. incident photos
 - j. drawing of accident analysis
 - k. information on analysing agency and personnel

6.6. Traffic Sensors Lights and Signals

- Appropriate camera based traffic sensors may be chosen to provide the operational levels and accuracy as required for successful function of the ATCS system as per the SLAs defined.
- Appropriate controller technology may be chosen to provide the operational levels

and accuracy as required for successful function of the ATCS system as per the SLAs defined. The proposed traffic controller shall be disabled friendly and shall also provide audio tones output

- **Traffic Lights: Key Features:**

- a. lowest power consumption for all colors
- b. Meets or exceeds intensity, color and uniformity specifications
- c. Temperature compensated power supplies for longer LED life
- d. Uniform appearance light diffusing
- e. Should be Intertek/ETL/EN certified
- f. LED shall be single source narrow beam type with clear lens & Luminance uniformity of 1:15
- g. Pedestrian traffic lights should be provided with clearly audible signals for the benefit of pedestrians with visual impairments
- h. Phantom Class 5 or equivalent. IP Rating: IP65
- i. LED aspects:
- j. Red, Amber, Green-Full (300 mm diameter) : Hi Flux
- k. Green-arrow (300 mm diameter): Hi flux
- l. Animated Pedestrian-Red and Green Animated c/w countdown (300 mm) Hi Brite with diffusions
- m. LED Retrofit Specifications:
- n. Power supply: Redundant
- o. Standards: EN 12368 certified
- p. Convex Tinted Lens: Available
- q. Fuse and Transients: Available
- r. Operating Temperature Range: 0 degree Celsius to 55 degree Celsius Turn Off/Turn On Time: 75 milliseconds max
- s. Total Harmonic Distortion: <20%
- t. Electromagnetic interference: Meets FCC Title 47, Subpart B, Section 15 Regulation or equivalent EN/IRC standard
- u. Blowing Rain/Dust Spec: MIL 810F or Equivalent EN/IRC standard complaint
- v. Minimum Luminous Intensity (measured at intensity point)(cd):
 - i. Red 400
 - ii. Amber 400
 - iii. Green 400
 - iv. Dominant Wavelength (nm):
 - v. Red 630
 - vi. Amber 590
 - vii. Green 490

- Lamp conflict compatibility system: Compatible with lamp failure and conflict detection

7. CCTV Surveillance System

7.1. Scope of Work

SI has to supply, install, commission and maintain the required number of camera in the location as mentioned in Annexure. SI has to provision for poles, switch, UPS and other equipment for installing the camera. The SI should do necessary cabling for electrical supply and connectivity required for the field devices. SI will also implement the following software to enable monitoring through the surveillance cameras. To facilitate the VMS system architecture, the SI shall ensure that sufficient capacity is designed into the data communications & telecommunications infrastructure to deliver the required functionality, along with the ability to allocate and reserve resources (including bandwidth). Video Management System (VMS) and Video Analytics System.

General specifications of all type of cameras are as below:

- a. All the network cameras supplied must be certified for: FCC ,CE and UL (Certificates to be enclosed)
- b. All cameras should have feature for Bandwidth Compensation & Optimization, it should also support 3rd Party Analytics, with continuous Learning
- c. Ability to support use of HTTPS and SSL/TLS, providing the ability to upload signed certificate to encrypt and secure authentication and communication of both administration data and video streams.
- d. The Camera shall support IEEE 802.1X authentication, Password protection, IP address filtering, HTTPS encryption, Digest authentication, User access log, Centralized certificate management
- e. Ability to support open and published API
- f. Programmers Interface shall provide necessary information for integration of functionality into third party applications. It should have standard components and proven technology using open and published protocols and adopt to industry established standards.
- g. The implemented API shall be standardized and supported by all network video products offered by the various manufacturers.
- h. Ability to provide 24/7/365 availability and use.
- i. All the major components of the CCTV systems shall be latest but field-proven and shall not be End-of-Life / Outdated; the same shall have to be supported by concerned OEM for at-least 5 years' period from the date of supply.
- j. All the cameras shall have 5 Years OEM warranty and the same shall be submitted on OEM letter head.
- k. OEM of CCTV should be registered in India for last 5 years directly and not through distributor or Joint Venture. Proof of the same should be attached with the Technical bid.
- l. OEM of CCTV shall have local support centre.
- m. All the cameras shall have ability to change the GOP/ GOV for Bit rate optimization.

- n. VMS should have ability to select user defined shape for motion detection to include or exclude area to reduce false alarms, bandwidth and storage.
- o. All cameras shall have ability to send and receive triggers to perform any action without intervention of VMS.

7.2. Overview

City Safety and Security solution helps protect cities against crime, terrorism, and civil unrest, planning events, monitoring of infrastructure, encroachments etc. It helps law enforcement monitor public areas, analyze patterns, and track incidents and suspects enabling quicker response. Keeping the above perspective, PSCL for this purpose is intending to implement the high definition IP based surveillance cameras across various locations within PSCL. The exact location will be finalized after detailed survey, post award of the contract. The cameras should be housed on the intelligent/street poles. It shall also be possible to adjust the camera focus from a remote location.

Following is an indicative scope of work;

- a) Installation and commissioning work includes installation of all required, cameras, monitors, networking, cables laid in PVC conduit etc., commissioning all the systems at the pre-defined locations in the project area
- b) The SI shall prepare the final camera distribution plan at all the camera locations in discussion with PSCL
- c) Actual location for placement of pole & number of cameras at each location, type of cameras, fixation of height & angle for the cameras would be done carefully to ensure optimum coverage
- d) SI should use the industry best practices while positioning and mounting the cameras. Some of the check-points which need to be adhered by the SI while installing / commissioning cameras are as follows:
 - i. Ensure Project objectives are met while positioning the cameras, creating the required field of view
 - ii. Ensure appropriate housing is provided to protect camera from the on field challenges
 - iii. Carry out proper adjustments to have the best possible image
 - iv. Ensure that the pole /tower/ mast implementation is vibration resistant
- e) SI shall undertake detail assessment for integration of the Surveillance System with the Geographical Information System (GIS) so that physical location of cameras are brought out on the GIS map. SI is required to carry out the seamless integration to ensure ease of use of GIS in the Surveillance System Applications/ Dashboards in Command Control Centres. GIS Base Map shall be supplied and integrated by the SI at 1:1000 scale or better with all surveillance cameras located on the map apart from the updated map of all buildings, utilities and roads. Field survey needs to be done by the SI. SI is required to update GIS maps from time to time. GIS data need to be created that supports rule based model on industry standards such as Topology, Spatial connectivity rules, relationship, GIS layer domains and subtypes, GIS Geometric network, industry specific editing rules and future scalability. SI is suggested to visit government departments for review and better understanding of available data with them.
- f) SI shall carry out SMS Gateway Integration with the Surveillance System and develop necessary applications to send mass SMS to groups/individuals, which can be either manual or system generated. Any external/third party SMS gateway can be used, but this needs to be specified in the Technical Bid.

- g) SI will have to identify and obtain necessary legal / statutory clearances for erecting the poles and installing cameras, for provisioning of the required power, etc. the same will be facilitated by PSCL. It is important to mention that a timely communication and required follow-up will be required by the SI for the clearances.
- During implementation period, in case the pole is damaged by a vehicular accident (or due to any other reason outside the control of SI) and needs repair, then the SI will need to repair/ have the new pole within 15 days of the incident. Damages are to be borne by SIs in suchcases through proper insurance.
- i) For the successful commissioning &operation of the edge devices and to provide the video feeds to Command Control Centre, the SI will be required to provide electricity to the edgedevices through the aggregation points. SI has to plan the power backup based upon the power situation across the city. SI may propose solar based powering systems however fielddevices shall be operational 24x7 and power needs to be calculated accordingly.
- j) SI will be responsible for the solution deployment / customization for implementing end-to-end Surveillance System including its integration with other components as required.
- k) SI will ensure that the best practices for software development and customization are usedduring the software development/customization and implementation exercise.

7.3. Functional and Technical Requirements for VMS

Sr. No.	Technical Specification for Video Management System
	VMS General Requirements
1.0	The VMS application must seamlessly Integrate with the ICCC platform.
1.1	The VMS shall be based on a true open enterprise architecture that shall allow the use of non-proprietary workstation and server hardware, non-proprietary network infrastructure and non-proprietary storage. The VMS application provider must support any ONVIF compliant Camera and the list of integrations must be listed on the global web site of the application provider.
1.2	The VMS shall integrate cameras using dedicated driver or using the industry standards ONVIF Profile S and Profile G. The same must be listed on the ONVIF website.
1.3	The Security application shall offer a complete and scalable video surveillance solution which allows cameras to be added on a unit-by-unit basis. The database shall support more than 50000 cameras / IP end points in a single / multiple clusters of DB Hardware machine..
1.4	The Proposed VMS Solution Shall support native Fail over with in application with no dependency on any external application for both hardware and application redundancy. The native fail over architecture must be for both management and recording servers.

1.5	The Fail over and Fall-back management and recording Server shall be on hot standby, ready to take over during the primary management server fails. No manual action from the user shall be required. The fail over time should not be beyond 1 Min and there should not be any loss in the Live video and recorded video.
1.6	The Standby VMS server shall support disaster recovery scenarios where a server can be in another geographic area (or building) and only take over if Primary server become offline. Both Primary DC and Secondary DC must be based on a single instance Active – Passive architecture.
1.7	The Standby Server shall support real-time synchronization of the configuration databases for high reliability.
1.8	The Application shall offer a plug and play type hardware discovery service with the following functionalities:
1.9	Automatically discover Video surveillance units as they are attached to the network.
1.10	Discover Surveillance units on different network segments, including the Internet, and across routers with or without network address translation (NAT) capabilities.
1.11	The Application shall have the capacity to configure the key frame interval (I-frame) in seconds or number of frames.
1.12	The Application shall allow for multiple recording schedules to be assigned to a single camera.
1.13	The Application shall support Direct Multicast from Camera. For network topologies that restrict the Application from sending multicast streams, the application shall redirect audio/video streams to active viewing clients on the network using multicast directly from cameras and the architecture should not use Multicast streaming via recording servers or any other servers and increase the overall compute capacity of Recording servers.
1.14	The Application shall allow important video sequences to be protected against normal disk clean-up routines.
1.15	The application shall have the following options when protecting a video sequence: Until a specified date, for a specified number of days, indefinitely (until the protection is explicitly removed for evidence).
1.17	The proposed software shall be scalable / future ready to support live viewing and automatic transfer of video recorded to the cloud on demand basis from UC&C user interface, based on the age of the video for future scalability and

	the hosted Cloud Platform must be among the approved vendors as per the MeiTY approved GI Cloud initiative from Govt of India..
1.18	The Application shall be capable to handle both IP v4 and IP v6 Unicast and Multicast traffic with both PIM – SM and PIM – DM support.
1.19	The application management server should not have any limitation on the no of recording servers added on one single management / fail over server. Any limitations must be clearly specified by the organization.
1.20	There should not be any dependency on the end point MAC address for licensing for ease of operations.
1.21	VMS Software must be capable and certified to run on Physical or Virtualized Environment
1.22	The VMS Platform must have the capability to real time and scheduled backup video/ Flagged and critical data to Near DR Servers/Storage
1.23	The VMS platform must have the flexibility to deploy rules for storing and avoiding data deletion of the flagged data, critical data, & Incident reports based on the criticality of the data.
2.0	Client Interface
2.1	The Monitoring UI shall support the role of a Unified Security Interface that can monitor various Video events and alarms, as well as view live and recorded video.
2.3	The system shall have a single API interface for sending Analytics event alerts and other Maintenance Alerts over HTTP protocol to external systems such as Command and Control Application
2.4	The Client Viewer shall allow digital zooming on live view as well as on replay view on Fixed as well as PTZ Cameras.
2.5	The Client Viewer shall support the use of standard PTZ controller or 3-axis USB joysticks for control of pan, tilt, zoom and auxiliary camera functions.
2.6	The Client Viewer shall have the capability to receive multicast streams if a pre-set number of clients are requesting the same live view camera. The system shall have the capability to detect if the network becomes unreliable and to automatically switch to unicast to ensure that the operator is able to receive video.
2.11	User workspace customization:
2.12	The user shall have full control over the user workspace through a variety of user-selectable customization options. Administrators shall also be able to

	limit what users and operators can modify in their workspace through privileges.
2.13	Once customized, the user shall be able to save his or her workspace.
2.14	The user workspace shall be accessible by a specific user from any client application on the network.
2.15	Display tile patterns shall be customizable.
2.16	Event or alarm lists shall span anywhere from a portion of the screen up to the entire screen and shall be resizable by the user. The length of event or alarm lists shall be user-defined. Scroll bars shall enable the user to navigate through lengthy lists of events and alarms.
2.17	The Monitoring UI shall support multiple display tile patterns (e.g. 1 display tile (1x1 matrix), 16 tiles (8x8 matrix), and multiple additional variations).
2.18	Additional customization options include: show/hide window panes, show/hide menus/toolbars, show/hide overlaid information on video, resize different window panes, and choice of tile display pattern on a per task basis.
2.19	The Monitoring UI shall provide an interface to support the following tasks and activities common to Various systems
2.20	Monitoring the events from a live security system
2.21	Generating reports.
2.22	Monitoring and acknowledging alarms.
2.23	Creating and editing incidents and generating incident reports.
2.24	Displaying dynamic graphical maps and floor plans as well as executing actions from dynamic graphical maps and floor plans Unified with UC&C.
2.25	The live video viewing capabilities of the Monitoring UI shall include:
2.27	The ability to drag and drop a camera into a display tile for live viewing.
2.28	The ability to drag and drop a camera from a map into a display tile for live viewing.
2.29	Support for digital zoom on live camera video streams.
2.30	The ability for audio communication with video units with audio input and output.
2.31	The ability to control pan-tilt-zoom, iris, focus, and Presets.

2.32	The ability to bookmark important events for later retrieval on any archiving camera and to uniquely name each bookmark in order to facilitate future searches.
2.34	The ability to activate or de-activate viewing of all system events as they occur.
2.35	The ability to switch to instant replay of the video for any archiving camera with the simple click of button.
2.36	The ability to take snapshots of live video and be able to save or print the snapshots.
2.37	The ability to browse through a list of all bookmarks created on the system and select any bookmarked event for viewing.
2.38	Tools for exporting video and a self-contained video player on various media such as USB keys, CD/DVD-ROM and Proposed Evidence management and Collaboration system. This video player shall be easy to use without training and shall still support reviewing video metadata.
2.39	Tools for exporting video sequences in standard video formats, such as ASF, MP4 and any other open standard video format
2.41	The ability to encrypt exported video files with industry standard encryption.
2.42	A tool building and exporting a set of videos into a single container. This tool shall allow the operator to build sequences of video to create a storyboard and allow the export of synchronous cameras.
3.0	Cyber Security Requirements:
3.1	The VMS shall support only secured media stream requests, unless explicitly configured otherwise. Secured media stream requests shall be secured with strong certificate-based authentication leveraging RTSPS (aka RTSP over TLS). Client authentication for media stream requests is claims-based and may use a limited lifetime security token.
3.2	The VMS shall offer the ability to encrypt the media stream, including video, audio, and metadata with authenticated encryption. Media stream encryption shall be done at rest and in transit and be a certificate-based AES 128-bit encryption / Digital Signatures.
3.3	The VMS shall allow encryption to be set on a per camera basis for all or some of the cameras.
3.4	Provide up to 20 different certificates for different groups of users who have been granted access to decrypted streams.

3.5	Use Secure RTP (SRTP) to encrypt the payload of a media stream in transit and allow multicast and unicast of the encrypted stream.
3.6	Use a random encryption key and change periodically.
3.7	Allow encrypted streams to be exported.
3.8	The VMS shall support end to end encrypted streams with cameras supporting Secure RTP (SRTP) both in unicast and multicast from the camera.
3.9	The Application shall support digitally sign recorded video using 128-bit RSA public/private key cryptography / Digital Signatures.
3.10	The Application shall protect archived audio/video files and the system database against network access and non-administrative user access.
3.11	Media encryption shall support with latest industry standards – AES-128 / Digital Signatures.
3.12	The application must support encryptions / watermarking at the rest and not only on the exported videos footage
3.13	The proposed VMS platform must have international recognized certifications to prove the Cybersecurity standards adaption. Organizations to submit the certifications along with the technical bid. Bidders to submit the certifications along with the technical bid. VAPT / Encryption / security certificates from CERT-IN empanelled auditors should be acceptable.
3.14	User Authentication support:
3.15	The system shall support logon using the user name and password credentials shall allow distributed viewing of multiple cameras on the system on any monitor.
3.16	System shall be integrated with dual factor authentication using LDAP/ AD for User authentication.
3.17	The system shall include flexible access rights and allow each user to be assigned several roles where each shall define access rights to cameras.
3.18	The System shall provide a feature-rich administration client for system configuration and day to- day administration of the system.
4.1	The VMS shall support mobile apps for various off-the-shelf devices. The mobile apps shall communicate with the Mobile Server of the VMS over any Wi-Fi or cellular network connection.
4.2	All communication between the mobile apps and central server shall be based on standard TCP/IP protocol and shall use the TLS encryption with digital certificates to secure the communication channel.

4.3	<p>Functionalities:</p> <p>Core</p> <p>a. The mobile app should a COTS based app from the VMS provider being made available from the day 1 and must be easily be downloadable from IOS and Android stores online.</p> <p>b. Ability to display a geographic map with VMS entities geo-located on the map.</p> <p>c. Ability to view any camera configured on the map.</p> <p>d. Ability to search cameras or location on the map.</p> <p>e. Ability to view live and recorded video from the cameras of the central recording server.</p> <p>f. Ability to display live and recorded video side-by-side for a specific camera.</p> <p>g. Ability to perform digital zoom on cameras.</p> <p>h. Ability to perform actions on cameras such as add a bookmark, control a PTZ, control the iris/focus function, save a snapshot, start/stop recording.</p> <p>i. Ability to use the camera of the smartphone and stream a live video feed to a video recorder in the system.</p> <p>j. Ability to locate the mobile app user on map and provisioning to message and collaborate in real time with the central command center or field staff.</p>
4.4	It shall be possible to extend the widgets of a dashboard using the API / SDK / or any appropriate interfaace for this purpose.
4.5	The VMS shall support the following actions on a dashboard: print dashboard, export dashboard to PNG, JPEG, BMP etc file format, and automatically email a report based on a schedule and a list of one or more recipients/ users/ user groups.
4.6	<p>The VMS shall support the following operations:</p> <ul style="list-style-type: none"> • Adding an IP device • Updating an IP device • Updating basic device parameters • Adding/removing channels • Adding/removing output signals • Updating an IP channel

	<ul style="list-style-type: none"> • Removing an IP device • Enabling/disabling an IP channel • Refreshing an IP device (in case of firmware upgrade) • Multicast at multiple aggregation points
5	Community Surveillance Module:
.1	<p>Architecture overview:</p> <p>a. The feeds city wide Surveillance system and feeds from Community surveillance (Invested by Public property owners in the premises) shall also be viewed at the Command and Control Center through the UC&C platform.</p> <p>b. It is envisaged that about 2500 cameras from community surveillance feeds would be extended from various Police Area Offices, Railway Offices, SP-Offices police stations across the city of Patna.</p> <p>c. The feeds from Community surveillance cameras could be fed into city UC & C platform through below 3 means and the solution must be ready to consume all the format of feeds and provide native intelligence within the UC & C platform –</p> <p>i. Through LAN / WAN from each community operator or a set of community operators to the nearest police station of each Police Area Offices, Railway Offices, SP-Offices and further federated to the Command & Control UC & C platform. The solution must be capable of viewing the streams both at the local police station levels or Viewing centers or other Police Area Offices, Railway Offices, SP-Offices police stations and Command centers.</p> <p>ii. Community surveillance camera connected via Public cloud network and further connected to the Command center UC & C platform.</p>
5.2	<p>The UC & C and VMS module must be flexible to adapt all the possible architectures outlined above and the operators must get a unified view of the CCTV feeds irrespective of the architecture through which the community camera feeds are extended to Police network.</p>

7.4. Video Analytics Software for 1000 Cameras with average 2 use cases per camera

The followings are the AI based Video Analytis (nnot limited to) considering a smart City Scenarios

Violence & Violent Behaviour Activity:

- The human fighting.
- The human firing a weapon.
- The human throwing the stone.

- Person Tracking.

Women Safety Behaviour Activity:

- The women / person in distress raising his/her hand(s) for HELP.
- Chain / Mobile / Purse snatching
- The human lies or falls on the ground
- The human abandons an object.

Grouping Behaviour Activity:

- The Human or Humans group running.
- Humans Gathering in a group.
- Violation of Section 144 as per IPC

Vehicle Behaviour Activity:

- Vehicle Collision (such as Car, Bus, Truck, Motorcycle etc.)
- Vehicle Park on sidewalks or at no-parking areas. (Illegal Parking)

Other Activities

- Any kind of fire or smoke detection on the streets.
- Person Collapsing
- Crowd Estimation and management
- Camera Health Monitoring
- Abandoned Object Detection
- Advanced Intrusion Detection

7.5. Functional & Technical Requirements for Facial Recognition System

Sr. No	Key	ITEM DESCRIPTION
	Detection	Face Recognition System shall work on real time and offline mode for identifying or verifying a person from various kinds of inputs from digital image file and live video source from any IP video streaming sensor like IP Camera, Body Worn Cameras, Mobile handset cameras.
	Deep Learning Technology	FRS must be a latest generation Convolutional Neural Networks based facial and person tracking technology with Real-time 1:1 (one to one), 1: N (one to many) and N:N (many to many) matching.
	Live and Offline Mode	FRS shall be able to capture face images from live & pre-recorded CCTV feeds received and generate alerts if a blacklist (face from suspect list) match is found.

	Detections in crowd	The system shall be able work to detect more than 20 faces in crowd on moderate face rotation either horizontal or vertical. It should support a yaw angle of -40 to +40 degrees , a pitch angle of -30 to +30 degrees and a roll angle of -30 to +30 degrees.
	Detection of partial faces	The FRS shall recognize partial faces with varying angles from multiple videos simultaneously from Video clips, Group Photographs and VMS Playback directly from FRS Client Interface.
	Ability to add reference Images	The system shall be able to add photographs obtained from law enforcement agencies to the criminals' repositories tagged for sex, age, etc. for future searches.
	Support for cameras/video formats	<p>The system shall support diverse graphic & video formats as well as live cameras. FRS shall support day/night operation with ability to detect faces both in colour and in black/white mode by using any H.264, H.265 Fixed IP Cameras with / without IR Illuminators.</p> <p>Bidder to ensure the identified cameras for FRS purpose are mounted and configured as per the splution design in order to achieve the desired results and accuracy</p>
	User-management	FRS must support a user management module that enables different user level groups to support various permission levels.
		FRS client shall have ability to share recognition data like images & videos with multiple users and operators for better reference, alarm & incident management.
	Image Enhancement Capabilities	FRS system must have capability to enroll whatever images fed in the system with image enhancement and ability to verify the quality of the enrolled images with different colour indicator for low quality images enrolled in watchlist/database.
	Image Format support	The system shall be able to utilize any of the file formats like JPEG, PNG, BMP, TIFF etc. format for enrolment.

	De-duplication	FRS shall be able to check if new enrolled face is already enrolled in the database before registering the new enrolled face in the system. Also, the system shall be able to find a previous detection of a POI (person of interest) upon enrolment to watchlist (retrospective search) in less than 5 sec.
	Enrolment of faces	<p>The system shall have option to automatically enroll face images from CCTV cameras/video source.</p> <p>The system should also have an option for Bulk Enrollment either from file system or a 3rd party databases such as UID, SAARTHI, IT, NCRB, EPIC etc.</p> <p>The end user shall provide required interface with such Govt databases for integration purpose to the qualified bidder.</p>
	Categories of database faces	The system shall have capacity to create different categories of people with option to customize the matching threshold for different categories.
	Full HD Support	The system shall be able to work on full HD Camera video with maximum performance.
	Implementation	The system shall be able to be implemented on IT hardware like Server or Workstation.
	OS Support	The FRS algorithm should be able to use proven open source tools and technologies like Linux to bring down the total cost of ownership of the solution. FRS running on any other OS should be supplied with Pre-Licensed Server based latest version OS like Microsoft Server 2016 and Microsoft SQL as needed by the application
	Database Support	The system shall employ database system like MS SQL/ MYQL/ Leading Open Source Database/Sybase/ Mongo DB/ Postgres/Oracle etc. The FRS system should natively integrate with Video Intelligence platform and use a common database of the platform, so that common queries can be made on the common database for faces detection and other events.

	Algorithm Benchmarking	The Vendor should have any performance benchmarking certificate. NIST certificate will be preferred.
	Performance	The system must perform a full 1: N search of the probe image in under 5 seconds against a database of up to 1 mn face records.
	Mobile Application Support	FRS Software vendor shall have mobile application of the same FRS software to support iOS and android based smart field devices. Mobile application shall be capturing the face of suspect in field and sending back to the FRS server for matching. Matching result shall be shown on the mobile application screen with matching score. There shall be provision in mobile application to stream mobile device camera as video streamer.
	Detection robustness	System shall be able to detect the faces across the multiple CCTV video sources for online (real-time) and offline modes regardless of following conditions:
		a. Changes in Facial expression
		b. Changes in facial hair or hairstyle
		c. Changes by moderate aging (up to 15 years)
		d. Partially hidden faces or occluded faces like wearing dark glasses mask etc.
		e. Changes in lighting conditions
	Search Capabilities	Simple Search UI that facilitates quick and easy access to the collection of events recorded by the system without the constant monitoring by operators and must perform a full 1: N search of the probe image in under 5 seconds against a database of up to 5-8 Million POIs. It shall support following
		a. Search previous events by images from previous detections
		b. Search previous events by images uploaded by operator
		c. Search previous events by enrolled names
		d. Search previous events by date and time

		e. Search previous events by watchlist group
		f. Search in Watchlist by image
	Retrospective Search	FRS shall have capability of Search backwards for previous detections and/or recognitions (events) of the detected person without enrolment from live CCTV & other forensic videos / offline videos
	Upto 5 nearest matches support	FRS shall have ranking features to show next 5 closest & similar subjects in the Watchlist with nearest score to the detection. This option enables you to review POIs that are potential matches for this detection for efficient system performance.
	OEM owned algorithm	The FRS OEM should have ownership of Face Recognition Engine /Algorithm for any custom specific development as required by client
	Map feature	FRS must allow tracking of person on maps to be uploaded in the system for cameras connected to FRS and shall highlight the camera location on the map for each detection/alert.
	SDK/API for integration	FRS shall provide an SDK/API for integration with any third-party software like ICCC Command & Control Centre. API must be available with a full set of documentation of each method with accompanying sample code. All FRS function shall be fully accessible via API.
	Timeline of detections	FRS shall provide timeline sequence of all detections of subject with date, time & location.
	Email Integration	FRS shall support email Alerts via Gmail, Outlook or via an Exchange SMTP service. Different recipients can be defined for different Camera Groups. User shall be able to define how frequently recognition/detection emails are sent, the email subject and the email sender (among other things). The email itself includes the timestamp of the detection, the score, the description, the reference image (defined in the Watchlist) and the detected image.

Use of AI accelerator hardware	FRS shall use extensive AI Technology and perform video processing on GPUs like NVIDIA; INTEL or similar as per design & sizing vetted by AI FRS Algorithm OEM. The number of servers to be supplied, shall be based on the number of camera channels on which the FRS needs to be performed as per OEM design considerations.
---------------------------------------	--

Face Recognition System KPI Criteria/Evaluation Parameters:

Sr. No.	Aspect
2	Measuring following KPI (Key Performance Indicators) Detection Rate Number of True Positives Number of False Positives Number of True Negatives Number of False Negatives All vendors will be provided with a live stream with similar Field of View to ensure common ground along with suspects who can be enrolled. Above outcomes will be measured and compared among all vendors to check the accuracy.
3	Simultaneous detection of multiple faces in crowd: All vendors will be provided with a crowded video and outcomes will be recorded.
4	Deep Learning based algorithm: All vendors will have to demonstrate learning capabilities within their algorithm.
5	Global Threshold, Camera wise threshold and watchlist wise threshold
6	Real Time back search for newly enrolled subjects
7	Video & Image evidence of suspects
8	Easy Monitoring of System Health
9	Multiple detections to be collated using intuitive methods
10	Privacy as per GDPR compliance
11	Integration with leading VMS vendors
12	Integration with any sensor

7.6. Video Summarization Functional & Technical Specification:

Sr. No.	Specification of Video Summarization
1.	Video Summarization System (VSS) shall be a truly open platform that can rapidly transforms video into actionable intelligence and improves safety, security, and operational efficiencies also if required can interfaced with any existing or new ONVIF complied VMS system selected by the customer.
2.	System to make available live & recorded video surveillance feeds searchable, quantifiable, and actionable. The VSS shall be based on computer vision and AI (Artificial Intelligence) technology enabling rapid video review, search, quantitative video insights, and smart alerting, thereby shortening time-to-target to detect and mitigate security threats and enhancing safety and operational optimization significantly. The VSS system shall enable the generation of usable metadata from recorded offline-video files and online VMS platforms with full case management, multi-camera search, appearance similarity.
3.	System shall facilitate leveraging of quantitative video analysis-derived intelligence for informed, data-driven decision-making, including advanced trend and dimensional (area, path, duration, and other) KPI analysis as well as full dashboarding and scheduling capabilities.
4.	System shall be able to enhance safety and security with quick rapid human response to critical events recorded on video
5.	shall automatically extract all the moving objects (People/Vehicle/Animal) from the original video and without alerting the original image/video/data, simultaneously displaying events that have occurred at different times.
6.	System shall also able to pinpoint people of interest using digital images extracted from video or external sources, either by a specific person image selected or per watchlist.
7.	shall rapidly pinpoint people and vehicles of interest, using a range of appearance and movement filters, across video feeds from multiple cameras.
8.	System shall show the timestamp at which a specific object appeared in the video. This timestamp shall be visible on the image of that specific subject / object
9.	System shall be able to link together in a chain of separate video clips into a single video. All the video data shall be stored in a database for easy and quick review by operators.
10.	System shall allow the user to bookmark any event clip for ready reference at any later point of time also it shall allow the user to tag critical Event clips so that they do not get removed from the storage based on retention period settings.

11.	Shall provide a web-browser (Preferably Google Chrome) interface to upload the video files, generate the Summarization & for the management of multiple investigation cases
12.	System shall have a centralized single web-based administration module to view and activate cameras, configure hosts and any other related services.
13.	System shall be able to reduce bottlenecks by configuring people counting alerts for the selected spaces by the operator and can monitor and identify potential crowding and react preventively and proactively to mitigate risks by sending personnel to redirect traffic to other walkways or access points
14.	Time Range - Limit the search criteria to specific time ranges
15.	Source – Shall be able to limit the objects to specific CCTV Camera feed or offline pre-recorded multiple video files
16.	Classes – Post-analysis, reviewed video shall be shown based on People, Two-Wheeled Vehicles, Other Vehicles with the following categories: i. People Class: Man, Woman, child etc. ii. 2-Wheeled Vehicle Class: Bicycle, Motorcycle etc. iii. Other Vehicles Class: Car, Pickup, Van, Truck, Bus, etc. iv. Capturing license plates of Vehicles appeared in the video feeds.
17.	People Attributes – Shall be able to select the attributes within the people class to refine the search Like: i. Count : Total count of people in a pre-defined range of view or area. ii. Bags: Backpacks, Handheld Bags iii. Hats: Hats, No Hats iv. Upper Wear: Short/No Sleeves, Long Sleeves v. Lower Wear: Long, Short vi. Colour - Identify objects according to any combination of various colors like Yellow, Brown, Red, Orange, Green, Lime, Grey, Black, Cyan, Purple, Pink and White. vii. Faces of appeared people in the input video feeds.
18.	Size -Select objects based on their actual (real-life) size specified in meters.
19.	Speed - Select objects based on their actual speed specified in KMPH.
20.	Dwell - Select objects dwelling for longer than a certain period in a scene
21.	Area - Identify objects included or excluded within one or more user-defined 3- or 4-sided polygon areas. The user shall be able to set the minimum duration the object spends inside the area.

22.	Path - Identify objects traveling along one or more user-defined paths. The user shall be able to set the minimum duration the object spends inside the area.
23.	Supported Video Resolution – Minimum CIF and Maximum 4K
24.	Shall be able to results dwell time, changes to scene background; and path lines for object travel, apply visual layers and heat maps to identify the movement of objects/subjects depending upon the global filters subject to the situation.
25.	Supported Frame Rate – 8-30 FPS
26.	Shall support different video file formats & codecs: AVI, MKV, MPEG4, MOV, WMV, DVR, ASF, RT4, DIVX, 264, GE5, TS, 3GP, DAV, XBA, MP4, FLV, H.264, H.265/HEVC, MPEG-4, and H.263.
27.	System shall have mobile application, which runs on both Android and iOS devices which derives exponential value from surveillance camera investments by making video searchable on-the-go. It shall have on the move Access to Processing servers to achieve unmatched accuracy and seamless extensibility.
28.	System shall provide an OPEN API to interface any third-party systems (such as APP or QRT systems) without any additional cost to the customer.
29.	System shall also comply with PUBLIC HEALTH REGULATIONS of best practices and operating protocols, from barring travel to and from certain regions to minimizing gatherings over a certain number of participants.
30.	System shall be able to identify the CROWDING HOTSPOTS AND TRENDS by utilizing dashboards to visually represent object movement, behavior trending, hotspots, and object interactions.
31.	System shall be customizable to meet the specific needs and operational processes of a given user environment and to support unique requirements specific to forensic search and alert response.

7.7. Picture Intelligence Unit- Functional Requirement & Technical specification

Sr.no	Specification
	Picture Intelligence Unit

A	<p>This is envisaged to be a video forensic unit/ R&D Setup for Intelligent Analysis Centre.</p> <p>The PICTURE INTELLIGENCE UNIT (PIU) shall provide assistance to curb crime in the city as it will send real-time alerts generated by the connected sub-systems on the match of any desired subject or object based on the face, number plate, or the physical appearance.</p> <p>It will use live camera feeds, criminal and crime scene photographs/ videos etc. as support analysis to evidence and enable faster action and response by police forces.</p> <p>It will ensure video analytics, continuous time stamp and non-tampering of electronic evidence as per laws.</p>
	<p>Picture Intelligence Unit (PIU) shall be given secure access to the databases of Passport, CCTNS, Prisons, AMBIS or any similar database available with the State Government and Central Government and should be periodically updated with hotlists into respective sub-systems.</p> <p>The PIU system shall make use of standard data security and encryption technology to secure communication & exchanged data while interfacing respective databases, sub-systems, and users should not be affected by any cyber-attack</p> <p>It shall also have facility to create a repository of photographs obtained from various police sources like Newspapers, Photos during raids, Photos sent by people, etc. Such photographs would be tagged for sex, age, , etc. so that these become searchable.</p> <p>The PIU shall be able to connect, search, correlate & consolidate all connected data sub-systems (FRS, ANPR, VIDEO ANALYTICS, VIDEO SUMMARIZATION SOFTWARE, etc.</p> <p>Some of the approaches to be used by the Picture Intelligence Unit for implementation of Facial Recognition System would be as follows:</p>
1	Match a suspect/criminal photograph with these databases.
2	Search photographs from the database meeting certain suspect features.
3	Match a suspected Criminal face with Video Feeds of specific camera locations or with the feed received from private or other public organization's video feeds with last recorded location highlighted

	<p>Whenever there is a requirement at any of the Police team to check the identity of an individual, Police Station would make such a request to PIU, who in turn would search the databases available with it to match the individual. Such databases would either be accessed through web services or in a downloaded manner. Full audit trail of reports and data provided will be maintained.</p> <p>The PIU shall maintain audit logs of all data exchange, activities, requests, and responses related to databases, sub-systems, users, etc.</p> <p>The PIU shall have a unified dashboard to show the list of total requests made by users, request in process, request completed (user found the data), request in which matched data not found, requests for manual intervene & requests approved for providing video clip, etc.</p>
4	<p>PIU would also be able to interface with information from third parties — for example, banks, telecom companies, credit companies, etc. PIU shall also liaison with other institutes & agencies doing R&D work on Facial Recognition & related technologies. It is expected that the Systems Integrator look at this Picture Intelligence Unit as a Research & Development Center to test the best and latest technologies and ensure its continuous enhancement. SI is required to analyse the futuristic requirements for the effective functioning of PIU and propose tools like Data mining (application of statistical techniques and programmatic algorithms to discover previously unnoticed relationships within the data). SI needs to propose one of the most advanced (+ tried & tested in India) Facial Recognition System.</p>
5	<p>. SI needs to customise the application to the local conditions & carry out continuous enhancements during operational phase.</p>
6	<p>PIU shall oversee the integration of ANPR with the other relevant databases. Further the PIU shall also evaluate the use of various emerging technologies and their features such as Video Analysis Module to complete a historical analysis of person or object for review over a period of time</p>
	<p>The PIU system shall make use of standard data security and encryption technology to secure communication & exchanged data while interfacing respective databases, sub-systems, and users should not be affected by any cyber-attack</p>
	<p>The PIU shall help to discover the unnoticed relationship within the subjects and objects from the available data.</p>
	<p>The PIU shall allow creating of users or user groups and allow role-based access to them also the administrator shall be able to modify, customize, or create varying levels of permissions and pre-emption rules for each role.</p>
	<p>Experts in PIU Team</p>

	SI has to provide adequate team to operationalize PIU and train the Police Personnel to make optimum utilization of the same. Minimum requirement of the team to be proposed by SI for PIU is as follows:
1	01 Facial Recognition Analyst (with min. 1 year of relevant experience)
2	01 video Analytic Analyst (with min. 1 year of experience in video analytics (other than facial recognition))
3	01 IT Forensic Expert (with min. 2 years of experience in IT Forensic). Forensic Experts shall be responsible for preparing the incriminating video clips and shall also certify its integrity & chain of custody.
4	The above experts would be deployed for a period of 2 years, from the starting of PIU of the project. It may also be required from time to time for these experts to depose in the court of law. These experts will analyse the incriminating video footage and certify its integrity & chain of custody. These experts shall oversee the integration of ANPR with the other relevant databases and also undertake R&D to evaluate and analyse various analytics-related technologies and their implementation during the project period. All the necessary software, tools required for undertaking this activity should be provided by the bidder.
	Publishing of Guideline Documents by PIU
	PIU shall be responsible for preparing various guideline documents/manuals for the appropriate use of video data and for uniform operationalization of Surveillance systems across the city at different private/public institutions. An indicative list of such guideline documents / manuals to be prepared by the PIU is given below:
1	Guideline document/manual to standardize file Formats, compression types, interfaces, to be used by various agencies (such as Fire Dept., Ambulance Dept., Other Public Institutions, Pvt. Institutions, etc.) concerned with video / photograph recording & storage.
2	Guidelines for video data handling for submission of the video data to judiciary as legal evidence.
3	Guideline document / manual for setting up of Video Surveillance System by Private and Public institutions within the city.

	<p>Functional Requirement</p> <p>Picture Intelligence Unit (PIU) will maintain all Audit Trails and logs of all instances, triggers and incidental data derived out of VA platform, FRS Engine, ANPR Engine and the activities governed by the VMS. PIU will not replicate the incidental data however, will keep the track record of all such activities as a common directory which provide convenience during post investigation analyses.</p> <p>Picture Intelligence Unit (PIU) shall be given access to the databases of Passport, CCTNS, Prisons, AMBIS or open source databases or any similar database available with the State Government and Central Government. It shall also create a repository of photographs obtained from various police sources like Newspapers, Photos during raids, Photos sent by people, etc. Such photographs would be tagged for sex, age, etc. so that these become searchable. Some of the approaches to be used by the Picture Intelligence Unit for implementation of Facial Recognition System would be as follows:</p> <ol style="list-style-type: none"> Match a suspect/criminal photograph with these databases. Search photographs from the database meeting certain suspect features. Match a suspected Criminal face with Video Feeds of specific camera locations or with the feed received from private or other public organization’s video feeds. Whenever there is a requirement at any of the Police team to check the identity of an individual, Police Station would make such a request to PIU, who in turn would search the databases available with it to match the individual. Such databases would either be accessed through web services or in a downloaded manner. Full audit trail of reports and data provided will be maintained. PIU would also try to access information from third parties — for example, banks, telecom companies, credit companies, etc. PIU shall also liaison with other institutes & agencies doing R&D work on Facial Recognition & related technologies. It is expected that the Systems Integrator look at this Picture Intelligence Unit as a Research & Development Centre to test the best and latest technologies and ensure its continuous enhancement. SI is required to analyze the futuristic requirements for the effective functioning of PIU and propose tools like Data mining (application of statistical techniques and programmatic algorithms to discover previously unnoticed relationships within the data). Using the Key UI and integration capabilities of the Video intelligence platform, PIU shall oversee the integration of ANPR with the other relevant databases
--	---

7.8. AI with continuous Learning & Improvement System - Functional Requirement & Technical specification

S.no	Parameter	Specifications
------	-----------	----------------

1	Advanced AI compatible	The system shall be an AI/Deep-learning based Behavioral understanding systems for Real-Time video intelligence in the most dynamic and challenging urban environment on a 24x7 basis.
2	Training new models	The system shall be futuristic and keep improvising its accuracy on the existing behavior of diverse objects, and allow it to add more behaviors in the upcoming versions.
3	Annotation	<p>The system shall have an inbuilt annotation tool that allows a user to label the images with relevant information using both rectangle and polygon drawing facilities.</p> <p>The annotation should allow labeling of images or drawn objects with different class names. In case of persons, it should also support labeling of various attributes such as color of clothing, type of clothing, age, gender etc. as well.</p> <p>The user-interface should allow to plug-in the trained model in any of the relevant Video Analytics use-cases dynamically at each camera.</p> <p>The system should allow the user to plug newly trained AI models at runtime by simply selecting the models in the per-camera configuration page</p>
4	Model Comparison	The System shall have a library of standardized AI models developed by the OEM of the Video Analytics System. These models shall be used for comparing and benchmarking the performance of newly developed models. The system shall allow for both qualitative and quantitative comparison of models, i.e. it shall allow the end user to compare individual parameters of the model (such as learning rate) as well as the overall performance of the model on any given dataset when compared to a standardized model.
5	Monitoring and analytics	Autonomously objective metrics shall be available to be evaluated and Insights into the performance of each algorithm, model and their versions shall be made available to key stakeholders or users as defined. Visual map of composition, workflow, usage analytics, resource utilization, failure points etc. would be made available to provide complete control of A.I. workload.
6	Supervised deep learning methods	The system shall be automated and does not require typical rule or filter drawings to detect any interest in alarm.
7	Self-learning Capabilities	The system shall apply holistic and temporal analysis for scene participants through a top-down approach (scene -> event(s) -> action(s) -> object(s) -> attribute(s) by using the time dimension to connect between the video's image sequence and the different modalities.

8	Terminology	The system shall detect objects, actions, events, and scenes where the size of the participating objects is at least 10% of the frame. The objects and behaviors should not be obscured.
9	Applying Multiple Activity Rules	The system shall allow applying multiple or all behaviors on a camera or a set of behaviors on the camera group using a simple user interface also shall detect any changed behaviors within 03 seconds in front of the camera once the datasets are fully trained.
10	Key UI View and functionalities	The System shall provide the following key results from the use case
		Event Notifications: The result of each of the use case shall be in the form of events that contain the screenshot with other metadata describing the event, such as detected objects, timestamp, camera/video that generated the event and all other metadata representing the event from different use cases. The User Interface shall have a grid and list view with all the events from different use cases, cameras etc. These features should be supported through a mobile application to be utilized by various field users. The system should support customization of alerts, video feeds, and priority-based alerts for individual users from day one.
		Resource Management View: The User interface shall provide a list of all the resources available in the system such as computing servers and cameras. The status of each of the devices, whether they are online/offline shall also be available at all times.
		AI Training Tool: The User interface shall have a training tool to annotate and label images from the events to train new AI models and update the existing ones. The training tools shall also contain a list of all the models available in the system, which can be plugged into any AI use case easily.
		Use case deployment matrix: The user interface shall have a matrix to assign, start, stop and schedule any use case on any camera. The status of active and non-active use cases shall be clearly visible with colour coded information. All the licenses should be able to operate in floating mode for all cameras.
		Data Analytics Dashboard: The user interface shall also have an analytics dashboard listing all the patterns of events from different cameras with a heat-map of number of events on an hourly basis.
		The user interface shall be a unified dashboard that shows events from all the Video Analytics use-cases and all the cameras in a common UI, and which gets populated in real time from event notifications.

		The User interface of the system shall be a web interface that can be accessed from any system in the local area network with login credentials. It shall allow multiple users to log in at the same time, and receive real-time alerts and notifications.
11	Common UI for all the use-cases	The system shall be seamlessly integrated with the proposed VMS and showcase the generated metadata on the live & playback video stream.
12	Web based Interface	The system shall allow each use-case to be uniquely configured for every individual camera stream, with parameters for camera calibration, image quality improvement, night/day settings etc.
13	Live Video Interface	Each use-case shall be able to run on different cameras with different settings (e.g., different Zones for Intrusion, different lines for line crossing detection, etc.) at different hours of the day.
14	Configuration per-use-case per-camera level	The configuration page shall allow a user to choose any of the available AI models to detect and classify objects within the image. The description of the models shall clearly specify performance and hardware requirements of each of the model.
		The system shall be ready to deploy and does not require any additional camera calibration.
		The use case on each camera shall allow setting up configuration of multiple detections zones such as lines and regions that can be used to define perimeters, regions of interest.
15	Camera Calibration Tool	The configuration user interface shall allow adjusting various sensitivity and confidence parameters to adjust each video-analytics use-case's performance with respect to the physical deployment of the camera.
16	Key configuration parameters	The system shall allow a user to filter and retrieve all the events based on any combination of the following parameters: <ul style="list-style-type: none"> - Time of the event - Objects in the event - Type of the use-case - Camera Location etc.
		The architecture shall clearly demonstrate the technology stack with layers of the core platform, data governance and interface to different software applications.
17	Filtering and Retrieval	The system must have a consolidated alert dashboard where each alarm type can be accompanied by a video snippet in a form of different color codes.

18	Transparent and Open Architecture	The system shall support user with a hierarchical access level, with different access level for different users demarcated with respect to cameras, locations and the data. The user access control system shall allow setting of SOP's like CRUD (Create, Read, Update and Delete) operations for each user.
19	Highly parallel and distributed	The system shall allow deployment of any use case on any camera without any MAC level or IP level locking. Ideally any use case shall be deployable and redeploy able on any camera or video source as far as the camera view supports such use cases to be deployed.
20	User Management	The System shall be a real-time video analytics engine that utilizes advanced image processing algorithms to turn video into actionable intelligence. The AI based Video Analytics system shall consists of video-processing & analytics engine that works seamlessly both on saved videos or camera streams in real-time and provide events to the user based on the use-case basis. The system shall be compatible with all ONVIF compliant IP cameras with H.264/H.265 video decoding.
21	Deployment of use-case across any camera	All the video streams shall be processed centrally at the data centre with one or more servers for video processing. The user shall be able to log in to the system through the central dashboard to access all the data from all the servers. The processing of videos as well as alert generation shall be done on premise. At no point in time shall the data from the site be shared over the internet or sent over to the cloud. The System UI shall only be accessible using workstations and terminals available on premises.
22	Video Compatibility	The AI system shall also support third-party developed algorithms and use-cases that can provide the user with a large base of use-cases to choose from.
23	Centralized Deployment Support	If a new use-case needs to be developed based on Video Intelligence, the system shall provide a developer API / Software Development Kit (SDK) for this purpose. The API / SDK shall be provided along with detailed documentation for building end-to-end use-cases on the system.
24	Support for third-party use-cases	The system shall also allow the user to plug different AI models in the individual running of the video analytics use-case.
		The technology stack shall be modular and scalable based on containerized micro services. Each use-case shall be orchestrated as a stand-alone micro service, which communicates with a central server for exchanging of the data.
		A.I. micro services components shall be agnostic to language used in technology stack. It shall work with any language, framework, and library of choice without any impact on the rest of the architecture.

		This type of flexibility will ensure lower friction for collaboration and deployment of AI.
25	Flexible Technology Stack	Algorithms being containerized shall ensure both interoperability and portability, allowing for code to be written in any programming language or any version of library and framework but then seamlessly exposes a single API to be integrated and ported with multiple modules/AI components of diverse stack. It shall seamlessly integrate with other components and shall be portable/ replicable easily across the machines automatically.
		The Video Analytics shall be based upon Machine Learning and Deep Learning framework.
		To save the duplication of the video storage, the analytics should flag the video for the configurable duration of time pre and post event in the Video Management System. It should be possible for the operator to jump to the alert flag in the archived video for detailed investigation of the event.

7.9. Functional & Technical Requirements for Outdoor Fixed Cameras/Bullet/Dome(HD)

S.No	Features	Specifications
1.	Form Factor	Box Type / Bullet Camera
2.	Image Sensor	1/2.8" Progressive CMOS or better
3.	Day/NightvOperation	ICR with IR range of 100m or better
4.	Minimum Illumination	Color 0.10 lux , B/W 0.0005 lux
5.	Lens	Motorised Lens (5 mm to 50 mm / 12 mm to 40 mm or better) or as per field requirement to achieve the required FoV
6.	Electronic Shutter	1 ~ 1/10000 sec.
7.	Image Resolution	1920X1080 @ 30 fps (2MP)or better
8.	Compression	MJPEG, H.265,H.264 or better
9.	Frame Rate and Resolution	Full HD (2MP 1920x1080 or better) @ 25/30 FPS
10	Simultaneous Stream	Minimum 3 streams should be configurable at 1920 X 1080 @ 25 fps simultaneously
11	White Balance	Auto / Manual / ATW / One Push
12	Noise Reduction	3DNR / 2DNR / Color NR
13	Zoom	Digital Zoom
14	Video Streams	Three Stream supportable , All stream should be H.265
15	Image Setting	Saturation, Brightness, Contrast, Sharpness, Hue adjustable

16	Two way audio	Line in / Line out
17	Audio Compression	G.711 / G.726 / AAC / LPCM
18	Iris	P – Iris /Auto-Iris
19	Wide Dynamic Range	120 dB
20	Alarm	1 x Input / 1 x output
22	Network Interface	1 x RJ45
23	Storage backup on network failure	Camera should support network failure detection , Camera should have the capability to start the recording automatically on SD card(32 GB min at all locations) in case of connectivity between camera and NVR/Storage device goes down
24	Protocols	ARP,IPv4/v6, TCP/IP, UDP,RTP,RTSP,HTTP, HTTPS, ICMP,FTP,SMTP,DHCP,PPPoE,UPnP, IGMP, SNMP, QoS, ONVIF
25	Text Overlay	Date & time, and a customer-specific text etc.
26	Security	HTTPS / IP Filter / IEEE 802.1X;
27	Firmware Upgrade	The firmware upgrade shall be done through web interface, the firmware shall be available free of cost
28	Power	PoE / DC 12V / AC 24V
29	Operating Temperature	0°C ~ 60°C
30	Operating Humidity	,10% ~ 90%, No Condensation
31	Certification	UL/BIS , CE , FCC
32	ONVIF	ONVIF profile S & G
33	User accounts	10
34	Supported Web Browser	Internet Explorer (7.0+) / Firefox / Safari / chrome

7.10. Functional & Technical Requirements for PAN, Tilt & Zoom(PTZ) Camera

S. No.	Parameters	Specifications
1.	Certifications	UL /BIS ,CE,FCC, IP66
2.	Compatibility	ONVIF profile S , G
3.	Sensor	1/2.8" Progressive scan CMOS
4.	Resolution	Min 2 MP (1920X1080)
5.	Multiple Stream	Triple Stream
6.	Frame Rate	upto 25 fps @ 2 MP

7.	Focal Length	4.5 mm – 135 mm or 4.3 mm - 129 mm or 4.8 mm - 144 mm or 5mm – 150mm or 6mm -180 mm
8.	Field Of view	61.2° - 2.32 ° or better
9.	Optical Zoom	30X
10.	Digital Zoom	16X
11.	Focus	Auto / Manual
12.	WDR	120 dB
13.	Noise Reduction	2D / 3D
14.	Shutter Speed	1/1 ~ 1/10000 sec.
15.	IR	Inbuilt IR , IR distance up to 150 mtr
16.	Day & Night	IR Cut filter
17.	Min Illumination	0.05 @ F1.6 (Color), 0 (B/W) @ F1.6
18.	Iris	Auto-Iris / P-iris
20.	Storage backup on network failure	Camera should support network failure detection , Camera should have the capability to start the recording automatically on SD card in case of connectivity between camera and NVR/Storage device goes down
21.	Storage	Built in SD card slot with 128 GB SD card with class 10 speed.
22.	Video Compression	H.265,H.264 or better
23.	Privacy Mask	Min 8 privacy zones
24.	Audio	2 Way audio
25.	Audio Compression	G.711 / G.726 / AAC
26.	PAN	360 ° endless , Manual speed 0.1° ~ 90°/s , preset speed 9° ~ 240°/s
27.	Tilt	-15 ° ~ 90° , Manual speed 0.1° ~ 60°/s , Preset speed 7° ~ 240°/s , Auto flip
28.	Presets	256
29.	PTZ Operation	8 sequence , 8 cruise
30.	Speed by zoom	On / Off (Pan and tilt speed proportional to zoom ratio)
31.	Home Function	Preset / Sequence / Auto pan / Cruise
32.	Calibration	Auto(On/Off)
33.	Resume after power loss	Supported zero downtime power switching
34.	Protocols	IPv4/v6, TCP/IP, UDP, RTP, RTSP, HTTP, HTTPS, ICMP,FTP, SMTP,DHCP, PPPoE, UPnP, IGMP, SNMP, QoS, ONVIF
35.	Security	HTTPS / IP Filter / IEEE 802.1x
36.	Alarm	2 Input / 1 Output
37.	Alarm response	Preset / Sequence / Auto Pan / Cruise

38.	Ethernet Interface	1 X RJ 45
39.	Supported Web browser	Internet Explore (10.0+) / Firefox / Safari
40.	Weather Proof	IP 66 / NEMA-4X-rated casing
41.	Operating Temperature	As per city Requirements
42.	Power Supply	802.3at (PoE+) 4-Pair 60W / AC 24V \pm 20% / DC 12V
43.	Power Consumption	45W or less (with IR & Heater on)

7.11. Functional & Technical Requirements for ANPR System

Sr. No.	Description
1.	The ANPR Platform shall be an enterprise class IP-enabled security and safety software solution.
2.	The ANPR Platform shall support the seamless Integrate with the proposed C4i platform.
3.	The automatic number plate recognition Software will be part of the supplied system, Success rate of ANPR will be taken as 85% or better for both day and night time on all standard license plates with straight English roman font .
4.	The ANPR Platform shall allow the user to Protect a Read or Hit from deletion for a configurable period of time.
5.	The ANPR Platform shall allow the user to correct a Plate Read manually.
6.	The ANPR Platform shall present the user with a Simple Wizard for Hotlist creation.
7.	The ANPR Platform shall allow the user to create a Hotlist without the need for any attribute information other than license plate number.
8.	The ANPR Platform shall allow the user to search the configured hotlists for any data in any of the specified fields.
9.	The ANPR Platform shall allow the user to generate a read report specifically targeted to those reads that generated a hit.
10.	The ANPR Platform shall allow for map-based viewing of real-time read monitoring.
11.	The ANPR Platform shall allow the user to search for full or partial license plate numbers.

12.	The ANPR Platform shall allow the user to search for a license plate by using wildcards.
13.	The ANPR Platform shall allow the user to automate downloading Hotlists from a FTP/SFTP or HTTP/HTTPS server using username/password/certificate authentication.
14.	The ANPR Platform shall allow the user to customize the format of the Reports displayed on-screen.
15.	Reporting, including creating custom report templates and incident reports.
16.	The ANPR Platform shall be an IP enabled solution. All communication between the SSM and ANPR Platform shall be based on standard TCP/IP protocol and shall use TLS encryption with digital certificates to secure the communication channel.
17.	The ANPR Platform shall protect against potential database server failure and continue to run through standard off-the-shelf solutions.
18.	The ANPR Platform shall manage the central database that contains all the system information and component configuration of the ANPR Platform.
19.	The ANPR Platform shall authenticate users and give access to the ANPR Platform based on predefined user access rights or privileges, and security partition settings.
20.	The ANPR Platform shall support the configuration/management of the following components specific to ALPR:
A	ALPR units and cameras.
B	Hotlists and Wanted vehicles
C	It shall be possible to view video associated to ALPR events when viewing a report.
21.	The ANPR Platform shall support the following types of reports: ALPR-specific reports (mobile ALPR playback, hits, plate reads, reads/hits per day, reads/hits per ALPR zone, and more).
22.	The ANPR Platform shall support the configuration and management of users and user groups. A user shall be able to add, delete, or modify a user or user group if he or she has the appropriate privileges.
23.	The ANPR Platform shall support the generation of audit trails. Audit trails shall consist of logs of operator/administrator additions, deletions, and modifications.

24.	Audit trails shall be generated as reports. They shall be able to track changes made within specific time periods. Querying on specific users, changes, affected entities, and time periods shall also be possible.
25.	For entity configuration changes, the audit trail report shall include detailed information of the value before and after the changes.
26.	The ANPR Platform shall support the generation of user activity trails. User activity trails shall consist of logs of operator activity on the ANPR Platform such as login, ALPR event viewed, hotlist edits, camera viewed, badge printing, video export, and more.
27.	The ANPR Platform shall be an IP enabled solution. All communication between the SSM and ANPR Platform shall be based on standard TCP/IP protocol and shall use TLS encryption with digital certificates to secure the communication channel.
28.	The ANPR Platform shall monitor the health of the system, log health-related events, and calculate statistics.
29.	Calculates availability for clients, servers and ALPR/access/video units for efficient SLA management
30.	A web-based, centralized health dashboard shall be available to remotely view unit and role and status of the ANPR devices.
31.	Detailed system care statistics will be available through a web-based dashboard providing health metrics of ANPR Platform including Uptime and mean-time-between-failures.
32.	ANPR Platform should integrate with Vahan Database via C4I.
33.	ANPR should have at least Deployment in India in any Law Enforcement Project/Smart city project. Necessary Document evidence to be provided
34.	Vehicle Search: Shall have an option to search vehicles by vehicle colour vehicle colour +license plate vehicle make and type date & time location type of Vehicle

35.	<p>Number plate missing detection:</p> <p>The system should be able to detect if there is any vehicle in the camera view without a properly installed number plate or no number plate at all.</p> <p>The system should have capability to let the user search for all such vehicle through a UI based filtering system</p> <p>The user should be able to search and track any such vehicle using various vehicle search criteria as mentioned in the point above.</p>
-----	---

User Minimum Requirement

S.No.	Features	Specifications
1	Camera	2 Megapixel IP camera Make: Certified Camera for the Purpose as per certificate Shutter Speed 1/1000th sec or better. 5 – 50mm varifocal lens, IR corrected or as per site requirement to meet the desired functional and technical specifications. (see details specifications in Camera sheet)
2	Illuminator	Integrated external Infrared capable to take images in night time and detect automatically number plate at distance of minimum 25 meters.
3	Outdoor equipment housing	IP66 of better standards capable of withstanding vandalism and harsh weather conditions.(certification to be produced)

7.12. Functional & Technical Requirements RLVD System

S.No.	Features	Specifications
1	General	System should be totally digital
2	Vehicle violation criterion at Intersection	The system shall detect and capture vehicle details when: (a) It violates the stop line/zebra crossing (b) It violates the red light signal Option for Spot Speed (c) It violates the speed limit in any phase (red or green or even when the signal is not working) in places where instant speed system is installed along with RLVD system.
3	Red Light detection	System shall be Non-Intrusive. It shall not be connected with traffic light and red light status is detected without any physical connection to traffic light.
4	Fair System	Red light system shall be completely fair system with all evidences captured before and after the red light jumping infraction has happened.
5	Lane Coverage	Each camera system shall cover at least 1 lane having width of

		3.5 meter or more.
6	Detecting Vehicle Presence	Red light system should detect vehicle presence without intrusive sensors like magnetic loops. This is to avoid street working during installation and to reduce maintenance cost
7	System Mounting	System can be composite unit with all components inside the IP65 box OR comprised of camera or other units mounted on poles or gantries with controller and processors at side poles to make sure all lanes of the road are covered.
8	Number Plate Capture	System should be able to recognize automatically the number plate of cars in violation. The system shall perform OCR (optical character recognition) of the license plate characters (English alpha-numeric characters in standard fonts). ANPR system works with Indian number plates
9	Accuracy of Number Plate capture (ANPR)	OCR accuracy shall be at least 90% during day time and 85% during night time.
10	Infraction data to be provided by system	Date, time, location of incident image of vehicle, speed, Image of the number plate, text conversion of number plate after OCR At least one image for over-speeding violation and at least six images for pre and six images for post infraction for red light over jumping
11	Context Image	System shall provide Context image (always color to have proof of signal light) of the signal and shall show wide angled context of the offence as well as details of the offending vehicle. Multiple stitched images of the same is possible. The system shall produce, store and transmit a sequence of atleast 6 image relatives to red light violation, or a movie in standard format like avi, mp4, mov, vfwetc
12	Data Retrieval and Reports	Database search could be using criteria like date, time, location and vehicle number. The system is able to generate suitable MIS reports as desired by the user.
13	IP camera for License Plate Capture	The system shall support all standard brands. One camera shall cover at least 3.5 meter width of lane, and capture the license plates of vehicles which violates the traffic signal and

		moving at a speed upto 100 km/hr
14	IR Illuminator	Integrated external Infrared shall be capable to take images in night time and detect automatically number plate at distance of minimum 20 meters.
15	Working temperature	0 to +60 deg.C
16	Security	Strong encryption on data during local storage and data transfer to back office
17	Local Storage	Minimum local storage 64 GB
18	Communication	Connectivity from site to control room shall be through fibre optic/leased lines or better with minimum uptime of 99.5%
19	Alert Generation	On successful recognition of the number plate, system shall generate automatic alarm to alert the control room for vehicles which have been marked as "Wanted", "Suspicious", "Stolen", "Expired".
20	Compliance Certificate	CE and RoHS compliant certificate
21	Test reports	Third party (authorized company to do so) speed test reports can be submitted to client. On field detailed speed test reports for upto 100 km/hr with various speed limits. Alternatively, the system should be approved and homologated by some traffic or infrastructure department who directly over sees fine generation. or A certificate/test report from reputed research institutes accredited and recognized by Govt of India is acceptable. Certificate on the accuracy from any IPS officer for ± 2 kmph and running satisfactorily in Indian city for at least an year is a must.
22	BACK office software	The system should provide facility to privileged users to manually check the entry in database using standard Web browsers and edit the numbers which may be wrongly OCR-read, before the numbers are fed to the Challan generating sub-system. An audit trail should be maintained to record such editing activities.
		No deletion or addition of data without validation , proper password protection
		The system should provide facility to search for the cases of violations occurred during any specific span of time, and provide a statistical analysis of the number of such incidences occurring during various days of the month
23	e-Challan Integration	Integration with e-challan system

		Integration with RTO database in future should be possible and should also be integrated with the proposed Video Management System.
24	Certifications:	In case of Spot system with RLVD , Systems should be certified as per requirement of Speed Systems (as per Speed systems technical requirement)
25	End-User Certificate	Product should already in use with enforcement authorities and is used for generating fines. End user certificates for proper working shall be submitted.

7.13. Infrared Illuminators- Functional & Technical Specification

The infrared illuminators are to be used in conjunction with the cameras specified above (as required) to enhance the night vision, in case, SI wants for his proposed solution.

S.No.	Description	Required Parameters
1	Power	Auto on off, POE+ , AC24V
2	IR Control	Power level, Photocell sensitivity, Timer
3	Type	850 nm semi-covert
4	Distance & Angle of Beam -.	Minimum : 10° x 10°: 120 m (394 ft) or better as may be required for the application
5	Casing	Aluminium and Polycarbonate
6	LED Indicators	Required
7	Environmental Protection	IP66/IK09 Rated or better
8	Mount Options	Wall, Ceiling, Camera Housing Mount
9	Operating Temperature	0 °C to 55 °C or better
10	Standards/Certification	UL/CE/FCC & BIS

8. Project Governance and Change Management

8.1. Project Management and Governance

8.1.1. Project Management Office (PMO)

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

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

- Project Progress

Delays, if any – Reasons thereof and ways to make-up lost time

Issues and concerns

Performance and SLA compliance reports
Unresolved and escalated issues
Project risks and their proposed mitigation plan
Discussion on submitted deliverable
Timelines and anticipated delay in deliverable if any
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:

- Module development status
- Testing results
IT infrastructure procurement and deployment status
Status of setting up/procuring of Helpdesk, DC hosting
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.

8.1.2. Helpdesk and Facilities Management Services

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

SI shall setup a central helpdesk dedicated (i.e. on premise) for the Project. 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 SI is required to maintain for provisioning of the FMS services are described in the Service Level Agreement of this Tender.

Helpdesk System should be part of Workflow management system as mentioned section 5.6.2 with facilities like Auto-Routing, Auto-Escalation, User Management, Password Management, In-Built Form Builder & Process Designer etc.

8.1.3. Steering Committee

The Steering Committee will consist of senior stakeholders from PSCL, its nominated agencies and SI. SI will nominate its Smart City vertical head to be a part of the Project Steering Committee.

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, PSCL may call for a Steering Committee meeting with prior notice to SI.

8.1.4. Project Monitoring and Reporting

SI shall circulate written progress reports at agreed intervals to PSCL 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. PSCL reserves the right to ask the bidder for the project review reports other than the standard weekly review reports.

MSI has to provide one SUV vehicle with driver and fuel dedicatedly at disposal of Project Incharge during entire period of Commissioning and O&M for Project Monitoring and supervision purpose.

8.1.5. Risk and Issue management

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.

SI shall carry out a Risk Assessment and document the Risk profile of PSCL based on the risk appetite and shall prepare and share the PSCL Enterprise Risk Register. 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 PSCL.

SI shall monitor, report, and update the project risk profile. The risks should be discussed with PSCL 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.

8.2. Governance procedures

SI shall document the agreed structures in a procedures manual.

8.2.1. Planning and Scheduling

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. SI has to get the plan approved from PSCL 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:

- The project break up into logical phases and sub-phases;

- Activities making up the sub-phases and phases;
- Components in each phase with milestones;

The milestone dates are decided by PSCL 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.

- Key milestones and deliverables along with their dates including those related to delivery and installation of hardware and software;
- Start date and end date for each activity;
- The dependencies among activities;
- Resources to be assigned to each activity;
- Dependency on PSCL

8.2.2. License Metering / Management

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 ICCCL, and DC. This may be carried out through the use of standard license metering tools.

8.3. Manpower Deployment

SI shall deploy Manpower during implementation and O&M phases. The deployed resource shall report to PSCL 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	Min Qty	Minimum Deployment during Implementation phase	Minimum Deployment during O & M phase
1.	Team Leader-cum-Program Manager	1	100%	100%
2.	Solution Architect	1	80%	Onsite Support to Project team on need basis
3.	DC/DR/Cloud Expert	1	100%	100%
4.	IoT/Analytics/AI Expert	1	60%	Onsite Support to Project team on need basis
5.	ITMS Expert	1	50%	Onsite Support to Project team on need basis
6.	Database Expert	1	100%	Onsite Support
7.	Security Expert	1	60%	Onsite Support to Project team on need basis
8.	Network/Systems Administrator	1	100%	Onsite support
9.	GIS Expert	1	80%	Onsite support

S.No.	Type of Resource	Min Qty	Minimum Deployment during Implementation phase	Minimum Deployment during O & M phase
10.	Software Lead/ Mobile App Developer	1	80%	Onsite support
11.	Quality Assurance/Testing	1	On need basis	On need basis
12.	Operators for ICC	20	100%	20 in three shifts (shift distribution shall be decided by PSCL)
13.	Field Engineers for CCTV	5	100%	Onsite Support
14.	Field Engineers for ITMS	3	100%	Onsite Support

Apart from the above mentioned manpower, SI is required to provide suitable manpower to monitor the data feeds at the Integrated Command Control Centre and support PSCL in operationalization of the project. Total number of operators required for the project is 20 in three shifts. PSCL reserves the right to increase or decrease the number of operators. The exact role of these personnel and their responsibilities would be defined and monitored by PSCL and respective departmental personnel.

The manpower for viewing of feeds at the Police Station Monitoring Center (PSMC) and ICC shall also be provided by Police department. Minimum 10 police personal shall be provided by the Police department for monitoring purpose at the ICC and one police personal at each Police Station. However, technical engineers need to be deployed by the SI for 24x7 technical support to network and other infrastructures at police station level and at camera end-points on sharing basis in best economical way.

SI shall be required to provide such manpower meeting following requirements:

All such manpower shall be minimum graduates.

All such manpower shall be without any criminal background / record.

PSCL 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.

SI shall have to replace any person, if not found suitable for the job.

All field manpower must have independent two-wheeler for local commuting.

All the manpower shall have to undergo training from 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 PSCL officers on right approaches for monitoring the feeds & providing feedback to PSCL, Traffic Police and other associated government agencies.

SI has to also provide minimum 2 days' training to atleast 5 to 8 persons of each police

station, Railway Station and SP offices for City Surveillance and associated SOPs.

Each person shall have to undergo compulsory 1 day training every month.

Operational Manpower shall work in 3 shifts, with no person being made to see the feeds for more than 8 hours at a stretch.

Detail operational guideline document, standard operating procedure, governance and oversight plan shall be prepared by SI during implementation which shall specify detail responsibilities of these resources and their do's & don'ts.

The supervisors required for operationalization of the project will be provided by PSCL, as per requirements.

8.4. Change Management & Control

8.4.1. Change Orders / Alterations / Variations

SI agrees that the requirements given in the Bidding Documents are minimum requirements and are only indicative. The vendor would need to reach out the details at the time of preparing the design document prior to actual implementation. It shall be the responsibility of 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.

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.

Any upward revision and/or additions consequent to errors, omissions, ambiguities, discrepancies in the Bidding Documents which 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.

The Change Order will be initiated only in case (i) the Purchaser directs in writing 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 SI to incorporate changes or additions to the technical specifications already covered in the Contract.

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.

Any change order 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.

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.

Within ten (10) working days of receiving the comments from the Purchaser or the drawings, specification, purchase requisitions and other documents submitted by SI for approval, 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.

8.5. 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.

8.5.1. Cooperation and Provision of Information

During the exit management period:

- a. SI will allow the PSCL or its nominated agency access to information reasonably required to define the then current mode of operation associated with the provision of the services to enable the PSCL to assess the existing services being delivered;
- b. Promptly on reasonable request by the PSCL, 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 SI or sub-contractors appointed by SI). The

PSCL shall be entitled to copy of all such information. Such information shall include details pertaining to the services rendered and other performance data. SI shall permit the PSCL or its nominated agencies to have reasonable access to its employees and facilities, to understand the methods of delivery of the services employed by SI and to assist appropriate knowledge transfer.

8.5.2. Confidential Information, Security and Data

- a. SI will promptly on the commencement of the exit management period supply to the PSCL or its nominated agency the following:
 - information relating to the current services rendered and customer and performance data relating to the performance of sub-contractors in relation to the services;
 - documentation relating to Intellectual Property Rights;
 - documentation relating to sub-contractors;
 - all current and updated data as is reasonably required for purposes of PSCL or its nominated agencies transitioning the services to its Replacement SI in a readily available format nominated by the PSCL, its nominated agency;
 - all other information (including but not limited to documents, records and agreements) relating to the services reasonably necessary to enable PSCL or its nominated agencies, or its Replacement SI to carry out due diligence in order to transition the provision of the Services to PSCL or its nominated agencies, or its Replacement SI (as the case may be).
- b. Before the expiry of the exit management period, SI shall deliver to the PSCL 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 SI shall be permitted to retain one copy of such materials for archival purposes only.

8.5.3. Transfer of Certain Agreements

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

8.5.4. General Obligations of SI

- a. SI shall provide all such information as may reasonably be necessary to effect as seamless a handover as practicable in the circumstances to the PSCL or its nominated agency or its Replacement SI and which 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 SI.
- c. SI shall commit adequate resources to comply with its obligations under this Exit Management Schedule.

8.5.5. Exit Management Plan

- a. SI shall provide the PSCL 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 SI's sub-contractors, staff, suppliers, customers and any related third party as are necessary to avoid any material detrimental impact on the PSCL's operations as a result of undertaking the transfer;
 - Proposed arrangements for the segregation of SI's networks from the networks employed by PSCL and identification of specific security tasks necessary at termination(if applicable);
 - Plans for provision of contingent support to PSCL, and Replacement SI for a reasonable period after transfer.
- b. SI shall re-draft the Exit Management Plan annually thereafter to ensure that it is kept relevant and up to date.
- c. Each Exit Management Plan shall be presented by SI to and approved by the PSCL or its nominated agencies.
- d. The terms of payment as stated in the Terms of Payment Schedule include the costs of SI complying with its obligations under this Schedule.
- e. In the event of termination or expiry of MSA, and Project Implementation, each Party shall comply with the Exit Management Plan.
- f. During the exit management period, SI shall use its best efforts to deliver the services.
- g. Payments during the Exit Management period shall be made in accordance with the Terms of Payment Schedule.
- h. This Exit Management plan shall be furnished in writing to the PSCL or its nominated agencies within 90 days from the Effective Date of this Agreement.

9. Project Implementation Schedule, Deliverables and Payment Terms

T = 14 Days from Issue of Letter of Award (LOA) of Contract or signing of contract, whichever is earlier.

S. No.	Milestones	Deliverables	Timelines (in months)
1	Project Execution & Implementation Phase		T + 15 months
1.1	Project Inception Report Confirm scope of project and prepare the engagement brief Prepare a Strategy and Assess Stage plan Select required Program management procedures, standards, methods, tools & Preparation of quality Plan	Detailed site survey report including infrastructure requirement analysis, hardware deployment plan, Work breakdown Structure, Quality Management Plan, Risk & Its mitigation Plan, Resource Deployment Plan, Communication & Change Management Plan, Escalation & Exit Management Plan, recommended action plan to address the gaps, budget estimates for addressing the gaps uncovered during the survey, phase wise location distribution etc. Detailed Survey Report , Studying the design architecture, carrying out site survey and finalize the distribution, exact position of the various systems and its components, Studying the compatibility between the previous deployed systems. Project Plan including Information Security and Business Continuity, Roll Out Plan, Detailed Engineering Drawing & Marking, Sensitization & Training Plan, Operations management plan etc.	T + 1 month

1.2	Requirement Study <ul style="list-style-type: none"> Integrated Command Control and Communication Centre (ICCC) including Data Centre City IT Network Infrastructure (including OFC laying) Intelligent Traffic Management System (ITMS) Environmental Monitoring System Mobile App Integration of ICCC platform with existing & under-development external Systems/ Applications as per scope 	<ol style="list-style-type: none"> Architecture and design for ICCC, City IT Network and Data Centre including Data Centre Architecture, Network Architecture, Security Architecture Carrying out the survey & Finalize the distribution , Exact Position of various systems & Its components Submission of FRS, SRS including Solution Architecture, Application Design Documents (HLD & LLD) of the proposed system, HLD & LDD should be prepared by OEM, Design integration and customization approach for the project (including integration with legacy systems/applications), GIS – Creation of new layers as per Patna Smart City , data migration, training & operationalization of enterprise GISsystem for the city Roll out plan for each system and its components, which will include implementation phases and plan, migration plan, acceptance testing plan. Submission of Migration plan and system compatibility assessment report Final List of equipment including current infrastructure reusability report (If applicable) Detailed site engineering drawings with markings Integration report for external applications, Knowledge Transfer, Develop overall network design including last mile connectivity between the edge devices of all the systems and the network access points 	T + 2 months
-----	---	--	--------------

1.3	<p>Phase I: Go-Live</p> <p>a. Design, Procurement , supply, installation, commissioning including interior civil work, hardware, system software, network equipment for Datacentre, Network Connectivity for atleast 500 Cameras , Installation & Commissioning of JB, Poles, Switches, UPS in the Field for Camer Operationalization of Command Control & Communication Centre along with DC and DR including bandwidth procurement.</p> <p>b. City IT Network Infrastructure – OFC laying, pan city availability of secure network for all proposed edge devices & sensors. Guidelines issued by MoUD for cyber security requirement should be adhered to for designing network for sensor & Wi-Fi traffic</p> <p>Obtain all necessary approvals</p>	<ol style="list-style-type: none"> 1. Site Completion/readiness Report 2. Delivery Acceptance Reports from PSCL/authorized entity 3. Installation & Commissioning Reports 4. Software Licenses details requirement 5. Ensuring that all the components and sub-components are in compliance with the specifications as finalized with Patna Smart City Ltd.. The specifications provided in this document is the minimum requirement and System Integrator may procure a component of higher specification if required so as to as ensure services are provided in conformance with the SLA 6. Approval from PSCL on all documents such as, IT inspection test plan, Manufacturer's Test Certificates, Hazardous area certificated for Electrical Equipment/ Instrument, weather proof Certificate, datasheet, drawings, Manuals, Guarantee & Warranties certificates , etc. 7. Undertaking acceptance testing as per the agreed ATP plan including the Site Acceptance Test (SAT). 8. Testing of the independent sub systems and integrated system as a whole and providing the necessary satisfactory testing reports 	T + 5 months
-----	---	---	--------------

1.4	Phase II: Go-Live a. Design, Procurement , supply, installation, commissioning including interior civil work, hardware, system software, network equipment for Datacentre, Network Connectivity for atleast 1000 Cameras , Installation & Commissioning of JB, Poles, Switches, UPS in the Field for Cameras etc. b. Operationalization of Command Control & Communication Centre along with DC and DR including bandwidth procurement. c. City IT Network Infrastructure – OFC laying, pan city availability of secure network for all proposed edge devices & sensors. Guidelines issued by MoUD for cyber security requirement should be adhered to for designing network for sensor & Wi-Fi traffic d. ITMS – Supply, installation, commissioning, training and operationalization of ITMS components (ANPR, RLVD, SVDS, ATCS, PA, ECB) at 30% of total identified locations e. Environmental Sensors - Supply, installation, commissioning, training & operationalization of Environmental sensors at sensors f. Variable Messaging System- Supply, installation, commissioning, training & operationalization of Variable Messaging System at 50% of total identified locations g. Setting up DR	1) Site Completion/readiness Report 2) Delivery Acceptance Reports from PSCL/authorized entity 3) Installation & Commissioning Reports 4) UAT/FAT and Go Live Certificate from PSCL/authorized entity 5) Training Content & Completion Certificate 6) Security Audit Certificate from Cert-In/STQC for Data Centre and Applications	T+7 Months
1.5	Phase III: Go-Live a. Design, Procurement , supply, installation, commissioning including interior civil work, hardware, system software, network equipment for Datacentre, Network Connectivity for atleast 1000 Cameras , Installation & Commissioning of JB, Poles, Switches, UPS in the Field for Cameras etc.	1. Site Completion/readiness Report 2. Delivery Acceptance Reports from PSL/authorized entity 3. Installation & Commissioning Reports 4. Software Licenses details 5. Provide a c 6. entralized Help Desk and Incident Management	T + 12 months

	b. Operationalization of Command Control & Communication Centre along with DC and DR including bandwidth procurement. c. City IT Network Infrastructure – OFC laying, pan city availability of secure network for all proposed edge devices & sensors. Guidelines issued by MoUD for cyber security requirement should be adhered to for designing network for sensor & Wi-Fi traffic d. ITMS – Supply, installation, commissioning, training and operationalization of ITMS components (ANPR, RLVD, SVDS, ATCS, PA, ECB) at remaining 70% of total identified locations e. Integration Variable Messaging System - Supply, installation,	Support till the end of contractual period Recurring refresher trainings for the users and Change Management activities 7. Completing the documentation of Warranty, License & Agreement 8. Pent scanning & Network Dressing & Internal Audit 9. Third Party Administrator (TPA) 10. Security & Network Audit - Format & SOPs 11.	
1.6	Phase IV: Integration & Project Final Go-Live Integration with external applications (existing & proposed)- <ul style="list-style-type: none"> ▪ Intelligent Transportation System ▪ E-Challan System 	1. UAT/FAT and Go Live Certificate from PSCL/authorized entity 2. Training Content & Completion Certificate 3. Security Audit Certificate from Cert-In/STQC 4. Source code of portal, Mobile App & customized applications 5. Integrated Dashboard – Provision for generating configurable reports through dashboard and also real time monitoring and Alert Systems. 6. Integration of all New & Existing System	T + 15 months
2	Project Operation & Maintenance Phase		Go-Live+ 60 months
2.1	Operation & Maintenance (SOW Attached)	Monthly & Quarterly SLA Reports <ul style="list-style-type: none"> • Ad-hoc Reports Operation of Monitoring Centre (including Help Desk) • VAPT Execution • Facility Management Services 	Go-Live + 60 Months

		at Command & Control Centre <ul style="list-style-type: none"> • MIS Reports and Incident Reporting • Preventive Maintenance & Incident Management • SLA Management • Continuous Learning activities with Patna Smart City to make the system Mature & Stable 	
--	--	---	--

Based on findings of the site survey activity done by SI, SI may propose a change in the number of sites or individual units to be deployed in each phase as well as overall scope and a consequent change in phasing. PSCL also retains the right to suo-moto change the number of sites or individual units to be deployed for each scope item. The final decision on change in phasing and related change in payment schedules shall be at the discretion of PSCL.

SI should complete all the activities within the defined timelines as indicated above. The timeline will be reviewed regularly during implementation phase and may be extended in case PSCL feels that extension in a particular Request Order/Integration or any track is imperative, for the reason beyond the control of the bidder. In all such cases PSCL's decision shall be final and binding. SI will be eligible for the payment based on the completion of activities and approval of the relevant deliverables.

9.1. Payment Schedule

The total payment shall be paid separately for Capex and Opex. For payment release purpose, Capex value will not be considered more than 80% of total bid value at any stage, balance will be considered as Opex. Capex payment shall be released based on below mentioned milestones. Opex payment will be released in twenty (20) equal quarterly instalments spread across 5 years Post Final Go-Live. Other recurring/non-recurring expenses like for Electricity connections & bills, Fees for PUC/ROW/etc. to be paid to Government Departments for Project Execution will be released on actuals by PSCL (These expenses need not to be mentioned in Price Bid).

	Milestones	Timelines	Payment
Capex			
1 st	Delivery of Hardware/Software	T + 2 Months	<ul style="list-style-type: none"> • 50% of Value of Capex of supplied items (Hardware & Software) on Pro-rata basis. • 30% of Value of Capex of supplied items after installation of Hardware & Software on Pro-rata basis. • 10% of the Services items
2 nd	Phase I: Go Live	T + 5 Months	<ul style="list-style-type: none"> • 50% of Value of Capex of supplied items (Hardware & Software) on Pro-rata basis. • 30% of Value of Capex of supplied items

			after installation of Hardware & Software on Pro-rata basis. <ul style="list-style-type: none"> • 20% of the services items • 10% of the Phase I Go-Live
3 rd	Phase II: Go Live	T + 7 Months	<ul style="list-style-type: none"> • 50% of Value of Capex of supplied items (Hardware & Software) on Pro-rata basis. • 30% of Value of Capex of supplied items after installation of Hardware & Software on Pro-rata basis. • 20% of the services items • 10% of the Phase II Go-Live
4 th	Phase III: Go Live	T+12 Months	<ul style="list-style-type: none"> • 50% of Value of Capex of supplied items (Hardware & Software) on Pro-rata basis. • 30% of Value of Capex of supplied items after installation of Hardware & Software on Pro-rata basis. • 20% of the services items • 10% of the Phase III Go-Live
5 th	Phase IV: Integration & Project Final Go-Live	T1 = T + 15 months	<ul style="list-style-type: none"> • Value of Capex of supplied items (Hardware & Software) and installation in final Go-Live on pro-rata basis. • Remaining of Capex of all the phases
Opex			
1	Project Operations & Maintenance phase for a period of 60 months from the date of Final Go Live	T1 + 60 Months	OPEX will be paid in twenty (20) equal quarterly installments spread across 5 years Post Final Go-Live. However, recurring cost of Electricity shall be paid on actuals during Implementation and O&M phase

Note 1: If bidder requests for Mobilization advance, following conditions shall be applicable:

- Interest bearing Mobilization advance (@ 10% Simple Interest) can be of 5% of capex value can be given in two equal installments on production of Unconditional Bank Guarantee of 110% of the requested amount valid for 3 months beyond 10 months of release of advance.
- Mobilization advance shall be adjusted proportionately among all Phases' Payment Release but total recovery shall be made within 10 months of release of advance.

Note 2:

- All payments to the Systems Integrator shall be made upon submission of invoices along with necessary approval certificates from PSCL
- The above payments are subject to meeting of SLA's, failing which the appropriate deductions as mentioned in the Volume III of this RFP would be applicable.

10. Annexures:

10.1. Annexure 1 : Bill of Quantity

Mentioned below is the indicative Bill of Material for each proposed project component, however the below quoted quantity are minimum and MSI is required to access the exact requirement, location wise, for all the proposed solution components and shall accordingly size the hardware and software infrastructure requirement to meet the project objectives and SLA. Bidder can increase the line item/quantity, if required.

Proposed quantity should not be less than the Indicative quantity, in any case.

Wherever under the indicative quantities “As per requirement” is mentioned, the Bidder has to mention the proposed quantity along with the unit rates in the Price Bid. Bidder has to provide proposed quantity for each line item in Technical Bid and justify as per the solution requirements during the technical bid evaluation. This quantity and the increased line-item (if any) must be reflected in the Price Bid, failing which the bid may be rejected.

Initially part of the BoQ would be housed in the temporary building as per the minimum and essential requirements for the functioning of the ICCC. Later, full and final BoQ would be housed in the permanent new building including the transfer of the equipment from the temporary building to the permanent building. MSI has to do necessary minor changes in walls/partition in temporary building as per requirement.

Sr No	Solution / Component	Line Item (Component wise)	UoM	Indicative quantity	Proposed Quantity By Bidder As per His Assessment	Proposed Make & Model	Compliance to Specifications (Yes/No)	Referen ce to Supporti ng Docume nt/Broc hure
1	2	3	4	5	6	7	8	9
1	Pancity OFC Network Backbone	50 mm HDPE Pipe	Kms	220				
2	Pancity OFC Network Backbone	Backbone Fiber Cable Loose Tube, Gel-Free Cable 144 F, Single-mode (Armoured)	Kms	10				
3	Pancity OFC Network Backbone	Backbone Fiber Cable Loose Tube, Gel-Free Cable 144F, SM(Redundant) (Armoured)	Kms	10				
4	Pancity OFC Network Backbone	Distribution Fiber Cable Loose Tube, Gel-Free Cable 96 F, SMF for Secondary PoPs (Armoured)	Kms	40				

REQUEST FOR PROPOSAL
Master System Integrator for Implementation of
Integrated Smart Solutions, under Smart City
Mission in Patna

Sr No	Solution / Component	Line Item (Component wise)	UoM	Indicative quantity	Proposed Quantity By Bidder As per His Assessment	Proposed Make & Model	Compliance to Specifications (Yes/No)	Reference to Supporting Document/Brochure
5	Pancity OFC Network Backbone	Distribution Fiber Cable Loose Tube, Gel-Free Cable 96 F, SMF for Secondary PoPs (Armoured)	Kms	120				
6	Pancity OFC Network Backbone	Access Fiber Cable: Loose-Tube, Gel-Free Cable 48F, MMF (Armoured)	Kms	40				
7	Pancity OFC Network Backbone	Rate contract Price for Pancity OFC Connection in the premises of Government Building as and when required. Connectivity has to be provided on Fiber (Upto 100 Mtr) as well as on RJ45 Ethernet.	No.	1				
8	ICC	70 Inches Panel for DLP based Video Wall	No.	20				
9	ICC	Video Wall Controller (With Required Adaptors, Converter, 4-port Display Graphic card, 4-channel HD capture card with DVI splitter cables, Cabling & Other Fixtures, etc)	No.	2				
10	ICC	Video Wall Management Software	No.	1				
11	ICC	IP Phone	No.	10				
12	ICC	Keyboard Joystick to	No.	30				

Sr No	Solution / Component	Line Item (Component wise)	UoM	Indicative quantity	Proposed Quantity By Bidder As per His Assessment	Proposed Make & Model	Compliance to Specifications (Yes/No)	Reference to Supporting Document/Brochure
		control PTZ Cameras						
13	ICC	HD LED Display (55 Inches)	No.	16				
14	ICC	Workstation Desktop with three LED Monitors	No.	50				
15	ICC	FRS-Master Server Database (can store upto 10,00,000 Live Templates with Social Media/Offline Database matching) (50 Camera Licenses)	No.	1				
16	ICC	Online UPS (sizing as per proposed solution 100KVA 30 Minutes Battery Backup)	No.	2				
17	ICC	Network & WiFi enabled A4/A3/Legal Size MFP Color Laser Printer/ Scanner /Coupler with ADF (Heavy Duty-50K per month for minimum 50 PPM speed for B/W A4 Prints	No.	4				
18	ICC	Biometric access control System	No.	1				
19	ICC	Dome cameras for Internal Surveillance/Fixed Box Cameras	No.	30				
20	ICC	Building Management System (BMS)	No.	1				
21	ICC	Metal Detector (Hand Held)	No.	1				

REQUEST FOR PROPOSAL
Master System Integrator for Implementation of
Integrated Smart Solutions, under Smart City
Mission in Patna

Sr No	Solution / Component	Line Item (Component wise)	UoM	Indicative quantity	Proposed Quantity By Bidder As per His Assessment	Proposed Make & Model	Compliance to Specifications (Yes/No)	Reference to Supporting Document/Brochure
22	ICC	Addressable Fire Detection and Alarm System	Set	1				
23	ICC	Rodent Repellent system	Set	1				
24	ICC	Gas Based fire Suppression System	Set	1				
25	ICC	Portable fire Extinguishers (5 Kgs)	No.	20				
26	ICC	Split Air Conditioner 2 Ton (5 star energy efficiency rating)	No.	15				
27	ICC	Workstation Furniture and Fixtures for ICC	No.	35				
28	ICC	Revolving Chairs for office staff	No.	35				
29	ICC	Office Desk Furniture and Fixtures	No.	15				
30	ICC	Ergonomic Chairs for ICC/Chairs	No.	40				
31	ICC	Conference Table (for 10 personnel) & Chairs Set	Set	4				
32	ICC	Hand Set	No.	10				
33	ICC	Head Set	No.	10				
34	ICC	Voice Logger	Set	1				
35	ICC	Soft telephone	No.	10				
36	Data Centre Hardware	Core Router	No.	2				
37	Data Centre Hardware	Core Switch	No.	2				
38	Data Centre Hardware	Firewall	No.	2				
39	Data Centre Hardware	DC 48 Ports Switch for DMZ	No.	2				
40	Data Centre Hardware	Managed 24 Port L3 Edge Switches for Management	No.	2				

REQUEST FOR PROPOSAL
Master System Integrator for Implementation of
Integrated Smart Solutions, under Smart City
Mission in Patna

Sr No	Solution / Component	Line Item (Component wise)	UoM	Indicative quantity	Proposed Quantity By Bidder As per His Assessment	Proposed Make & Model	Compliance to Specifications (Yes/No)	Reference to Supporting Document/Brochure
41	Data Centre Hardware	24 Port Aggregation Switch	No.	8				
42	Data Centre Hardware	42U Server/Network Rack with necessary accessories	No.	16				
43	Data Centre Hardware	Blade Chassis with Fabric Interconnect Switches	No.	10				
44	Data Centre Hardware	Video Management/Analytics Server (Blade Server) (2 Processors)	No.	12				
45	Data Centre Hardware	Video Recording Server (Blade Server) (2 Processors)	No.	21				
46	Data Centre Hardware	ATCS Server (Blade Server)	No.	4				
47	Data Centre Hardware	ANPR Server (GPU Server)	No.	6				
48	Data Centre Hardware	RLVD Server (GPU Server)	No.	2				
49	Data Centre Hardware	TARS server	No.	2				
50	Data Centre Hardware	Automatic Call Distributor Server (Blade Server)	No.	1				
51	Data Centre Hardware	Digital Voice Logger Server (Blade Server)	No.	1				
52	Data Centre Hardware	Continuous Learning Server A.I/Training Server)	No.	2				
53	Data Centre Hardware	GIS server (Blade Server)	No.	1				
54	Data Centre Hardware	Database Server (Blade Server)	No.	4				
55	Data Centre Hardware	Anti-Virus and Anti-Spam Server (Blade Server)	No.	2				

REQUEST FOR PROPOSAL
Master System Integrator for Implementation of
Integrated Smart Solutions, under Smart City
Mission in Patna

Sr No	Solution / Component	Line Item (Component wise)	UoM	Indicative quantity	Proposed Quantity By Bidder As per His Assessment	Proposed Make & Model	Compliance to Specifications (Yes/No)	Reference to Supporting Document/Brochure
56	Data Centre Hardware	Enterprise Mail and Message Server (Blade Server)	No.	1				
57	Data Centre Hardware	Domain Controller (DC + ADC) Server (Blade Server)	No.	1				
58	Data Centre Hardware	Server Load Balancer	No.	2				
59	Data Centre Hardware	SAN Switch	No.	2				
60	Data Centre Hardware	Scale Out Storage (Primary)- 10 PB	TB	1				
61	Data Centre Hardware	Unified Storage (Storage) - 1PB	TB	1				
62	Data Centre Hardware	300 KVA UPS (sizing as per proposed solution) in N+N redundancy	No.	2				
63	Data Centre Hardware	Precision Air Conditioning System for the Server Farm Area	No.	5				
64	Data Centre Hardware	Split Air Conditioner 2 Ton (5 star energy efficiency rating) for the Auxiliary Area	No.	8				
65	Data Centre Hardware	Site Preparation Cost for ICC & DC	Specification Enclosed	1				
66	Data Centre Hardware	Water Leak Detection	No.	3				
67	Data Centre Hardware	Rodent Repellent system	No.	3				
68	Data Centre Hardware	Fire Suppression System	No.	3				
69	Data Centre Hardware	Fire Alarm System	No.	3				
70	Data Centre Hardware	Copper Cabling	Mtr	15000				

REQUEST FOR PROPOSAL
Master System Integrator for Implementation of
Integrated Smart Solutions, under Smart City
Mission in Patna

Sr No	Solution / Component	Line Item (Component wise)	UoM	Indicative quantity	Proposed Quantity By Bidder As per His Assessment	Proposed Make & Model	Compliance to Specifications (Yes/No)	Reference to Supporting Document/Brochure
71	Software Solutions	Server OS License	No.	1				
72	Software Solutions	HIPS for 50 Servers farm (For all servers)	No.	1				
73	Software Solutions	Licenses for Facial Recognition (Channels)	No.	25				
74	Software Solutions	Licenses for Video Analytics (2 usecases for 500 cameras)	No.	1000				
75	Software Solutions	Virtualization Software License	No.	104				
76	Software Solutions	Anti-virus & Anti-Spam Enterprise software (License per endpoint)	No.	130				
77	Software Solutions	Any/All Off the Shelf Software License required for complete solution	Lot	1				
78	Software Solutions	Enterprise Management system/Help Desk Management	No.	1				
79	Software Solutions	ICCC core application (HA)/ICCC Software	No.	1				
80	Software Solutions	SMS Gateway with annual 200,000 SMSs	No.	1				
81	Software Solutions	Video Management Software licenses for recording and managing for all new and existing Cameras with redundancy	No.	1				

REQUEST FOR PROPOSAL
Master System Integrator for Implementation of
Integrated Smart Solutions, under Smart City
Mission in Patna

Sr No	Solution / Component	Line Item (Component wise)	UoM	Indicative quantity	Proposed Quantity By Bidder As per His Assessment	Proposed Make & Model	Compliance to Specifications (Yes/No)	Referen ce to Supporti ng Docume nt/Broc hure
82	Software Solutions	CTI/PBX System with IVR and Automated Call Distribution Software	No.	1				
83	Software Solutions	ITMS ATCS Software	No.	1				
84	Software Solutions	ITMS ANPR & RLVD Software	No.	1				
85	Software Solutions	ITMS-SVD software	No.	1				
86	Software Solutions	ITMS-TARS	No.	1				
87	Software Solutions	ITMS PA Software	No.	1				
88	Software Solutions	ITMS ECB management software	No.	1				
89	Software Solutions	ITMS-Variable Message Software	No.	1				
90	Software Solutions	Mobile Application	No.	1				
91	GIS	Enterprise GIS for Web GIS with Geo Analytics	Specif icatio n Enclo sed	1				
92	Software Solutions	e-challan software	No.	1				
93	Software Solutions	Rack Servers with 3 GPUs in Datacentre (Video Analytics Servers)	No.	16				
94	Data Centre Hardware	Diesel Genset, 650 KVA	No.	1				
95	Data Centre Hardware	32A IP PDU with Ethernet based Environment Monitoring System with one Temperature Sensor	No.	30				
96	Data Centre Hardware	164 1P PDU with Ethernet based Environment Monitoring	No.	10				

REQUEST FOR PROPOSAL
Master System Integrator for Implementation of
Integrated Smart Solutions, under Smart City
Mission in Patna

Sr No	Solution / Component	Line Item (Component wise)	UoM	Indicative quantity	Proposed Quantity By Bidder As per His Assessment	Proposed Make & Model	Compliance to Specifications (Yes/No)	Reference to Supporting Document/Brochure
		System with one Temperature Sensor						
97	Data Centre Hardware	Blanking Panels	No.	300				
98	DR Site	Rate Contract for Server Computing with OS, Database, Security Features as per MEITY Guidelines. (4 Core, 32 GB RAM per VM per month)	VM	1				
99	DR Site	Rate Contract for Onetime DR Provisioning 8 Installation Charges (Per VM-at the time of new VM addition)	VM	1				
100	DR Site	Rate Contract for Storage for all Critical Applications, Enterprise database GIS data and Flagged video Feed (Not for regular feed) with all Security features as per MEITY guidelines.	TB	1				
101	ITMS-ATCS	ATCS Traffic signal controller	No.	30				
102	ITMS-ATCS	Vehicle Detection Camera	No.	120				
103	ITMS-ATCS	Countdown timer	No.	120				
104	ITMS-ATCS	Supply & Installation of signal head with 3 signal aspect -	No.	240				

REQUEST FOR PROPOSAL
Master System Integrator for Implementation of
Integrated Smart Solutions, under Smart City
Mission in Patna

Sr No	Solution / Component	Line Item (Component wise)	UoM	Indicative quantity	Proposed Quantity By Bidder As per His Assessment	Proposed Make & Model	Compliance to Specifications (Yes/No)	Reference to Supporting Document/Brochure
		Red, Yellow, Green Arrow						
105	ITMS-ATCS	Supply & Installation of Signal head with 1 signal aspect - Green Arrow	No.	480				
106	ITMS-ATCS	Supply & Installation of Signal head with 2 signal aspect - Pedestrian Red & Ped Green	No.	120				
107	ITMS-ATCS	Supply & Installation of Galvanised Iron Class B Traffic Signal straight pole of 6 m height with all accessories	No.	120				
108	ITMS-ATCS	Supply Installation of Galvanised Iron Class B Traffic Signal cantilever pole with all accessories	No.	120				
109	ITMS-ATCS	Supply & Installation of Cabinet for UPS, Switches, etc with Mounting Structure, junction boxes, other accessories, etc	Set	240				
110	ITMS-ATCS	8 Port PoE Ruggedized Switch	No.	800				
111	ITMS-RLVD	Red light Violation Detection (RLVD) Evidence Cameras	No.	360				
112	ITMS-RLVD	ANPR Cameras for RLVD System	No.	720				

REQUEST FOR PROPOSAL
Master System Integrator for Implementation of
Integrated Smart Solutions, under Smart City
Mission in Patna

Sr No	Solution / Component	Line Item (Component wise)	UoM	Indicative quantity	Proposed Quantity By Bidder As per His Assessment	Proposed Make & Model	Compliance to Specifications (Yes/No)	Reference to Supporting Document/Brochure
113	ITMS-RLVD	Local processing unit / Rack Servers with 3 GPUs in Data Centre (ANPR Servers)	No.	40				
114	ITMS-RLVD	Mounting structure with junction boxes etc	Set	720				
115	ITMS-RLVD	8 Port PoE Ruggedized Switch	No.	90				
116	ITMS-Speed Detection	Speed Detection System for covering 2 lanes In one direction with complete subcomponents including ANPR Camera, sensors, wide angle evidence camera, IR Illuminator, non-Intrusive speed sensor, with cabling & mounting infrastructure as required	No.	10				
117	Surveillance System	Outdoor Fixed Box Bullet Camera	No.	60				
118	Surveillance System	Outdoor PTZ Camera	No.	60				
119	Public Address System	Public Address System-IP based PA with speakers, UPS etc.	No.	50				
120	Variable Messaging System	Variable Message Sign Board with all accessories	No.	30				
121	Variable Messaging System	Mounting structure with all	No.	15				

REQUEST FOR PROPOSAL
Master System Integrator for Implementation of
Integrated Smart Solutions, under Smart City
Mission in Patna

Sr No	Solution / Component	Line Item (Component wise)	UoM	Indicative quantity	Proposed Quantity By Bidder As per His Assessment	Proposed Make & Model	Compliance to Specifications (Yes/No)	Reference to Supporting Document/Brochure
		required accessories						
122	Emergency Call Box	ECB system with Mounting structure, UPS, pole etc	No.	50				
123	Environmental Sensors	All type of Environmental Sensors with Management Software	No.	5				
124	ICCC	SIEM Forensic (Separately for Information & Event Management)	No.	2				
125	CCTV-Police Area	IP Fixed Bullet Cameras	No.	374				
126	CCTV-Police Area	Outdoor PTZ Cameras	No.	330				
127	CCTV-Police Area	ANPR Box camera with External IR Illuminator	No.	134				
128	CCTV-Police Area	8 Port PoE Ruggedized Switch	No.	505				
129	CCTV-Police Area	Junction Boxes (including last mile passive networking, earthing, etc.)	No.	505				
130	CCTV-Police Area	UPS- (500 VA with 40 Mins battery backup at full load)/UPS with 1 hr backup)	No.	800				
131	CCTV-Police Area	Anti-Climb Poles for Cameras and other Equipment at junctions with fixing Cost	No.	480				
132	CCTV-Police Area	Cantilever /Gantry Poles for cameras upgradable to ANPR	No.	73				

REQUEST FOR PROPOSAL
Master System Integrator for Implementation of
Integrated Smart Solutions, under Smart City
Mission in Patna

Sr No	Solution / Component	Line Item (Component wise)	UoM	Indicative quantity	Proposed Quantity By Bidder As per His Assessment	Proposed Make & Model	Compliance to Specifications (Yes/No)	Reference to Supporting Document/Brochure
133	CCTV-Police Area	Supply and Underground laying of Cat 6 /cable in HDPE Pipe Including Digging, Piping Re-filling	Mtr	15000				
134	CCTV-Police Area	Workstation Desktop with three LED Monitors	No.	37				
135	CCTV-Police Area	IP Phone	No.	30				
136	CCTV-Police Area	HD LED Display (55 Inches)	No.	37				
137	CCTV-Police Area	8 Port PoE Ruggedized Switch	No.	30				
138	CCTV-Police Area	Split Air Conditioner 2 Ton (5-star energy efficiency rating)	No.	30				
139	CCTV-Police Area	Furniture (Table +Chair)	Pair	30				
140	CCTV-Railway	Outdoor Fixed Bullet Cameras	No.	390				
141	CCTV-Railway	Monitoring Desktop PC with one LED Monitor	No.	14				
142	CCTV-Railway	IP Phone	No.	6				
143	CCTV-Railway	HD LED Display (55 inches)	No.	14				
144	CCTV-Railway	Managed 24 Port L3 Edge Switches	No.	6				
145	CCTV-Railway	9U Racks with necessary accessories	No.	6				
146	CCTV-Railway	Split Air Conditioner 2 Ton (5-star energy efficiency rating)	No.	6				
147	CCTV-Railway	Online UPS (3 KVA with 2hrs backup)	No.	6				

REQUEST FOR PROPOSAL
Master System Integrator for Implementation of
Integrated Smart Solutions, under Smart City
Mission in Patna

Sr No	Solution / Component	Line Item (Component wise)	UoM	Indicative quantity	Proposed Quantity By Bidder As per His Assessment	Proposed Make & Model	Compliance to Specifications (Yes/No)	Reference to Supporting Document/Brochure
148	CCTV-Railway	Furniture (Table +Chair)	Pair	6				
149	CCTV-SP Office	HD LED Display (55 inches)	No.	4				
150	CCTV-SP Office	Monitoring Desktop PC with one LED Monitor	No.	4				
151	CCTV-SP Office	PTZ Joystick	No.	4				
152	CCTV-SP Office	Managed 24 Port L3 Edge Switches	No.	4				
153	CCTV-SP Office	9U Racks with necessary accessories	No.	4				
154	CCTV-SP Office	Split Air Conditioner 2 Ton (5-star energy efficiency rating)	No.	4				
155	CCTV-SP Office	Online UPS (3 KVA with 2hrs backup)	No.	4				
156	CCTV-SP Office	Furniture (Table + Chair)	Pair	4				
157	DC-Hardware	Link Load Balancer	No.	1				
158	DC-Security	AAA, Guest, Device Profiling for 25000 Concurrent Sessions	No.	1				
159	DC-Security	DLP	No.	250				
160	DC-Security	IDAM, SSLi, PAM, SSO	No.	1				
161	Data Centre Hardware	Backup Appliance with Backup Software	No.	1				
162	DC-Software	Mail & Messaging	No.	1				
163	Data Centre Hardware	Web Application Firewall (WAF)	No.	1				
164	Services	Project Implementation and Commissioning Cost till Go-Live	Specification Enclosed	1				

REQUEST FOR PROPOSAL
Master System Integrator for Implementation of
Integrated Smart Solutions, under Smart City
Mission in Patna

Sr No	Solution / Component	Line Item (Component wise)	UoM	Indicative quantity	Proposed Quantity By Bidder As per His Assessment	Proposed Make & Model	Compliance to Specifications (Yes/No)	Reference to Supporting Document/Brochure
165	Services	Program Management Cost during Go-Live, O&M period and Manpower as per SLA	Specification Enclosed	1				
166	Training Cost	Training Cost	Specification Enclosed	1				
167	Services	Integration with Existing System (Cloud Application, Various databases)	Specification Enclosed	1				
168	Services	Integration of Existing cameras with ICCV (Through edge gateway)	Specification Enclosed	1				
169	Data Centre Hardware	Network Intrusion Prevention System (NIPS) in HA (N+N)	Specification Enclosed	1				
170	Services	One time setting-up charges for 50 Mbps NLD link, 100 Mbps NLD link and 100 Mbps Internet link	Specification Enclosed	1				
171	Services	Billboards for poles	No.	500				
172	Services	TPA	Specification Enclosed	1				
173	Services	Penta scanning & VAPT	Specification Enclosed	1				

REQUEST FOR PROPOSAL
Master System Integrator for Implementation of
Integrated Smart Solutions, under Smart City
Mission in Patna

Sr No	Solution / Component	Line Item (Component wise)	UoM	Indicative quantity	Proposed Quantity By Bidder As per His Assessment	Proposed Make & Model	Compliance to Specifications (Yes/No)	Reference to Supporting Document/Brochure
174	Data Centre Hardware	Anti-Advance Persistent Threat (APT) in HA (N+N)	Specification Enclosed	1				
175	Data Centre Hardware	KVM Switch	No.	2				
176	Services	Endpoint Health Check for Existing Items	Specification Enclosed	1				
177	Additional Software	Video Summarization	50 Camera License	1				
178	Additional Software	Picture Intelligence Unit	1	1				

10.2. Annexure 2 : Floor Wise Layout for Final Building

This building will be constructed in an approximate time of 18 months. ICCC & DC along with the cabling and other accessories will be shifted to this building after that. Desired solution is based on this layout only.

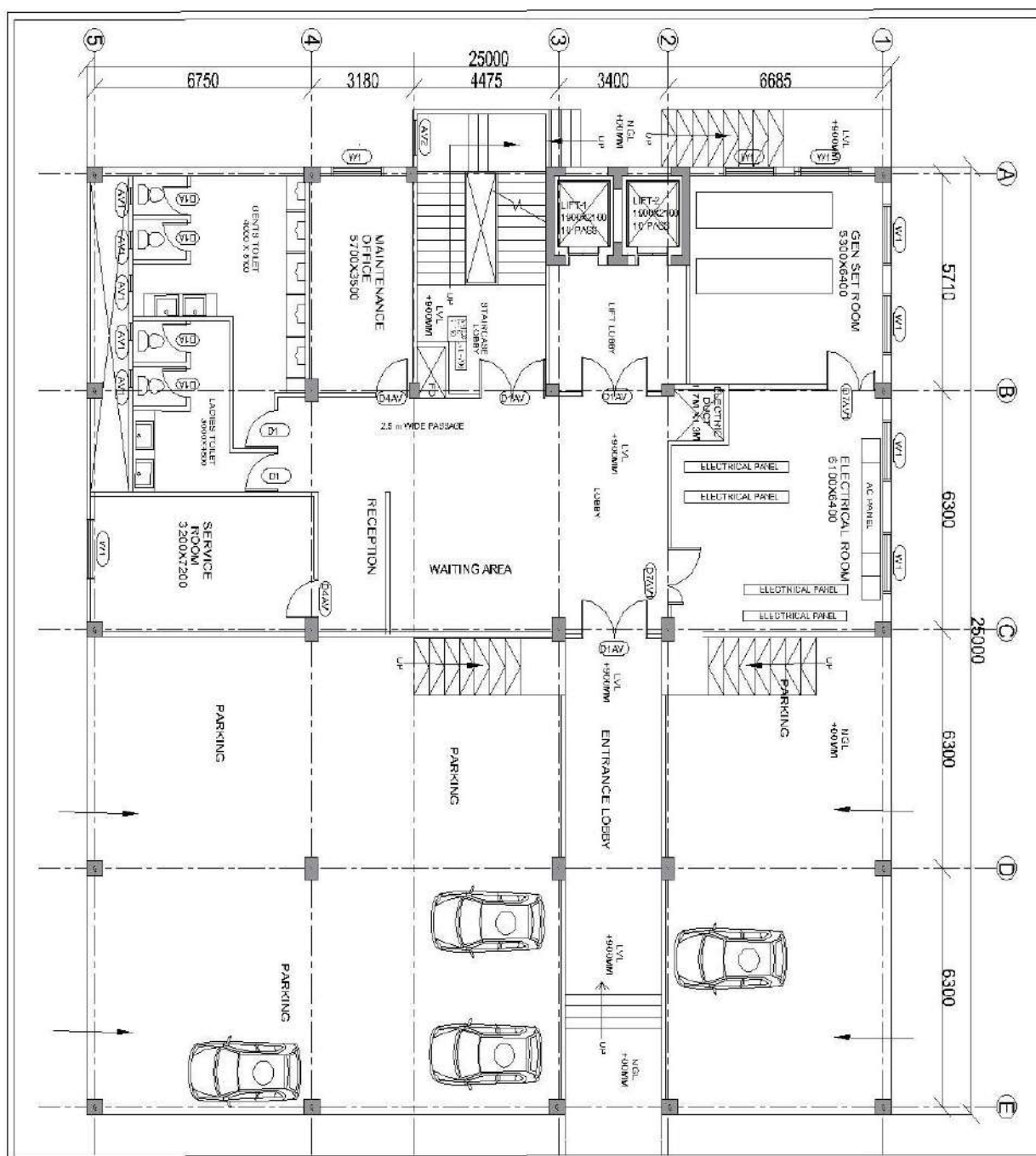
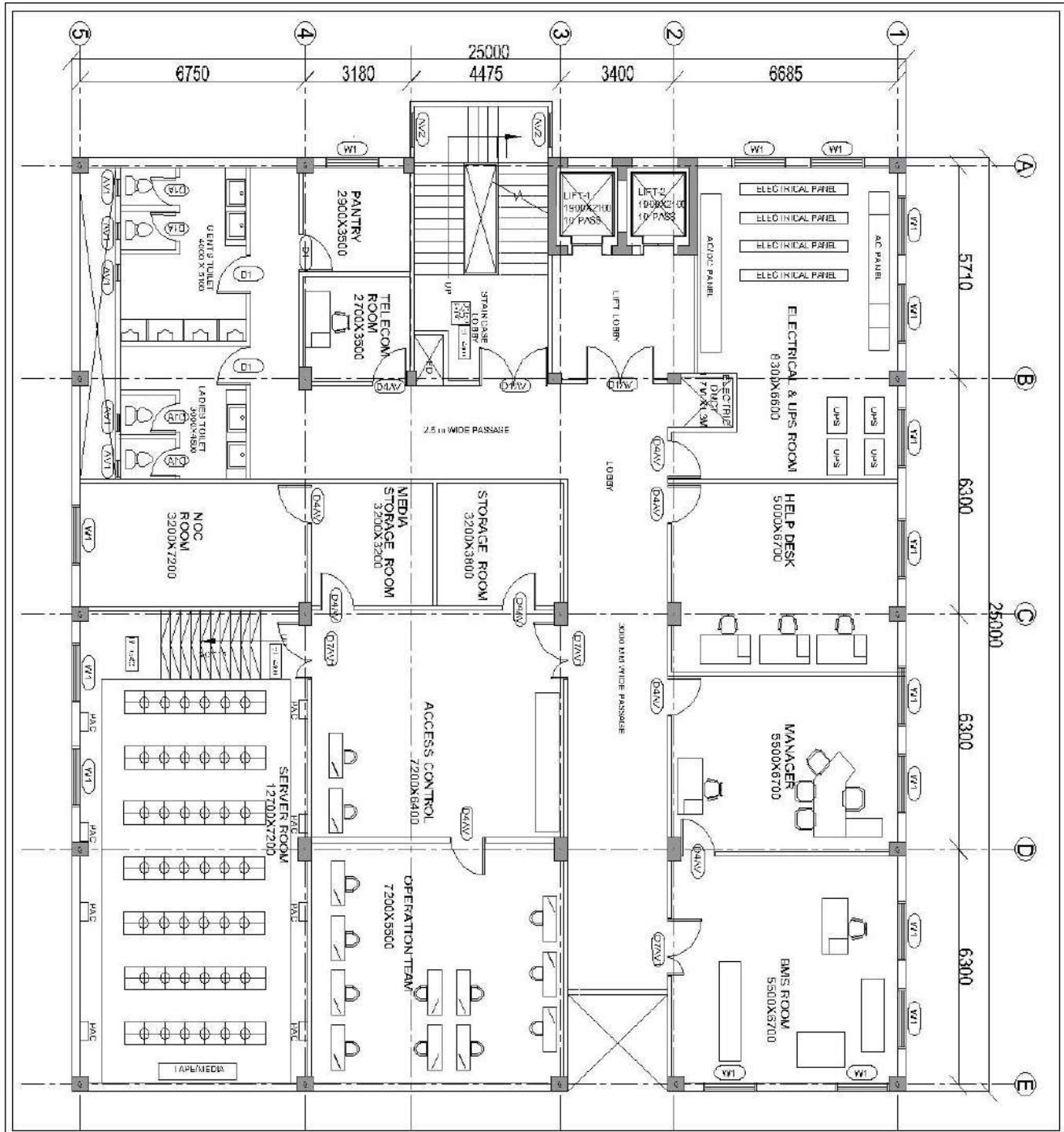


Figure 7 : Layout of Ground Floor at Final Building

Figure 8 : Layout of Floor-1 at Final Building



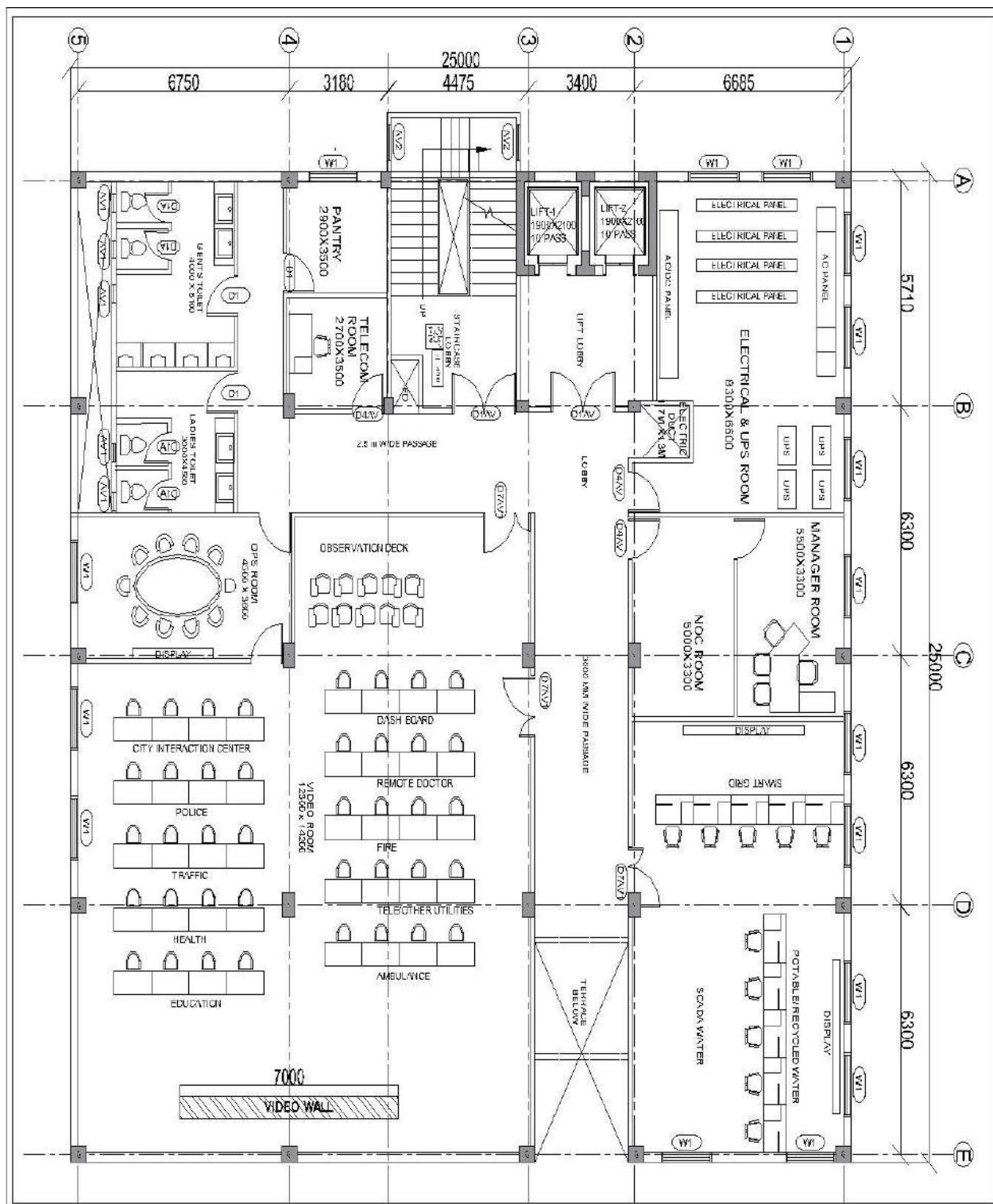


Figure 9 : Layout of Floor-2 at Final Building

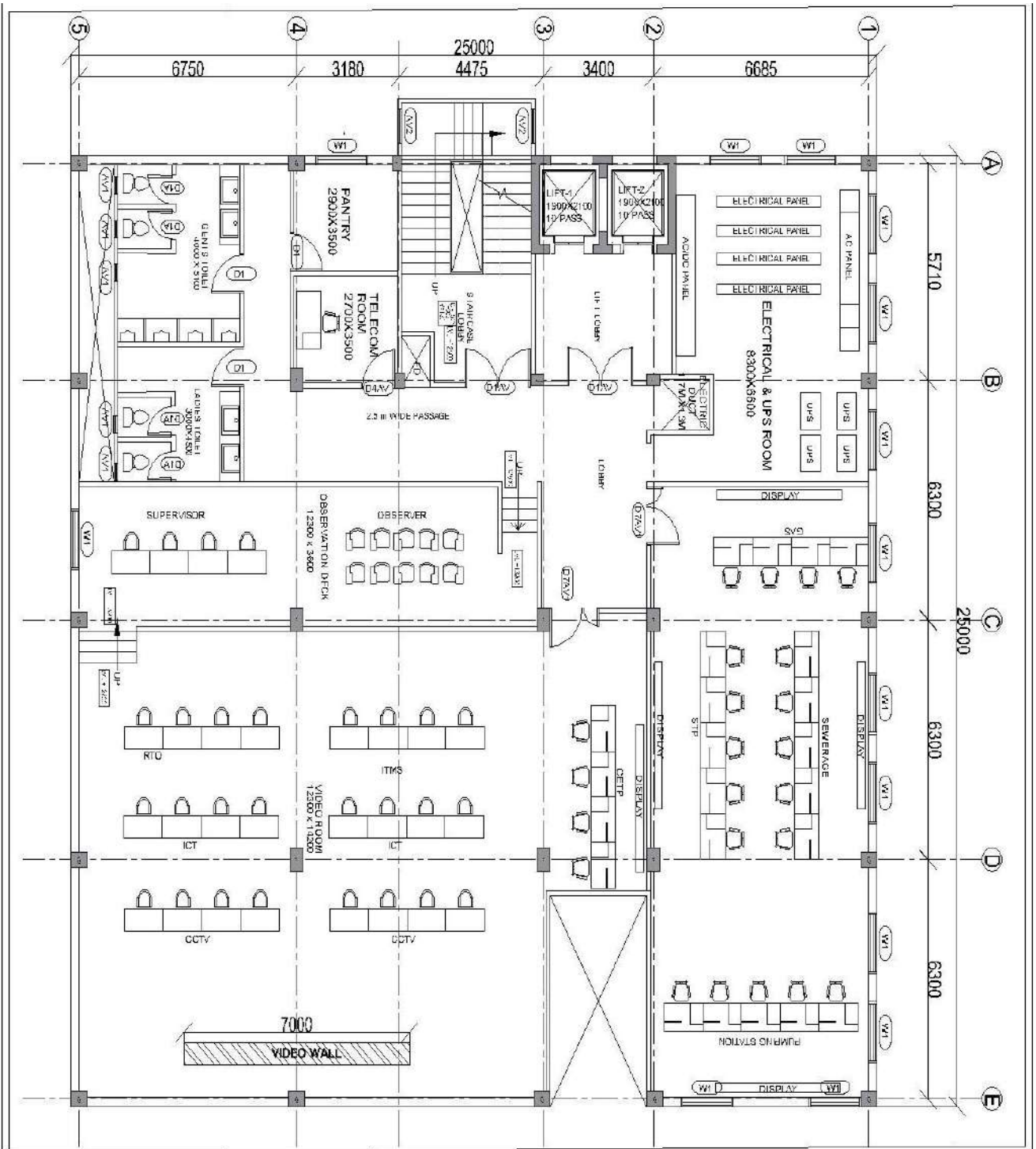


Figure 10 : Layout of Floor-3 at Final Building

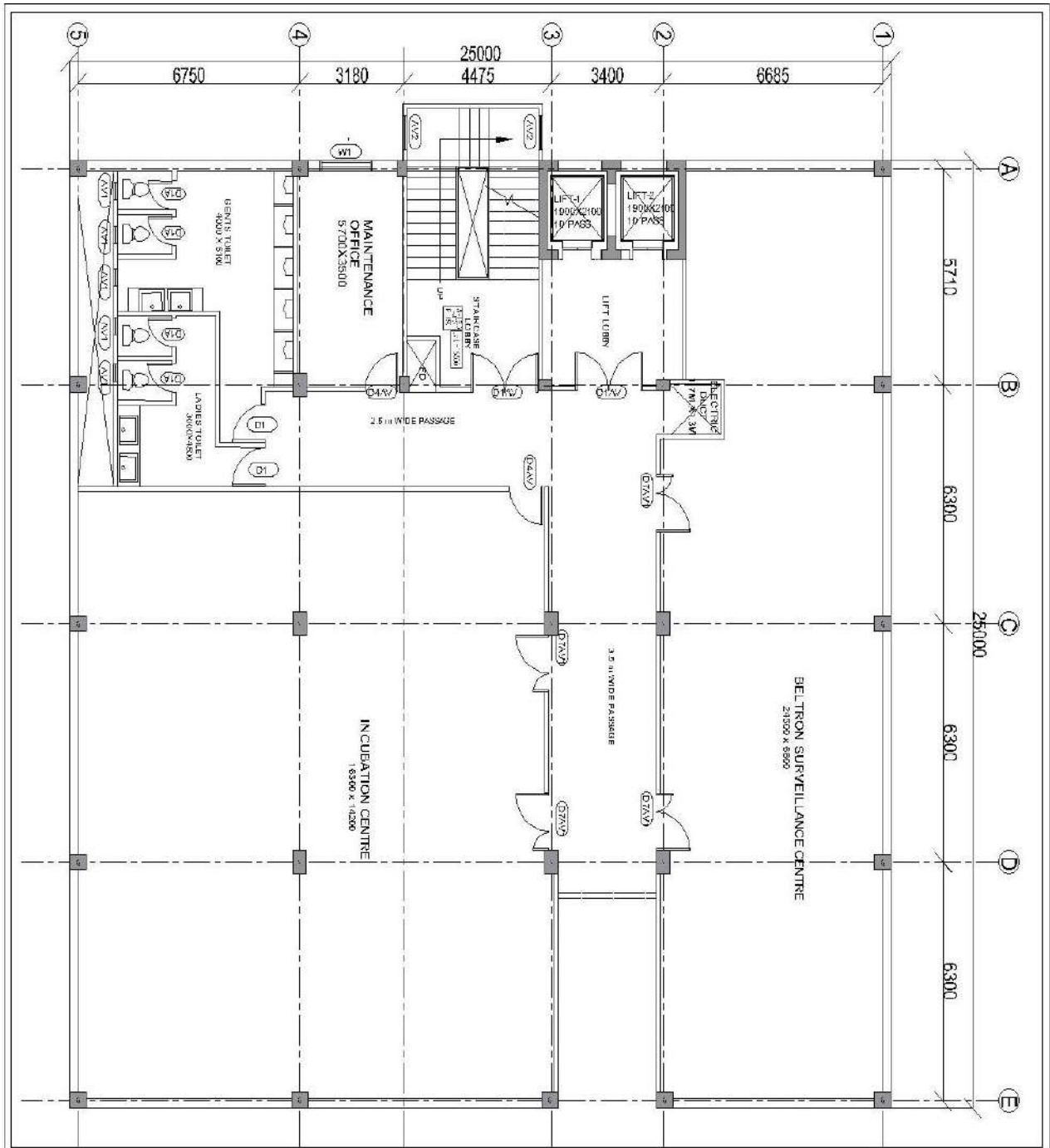


Figure 11 : Layout of Floor-4 at Final Building

10.3. Annexure 3 : Existing Wi-Fi Hotspots in City

S.No.	Wi-Fi Location	Qty. of Access Points
COLLEGE CAMPUS		
1	A N Sinha Institute of Social Sciences, Patna	12
2	A.N.College ,Patna	24
3	A.N.S. College, Barh	20
4	Aryabhatt Knowledge University, Patna	10
5	B.D.College ,Patna	10
6	B.S.College, Danapur	19
7	Bihar College of Physiotherapy & Occupational Therapy ,Patna	12
8	Bihar National College ,Patna	15
9	Bihar Veterinary College, Patna	19
10	BIT, Mesra, patna Campus	18
11	Central University of South Bihar ,Patna	12
12	Chanakya Law University ,Patna	77
13	Chandragupta Institute of Management, Patna	25
14	College of Arts & Craft ,Patna	9
15	College of Commerce ,Patna	33
16	G.J.College, Rambagh, Bihta	15
17	Government Sanskrit College, Kajipur, Patna	10
18	IIT ,Bihta,Patna	85
19	Indira Gandhi Institute of Medical Sciences ,Patna	55
20	J.D. Women's College,Patna	18
21	J.N.L.College, Khagaul	12
22	L.N.Mishra Institute, Patna	13
23	M.D.College, Naubatpur	14
24	M.M.College, Bikram	9
25	Magadh Mahila College ,Patna	12
26	Mahanth Keshaw Sanskrit College, Fathuha, Patna	5
27	Mahila College, Khagaul	9
28	Maulana Mazharul Haque Arabian and persian University, Patna	7
29	Nalanda Medical College ,Patna	19
30	Nalanda Open University, Patna	8
31	NIFT ,Patna	35
32	Nimbark Krishna Madhawanand Skt. College, Dhanamath, Patna	3
33	NIT ,Patna	PUT ON HOLD
34	Patna College ,Patna	15
35	Patna Law College ,Patna	14
36	Patna Medical College ,Patna	26
37	Patna Science College ,Patna	42
38	Patna Training College ,Patna	10
39	Patna University ,Patna	20
40	Patna Women's College ,Patna	PUT ON HOLD

41	Prabhu Nath College, Parsa	6
42	R.K.D. College ,Patna	11
43	R.L.S.Y. College, Bakhtiyarpur	14
44	R.P.M. College, Patna city	7
45	R.R.S. College, Mokamah	15
46	Raghavendra Sanskrit College, Taretpali, Naubatpur, Patna	6
47	S.G.G.S. college, Patna city	7
48	S.M.D. College, Punpun	10
49	Sanbals Gandhi Institute of Dairy Technology, Patna	12
50	Sri Arvind Mahila College ,Patna	14
51	T.P.S. College,Patna	14
52	Vanijya Mahavidayala ,Patna	6
53	Women's Training College ,Patna	6
54	A.S. College, Bikramganj	16
VASUDHA KENDRA (CSC)		
55	Rajiv Nagar	1
56	Kumhar Toli, Kankarbagh	1
57	Salimpur Ahra	1
58	West Boring Canal Road	1
59	Prithwipur	1
60	Beur More , Anishabad	1
61	Beur Vasudha Kendra , Anishabad	1
INSTALLED BY BSNL		
62	PATNA HIGH COURT	24
63	Dulhinbazar GBT	4
64	ZTE_Beldarichak	3
65	Ministry of Tourism_64_Bodhgaya	3

10.4. Annexure 4 : Existing Installed Adaptive Traffic Management System

Sr. No.	Junction Name	Junction No.	Mode	Camera Details		
				Detection Camera	Surveillance Camera	PTZ Camera
1	Dhanuki Mode Down	12	Adaptive	4	4	1
2	Kumhrar	19	Adaptive	4	4	1
3	Bhoothnath Mode	20	Adaptive	4	4	1
4	Kanti Factory	21	Adaptive	4	4	1
5	Rajendranagar Golamber (South) (Doctors Colony)	23	Adaptive	4	4	1
6	Malahi Pakadi	24	Adaptive	4	4	1
7	Thakurbadi chowk	30	Adaptive	4	4	1
8	Nala road more	31	Adaptive	4	4	1
9	Ramgulam Chowk	32	Adaptive	4	4	1
10	Bakarganj More	33	Adaptive	4	4	1
11	J P Golamber (4 Sides)	34	Adaptive	4	4	1
12	Kargil Chowk	35	Adaptive	4	4	1
13	Convent More	36	Adaptive	4	4	1
14	PMCH More	37	Adaptive	4	4	1
15	Engineering College more	38	Adaptive	4	4	1
16	Bhattacharya Chowk	41	Adaptive	4	4	1
17	SP Verma more	42	Adaptive	4	4	1
18	Dakbanglow Circle	43	Adaptive	4	4	1
19	Kotwali (T)	44	Adaptive	4	4	1
20	Voltas More	45	Adaptive	4	4	1
21	Incometax Golamber	46	Adaptive	4	4	1
22	Hartali More Chowraha	48	Adaptive	4	4	1
23	Punaichak New secretariat	49	Adaptive	4	4	1
24	IPS More	51	Adaptive	4	4	1
25	Rajvanshi Nagar more	52	Adaptive	4	4	1

26	Dumra Chowki (Sheikhpura More)	53	Adaptive	4	4	1
27	Ashiyana More	54	Adaptive	4	4	1
28	Jagdev Path	55	Adaptive	4	4	1
29	Gola Road	56	Adaptive	4	4	1
30	Saguna More	58	Adaptive	4	4	1
31	Beur More	61	Adaptive	4	4	1
32	Balmi Chowraha	63	Adaptive	4	4	1
33	Mithapur overbridge East	65	Adaptive	4	4	1
34	Mithapur overbridge West	66	Adaptive	4	4	1
35	Panchmandir Path (Naya Daroga rai Path)	69	Adaptive	4	4	1
36	Chitkohra Circle	71	Adaptive	4	4	1
37	Patel Golamber	72	Adaptive	4	4	1
38	Anishabad More	73	Adaptive	4	4	1
39	Adalatganj West	78	Adaptive	4	4	1
40	Mohini More	81	Adaptive	4	4	1
41	Boring Road chowraha	82	Adaptive	4	4	1
42	Pani Tanki more	83	Adaptive	4	4	1
43	Kurji More	84	Adaptive	4	4	1
44	Digha Ashiyana more	85	Adaptive	4	4	1
45	Rajapur Pul more	87	Adaptive	4	4	1
46	Buddha Colony Thana more	88	Adaptive	4	4	1
47	Golghar Tiraha	90	Adaptive	4	4	1
48	Children Park	91	Adaptive	4	4	1
49	Tapasya Complex	92	Adaptive	4	4	1
50	Airport North Gate	95	Adaptive	4	4	1
51	RPS More	98	Adaptive	4	4	1
52	Exhibition Road	99	Adaptive	4	4	1
				208	208	52

10.5. Annexure 5 : List of Sites for CCTV Surveillance at Police Station and Railway Station Area

Sr#	Type of Camera	Brief Specification	Quantity
1	Outdoor IP Fixed Bullet Camera	At Police Station Area	374
2	Outdoor PTZ Camera	At Police Station Area	292
3	Box Camera with External IR	At Police Station Area	134
4	Outdoor Fixed Bullet Camera	At Railway Station Area	390

List of Locations under various Police Station:

Sr No	Police Station	Location for City Surveillance
1	Gandhi Maidan Thana	G P Golumber
2	Gandhi Maidan Thana	Ramprit Dhramshala Pirmuhani
3	Gandhi Maidan Thana	Sam Nandan Tiraha Akaswani Corner
4	Gandhi Maidan Thana	Jamal Road
5	Gandhi Maidan Thana	Near CDA Building
6	Gandhi Maidan Thana	Railway Colony Hospital
7	Gandhi Maidan Thana	Near Jamal Road Post Office
8	Gandhi Maidan Thana	East Road of The Back Side Salimpur Ahara RBI
9	Gandhi Maidan Thana	IMAI Hall
10	Gandhi Maidan Thana	Coal Dipo at Pirmuhani Talab
11	Gandhi Maidan Thana	Bank Road Near Taramandal Hospital
12	Gandhi Maidan Thana	Anta Ghat Bikhs Bhawan
13	Gandhi Maidan Thana	Collectorate Patna + Infront Registration Office
14	Gandhi Maidan Thana	Salimpur Ahara Gali no. 5, Near Domkhana
15	Gandhi Maidan Thana	Near Anda Ghat Chamber of Commerce Office
16	Pirbahor Thana	Sabjibag
17	Pirbahor Thana	G M Road
18	Pirbahor Thana	Sotan Market
19	Pirbahor Thana	Makniya
20	Pirbahor Thana	B N College
21	Pirbahor Thana	Patna University

Sr No	Police Station	Location for City Surveillance
22	Pirbahor Thana	Bhavar Pokhor more
23	Pirbahor Thana	Langartoli Square
24	Pirbahor Thana	Kali Ghat
25	Pirbahor Thana	Krishna Ghat
26	Pirbahor Thana	Ramna Road
27	Pirbahor Thana	B M Das Road
28	Kadamkuan Thana	Mahuya Toli Sabji Bagh Entry
29	Kadamkuan Thana	Rajendra Nagar Road no 3 Corner
30	Kadamkuan Thana	Congress Maidan
31	Kadamkuan Thana	Mela Tanki road no. 6
32	Kadamkuan Thana	Modi Park
33	Kadamkuan Thana	Road no. 10 Mahamadrchowk Jain Mandir
34	Kadamkuan Thana	Lohanipur Bajrangbali Mandir Prithiraj chowk
35	Kadamkuan Thana	West Lohanipur Dr. Vijay Singh Gali
36	Kadamkuan Thana	Inter Road Debi Soni
37	Kadamkuan Thana	Lohar Gali
38	Kadamkuan Thana	Rajdhani Market Dariyapur Road
39	Kadamkuan Thana	Briyasthan
40	Kadamkuan Thana	Kazipur Naya Tola
41	Kadamkuan Thana	Kazipur Quarter
42	Kadamkuan Thana	Daldali More
43	Kadamkuan Thana	Rajendra Nagar Road No. 12
44	Kadamkuan Thana	Rajendra Nagar Road No. 11
45	Kadamkuan Thana	Maharana Pratap Bhawan
46	Kadamkuan Thana	Railway Hanter Asoke Gupta
47	Kadamkuan Thana	Nisha Debi mandir
48	Sachivalay Thana	TheTwo main gates at Echo park
49	Sachivalay Thana	The Main gate at Kendriya Bidyalaya
50	Sachivalay Thana	Besides Hartali Gate
51	Sachivalay Thana	Mangalesh Road Near Nibachan Office
52	Sachivalay Thana	25 No. Check Post
53	Sachivalay Thana	Jagjiban Golumber
54	Sachivalay Thana	Near Rajdhani Balika Golumber
55	Sachivalay Thana	Near IRO Block Square
56	Sri Krishnapuri Thana	The two gates at Children Park
57	Sri Krishnapuri Thana	The two gates at A N College
58	Sri Krishnapuri Thana	Outside at Cimag Coaching Centre
59	Sri Krishnapuri Thana	Mohini More
60	Sri Krishnapuri Thana	Panchmukhi Mandir
61	Sri Krishnapuri Thana	Near Rajapul
62	Gardanibagh Thana	The Main Gate at Chitkohora Kamla Naharu Girls High School
63	Gardanibagh Thana	Ambedkar Chowk
64	Gardanibagh Thana	Road no 21 Near the Church

Sr No	Police Station	Location for City Surveillance
65	Gardanibagh Thana	Road No 10 Panchmandir Talab
66	Gardanibagh Thana	Ramlakshhan Mahato Flat
67	Gardanibagh Thana	Gupta Complex near Durga Mandir
68	Gardanibagh Thana	Road No 01, near the Thana
69	Gardanibagh Thana	Near Anishabad Lal Mandir
70	Gardanibagh Thana	70 Feet
71	Gardanibagh Thana	Near Thakurbari Gate No. 16 Gardanibag
72	Gardanibagh Thana	Near B D Evening College
73	Gardanibagh Thana	Balmichowk more, Near the Market
74	Shastri Nagr Thana	Rajbanshi Nagar
75	Shastri Nagr Thana	Under the Big Bazar Fly over
76	Shastri Nagr Thana	Ashiyana More
77	Shastri Nagr Thana	Rabi Chowk
78	Shastri Nagr Thana	Ghandi Murti patelnager
79	Shastri Nagr Thana	IGIMS Gate
80	Shastri Nagr Thana	Rajbanshinagar Panchmukhi Human Mandir Gali
81	Shastri Nagr Thana	Punaichowk Pump House
82	Shastri Nagr Thana	Shivpuri Tala
83	Hawai Adda thana	Amukore More
84	Hawai Adda thana	Garmuchowk More
85	Hawai Adda thana	Jagdeo Path
86	Hawai Adda thana	Raja Bazar
87	Hawai Adda thana	Saikhpora More
88	Hawai Adda thana	Ashiyana BMP More
89	Hawai Adda thana	The Main Gate at B I Bhoshra
90	Jakkanpur Thana	Guriya Math
91	Jakkanpur Thana	Postal Park Chouraha
92	Jakkanpur Thana	Sipara pul Chandpur Bela
93	Jakkanpur Thana	Prakritik School - Jayprakas Nagar
94	Kankarbagh Thana	Sri Ram Hospital
95	Kankarbagh Thana	Patliputra Sport Club
96	Kankarbagh Thana	Gaytri Mandir
97	Kankarbagh Thana	Ashok nagar road no- 14 B
98	Kankarbagh Thana	F sector Sahnaj Beauty
99	Kankarbagh Thana	Raghunath Balika
100	Kankarbagh Thana	Tiwari Bechan Gali Churaha
101	Kankarbagh Thana	Manju Sinha Park
102	Kankarbagh Thana	RMS Colony Main Road
103	Kankarbagh Thana	Buddha Marg
104	Kankarbagh Thana	Panchsib Mandir
105	Kankarbagh Thana	Ashoknagar Dena Bank More
106	Kankarbagh Thana	Ramlakshhan path new baypass
107	Kankarbagh Thana	Clony More

Sr No	Police Station	Location for City Surveillance
108	Kankarbagh Thana	Near Durga mandir under Chiriyatal Pul
109	Kankarbagh Thana	Postal Park Square
110	Patrakar Nagar Thana	Main gate of Kandriy Vidyalaya
111	Patrakar Nagar Thana	Munna Chok
112	Patrakar Nagar Thana	Jaleshwer Mandir Road
113	Patrakar Nagar Thana	Malari pakri Hanuman Nagar Turning
114	Patrakar Nagar Thana	Besides South Golumber
115	Patrakar Nagar Thana	East 90 Feet New Baypass
116	Patrakar Nagar Thana	West 90 Feet New Baypass
117	Patrakar Nagar Thana	East Road at Kali Mandir
118	Patrakar Nagar Thana	Yogipur Nahra
119	Patrakar Nagar Thana	Ishwar Dayal Hospital
120	Patrakar Nagar Thana	Kali Mandir
121	Patrakar Nagar Thana	MIG Sector Park
122	Patrakar Nagar Thana	Big Horpital Choraha
123	Patrakar Nagar Thana	Infront of Thana
124	Ramkrishna Nagra Thana	Sabji Mandi
125	Ramkrishna Nagra Thana	Near Ramkrishna Nagar Bazar
126	Ramkrishna Nagra Thana	Near Jakriya pul
127	Ramkrishna Nagra Thana	Bhupatipur
128	Ramkrishna Nagra Thana	Besides Krishna Niketan school - Chakriyapur
129	Ramkrishna Nagra Thana	Bishop Scott School
130	Ramkrishna Nagra Thana	Sahpur More
131	Ramkrishna Nagra Thana	Nayachak
132	Alamganj Thana	West Gate at Guljarbagh Station Square
133	Alamganj Thana	Guljarbagh Tin Muhani
134	Alamganj Thana	Paschim Darwaja
135	Alamganj Thana	Belwarganj
136	Alamganj Thana	Bhadraghat More
137	Alamganj Thana	Laddu Akhara
138	Alamganj Thana	Minibazar
139	Alamganj Thana	Under the Kumrar Bridge
140	Alamganj Thana	Namuhiya More
141	Alamganj Thana	Under Agamkuwan ROB More
142	Alamganj Thana	Agamkuwan ROB near Tulsi Mndi More
143	Alamganj Thana	Biskoman Choraha Gaya Ghat Mare
144	Alamganj Thana	Danka Imli
145	Alamganj Thana	Gayghat South and Utri More
146	Alamganj Thana	Gurudwara Gayghat
147	Alamganj Thana	Jalla Roadway
148	Alamganj Thana	laddu Akhara more
149	Alamganj Thana	Maharajgunj More
150	Alamganj Thana	Mahaveer Ghat More - Turning Point

Sr No	Police Station	Location for City Surveillance
151	Alamganj Thana	Mehdigunj Near Gumti
152	Alamganj Thana	NMCH Kali Mandir - Terminal Point
153	Alamganj Thana	Polo Hospital More
154	Alamganj Thana	Samuchor ka Chouraha - Turning point
155	Alamganj Thana	Guljarbagh Gumtti
156	Agamkuan Thana	Back Side of Thana
157	Agamkuan Thana	Bhagwat Mandir More
158	Agamkuan Thana	Care Hospital
159	Agamkuan Thana	Kumhar Toli More
160	Agamkuan Thana	St Josheph School
161	Agamkuan Thana	Amarnath Mandir
162	Agamkuan Thana	Transport Nagar Gate 1
163	Agamkuan Thana	Transport Nagar Gate 2
164	Agamkuan Thana	Sonal Petrol Pump
165	Agamkuan Thana	Paramaunt Hospital
166	Agamkuan Thana	Bhooth Nath Road T.V Tower
167	Agamkuan Thana	DAV School
168	Agamkuan Thana	Zero Mile
169	Agamkuan Thana	Pahari More
170	Agamkuan Thana	Railway Over Bridge Near Sitala Mandir
171	Agamkuan Thana	Bhootnath Mahaveer Mandir
172	Agamkuan Thana	Gandhi Nagar More
173	Agamkuan Thana	Nandlal Chapra More
174	Khajekala Thana	Nun Square
175	Khajekala Thana	Nabab Bahadur Road
176	Khajekala Thana	Lodhi Katra
177	Khajekala Thana	Gobardhan Charaha
178	Khajekala Thana	Machharhatta
179	Khajekala Thana	Sadargali Square
180	Khajekala Thana	Nojar Katra
181	Khajekala Thana	Gurhatta More
182	Khajekala Thana	Mouri Gali
183	Khajekala Thana	Ranipur Khirki
184	Khajekala Thana	Sadar gali More
185	Khajekala Thana	Sadar Gali Tin Mohanai
186	Chowk Thana	Above ROB Near Tin Mohani
187	Chowk Thana	Chamria More
188	Chowk Thana	Chhoti Patan Devi , Hajigunj More
189	Chowk Thana	Chowk Thana More
190	Chowk Thana	Kanghat Ghat ,
191	Chowk Thana	kanghat Ghat Thana Residence
192	Chowk Thana	Kanya Mandir Keshab Rai Gali
193	Chowk Thana	Kila Ghat

Sr No	Police Station	Location for City Surveillance
194	Chowk Thana	Langur Gali
195	Chowk Thana	Mangal Talab More
196	Chowk Thana	Patna Saheb Out side
197	Chowk Thana	Purab Darwaza More
198	Chowk Thana	Chowk More
199	Chowk Thana	Hazipur Lakki Biscuit Factori More
200	Chowk Thana	Chowk Sikharpur Nala
201	Chowk Thana	Near Patna Sachib Station
202	Chowk Thana	Lodhi Katra More
203	Chowk Thana	Near Janta Hotel
204	Chowk Thana	East Gate at Mangal Talab
205	Malslami Thana	Guruka Bagh More
206	Malslami Thana	Katra Bazar Samity More
207	Malslami Thana	Nuruddinganj More Bhatti
208	Malslami Thana	Railway Crossing
209	Malslami Thana	Sahadra Ramdhani More
210	Malslami Thana	Malsalami Thana More
211	Malslami Thana	Dalhatta
212	Malslami Thana	Marufganj More Near Hanuman Mandir
213	Malslami Thana	State Bank More
214	Malslami Thana	Near Haldipatti Shankar Prasad
215	Malslami Thana	Railway Congress Patna Ghat
216	Malslami Thana	Near Nuraddinganj Charaha
217	Malslami Thana	Guru Ke Bag More
218	Malslami Thana	Katra Bazar Samati More
219	Sultanganj Thana	Banbari Chowk
220	Sultanganj Thana	BNR
221	Sultanganj Thana	Near Mahendra Post Office
222	Sultanganj Thana	Near The Thana
223	Sultanganj Thana	Pasthar Masjid -Dargaha
224	Danapur Thana	Saguna Danapur Cantt City Road
225	Danapur Thana	RPS More
226	Danapur Thana	Hatikhana More
227	Danapur Thana	Hospital More
228	Danapur Thana	Infront of the jail
229	Danapur Thana	Bibjang More
230	Danapur Thana	Auto Stand
231	Danapur Thana	Moda Toli More
232	Danapur Thana	Near registry Office
233	Danapur Thana	Near Takia Complex
234	Danapur Thana	Court More
235	Khagaul Thana	Gansayam Girls School - Besides New Colony
236	Khagaul Thana	DRM Office Chowk

Sr No	Police Station	Location for City Surveillance
237	Khagaul Thana	Moti chowk
238	Khagaul Thana	Khagul Lakh
239	Khagaul Thana	Jayram bazar
240	Rupaspur Thana	R Garden More - Ambedkar path
241	Rupaspur Thana	Infront of Sai Corporate Bhawan - Uppar place of RGB Square
242	Rupaspur Thana	Station Road Infront of Rupaspur Thana
243	Rupaspur Thana	Esan International Girls School
244	Rupaspur Thana	Under Rukanpura New Flyover Patliputra Station More
245	Rupaspur Thana	Nitibag Shayama Appartment
246	Rupaspur Thana	Gola Road, Sonu Market
247	Rupaspur Thana	RPS More
248	Kotwali Thana	Milar School
249	Kotwali Thana	Stations Golumber Buddha Park Corner
250	Kotwali Thana	Stations Golumber Pul Market
251	Kotwali Thana	EAST WEST GPO
252	Kotwali Thana	Station Road Chiriyatal Pul
253	Kotwali Thana	Ayakar Golumber Infront of Income tax Off
254	Kotwali Thana	Jamal Road and SP Verma Road Square
255	Kotwali Thana	Harding Road Phatak
256	Kotwali Thana	Daroga rai Road infront of the Bisesh Nigrani Hakai Mandir
257	Kotwali Thana	PNT Colony More
258	Kotwali Thana	The Backside road of Boring road and Womens College
259	Kotwali Thana	Infront Of Central Mall
260	Kotwali Thana	Near Mahalekhakar Bhawan Daroga Rai Path
261	Kotwali Thana	SBI Bank near PNT Colony in Kidwaipuri More
262	Kotwali Thana	East Gate at Taramandal
263	Phulwari Sharif Thana	Sahid Chowk
264	Phulwari Sharif Thana	Tamtam parab
265	Phulwari Sharif Thana	Pethiea Bazar
266	Phulwari Sharif Thana	Masjid Square
267	Phulwari Sharif Thana	Near Esopur Pul
268	Phulwari Sharif Thana	Near BMP Gate
269	Phulwari Sharif Thana	Near Mahabir Cancer Organization
270	Phulwari Sharif Thana	Khaja Hamli
271	Phulwari Sharif Thana	Ishopur nagar
272	Phulwari Sharif Thana	Fulwari Sarif High School Gate
273	Beur Thana	Near Beur Jail
274	Beur Thana	Near Sipara manmohak Street
275	Beur Thana	Gandhimurti Sipara Matkan
276	Beur Thana	Hansi Chok
277	Beur Thana	Inner side of Bayur more
278	Beur Thana	Under sipara pul
279	Beur Thana	Dorasta More

Sr No	Police Station	Location for City Surveillance
280	Beur Thana	IOC Gate
281	Beur Thana	Kulbaha Chok
282	Bahadurpur Thana	Near Sodhpur Hostel
283	Bahadurpur Thana	Sai Ch0wk
284	Bahadurpur Thana	Kali Mandir Nera Jhoparpatti
285	Bahadurpur Thana	Rajendra Nagar Road no 13B
286	Bahadurpur Thana	Ramkrisna Colony More
287	Bahadurpur Thana	Jay Mahabir Colony near shiv mandir
288	Bahadurpur Thana	Kumaharra Gumati North Side
289	Bahadurpur Thana	Sanichra More
290	Bahadurpur Thana	Sandalpur More
291	Bahadurpur Thana	Ramkrisna Mandir More
292	Bypass Thana	Karmali ch0wk State Bank More
293	Bypass Thana	Mathani Tal
294	Bypass Thana	Sati Churaha
295	Bypass Thana	Jagdeo Park
296	Bypass Thana	Mandai Chouraha
297	Digha Thana	Snt. Micle School (Senior Scc) Gate
298	Digha Thana	The Two Gate at IIT
299	Digha Thana	Digha Ghat
300	Digha Thana	Digha Ashiyana More
301	Digha Thana	St. Xavior College Gate
302	Digha Thana	Thana Gate
303	Digha Thana	Railway Bridge
304	Digha Thana	In the Bata Gate
305	Digha Thana	Ramjichowk Petrol Pump Gate
306	Digha Thana	Don Basco School Gate
307	Patliputra Thana	Indrapuri Railway Crossing
308	Patliputra Thana	GD Mishra Path More main Road
309	Patliputra Thana	Gosai Tola Main Road
310	Budha Colony Thana	Panchmukhi Hanuman Mandir Square
311	Budha Colony Thana	Golghar Square Near Police Line
312	Budha Colony Thana	Lady Steafence hall besides the Museum
313	Budha Colony Thana	Srikrishna Nagar
314	Budha Colony Thana	Basban Park
315	Budha Colony Thana	Santusti Gali More
316	Rajiv Nagar Thana	Near Jaiprakas Nala Tiraha
317	Rajiv Nagar Thana	In the tiraha on the turning of Gandhi Nagar, from Ramnagari Sector 4
318	Rajiv Nagar Thana	Near SBI on Rajivnagar Main Road
319	Rajiv Nagar Thana	Near Mahima Mandir
320	Rajiv Nagar Thana	Near Ramnagari More
321	Phulwari Thana	AIIMS Entry

List of location for ANPR Box Camera :

Sl. #	ANPR Camera Location	No of ANPR Box Cameras
1	Dhanuki More	4
2	Nandlal Chapra	12
3	Karbigahiya Fly Over	4
4	Saguna More	4
5	Kanti Factory More	4
6	Kurji More	4
7	R Block More	8
8	Patna Hawaii Adda More	6
9	Dumra Chouki	4
10	Anishabad More	12
11	Dakbanglow Chauraha	2
12	New Sachiwalay Punai Chak	8
13	Poltacnic More	4
14	Income Tax Gloumber	6
15	Budhha marg	6
16	Gandhi Maidan	4
17	A N College	7
18	S P Verma Road	6
19	City Chaouk	3
20	Patna College	4
21	Malahi pakri More	4
22	Mc Dowel Golumber Rajender Nagar	2
23	S P Verma Road	4
24	Patna Zoo 1	4
25	Gayghat Patna City	8
Total		134

List of Railway Stations to be covered under CCTV Surveillance :

Sl. #	Area Around Railway Stations	IP Bullet Camera
1	Patna Juction	125
2	Rajendra Nagar	77
3	Patna Shaib	58
4	Guljarbag	13
5	Danapur	65
6	Patliputra	52
Total Cameras		390

10.6. Annexure 6 : Existing Installed Camera for City Surveillance under DIAL 100

S. No.	Camera Type	Indicative no. of locations
1	PTZ Camera (including Critical Locations)	35
2	FIXED Camera (including Critical Locations)	45
3	ANPR Camera (including Critical Locations)	32

Existing installed Camera for City Surveillance :

Sr. #	Location for City Surveillance	PTZ Camera	Fixed Camera	Total
1	Dakbangla Chouraha(Traffic post)	1		1
2	Station Golamber	1		1
3	Station Golamber Beside Temple (Flower market)		1	1
4	Meethapur Mandi road	1		1
5	G. P. O. East		1	1
6	G. P. O. East		1	1
7	G. P. O. West		1	1
8	Moryalok Parisar gate - opp Kotwali Thana	1		1
9	Bakarganj Police Post (Model Thana) east & north		1	1
10	Moryalok Parisar gate -Intermediate Council	1		1
11	Gandhi Maidan VIP gate ke samne	1		1
12	Gandhi Maidan (Viskoman IOB bank building)		1	1
13	Gandhi Maidan (Kargil chock)	1		1
14	Gandhi Maidan (Ramgulam chock)	1		1
15	Childrens Park Gandhi Maidan		1	1
16	Exhibition Road Chouraha	1		1
17	New sachivalay gate choki no 28.	1		1
18	Boring Road Pani Tanki		1	1
19	Boring Road Pani Tanki		1	1
20	Aaykar Golamber		1	1
21	Vishvesariya bhawan		1	1
22	Chidiyakhana G.no. 1 (Baily Road)	1		1
23	Anisabad Chock	1		1
24	Patna Womens College		1	1
25	Patna Womens College		1	1
26	Boring Road Chouraha (North) Sahara.	1		1
27	Boring Road Chouraha (South) Red Light. Sk Puri	1		1
28	Hanuman Mandir Baily Road		1	1
29	Hanuman Mandir Baily Road		1	1

Sr. #	Location for City Surveillance	PTZ Camera	Fixed Camera	Total
30	Phulwarisharif Thana Shahid Chock - Golamber	1		1
31	Dumra Police Chocki	1		1
32	Mahendru Chouraha	1		1
33	Patna College (NIT Mod)	1		1
34	Bhikna Pahari		1	1
35	Bhikna Pahari		1	1
36	Airport Bhawan 1		1	1
37	Airport Bhawan 2.		1	1
38	Chidiyakhana G.no. 2		1	1
39	Chidiyakhana G.no. 2		1	1
40	Vidhan Sabha - SAPTMURTI.	1		1
41	Karpuri golamber	1		1
42	Rajendra Chock Golamber (Rajbhavan)		1	1
43	Rajendra Chock Golamber (Rajbhavan)		1	1
44	Rajendra Chock Golamber (CM House)		1	1
45	Karbhigiya Station		1	1
46	Sichai Bhawan		1	1
47	Gaighat	1		1
48	Danka Imli Chouraha		1	1
49	Viskoman chouraha -Gaighat		1	1
50	Viskoman chouraha -Gaighat		1	1
51	Zero Mile	1		1
52	Pahari Mod		1	1
53	Pahari Mod		1	1
54	Gulzarbagh station Chouraha	1		1
55	Nun ka chouraha	1		1
56	Guru GobindSingh Chouraha	1		1
57	Dhanuki Mod		1	1
58	Dhanuki Mod		1	1
59	Purab Darwaja city chock	1		1
60	Patthar ki masjid		1	1
61	Didar Gang	1		1
62	Thakurbadi Rosi Sweets	1		1
63	Rajender Nagar terminal (front gate at road).		1	1
64	Rajender Nagar terminal (front gate at road).		1	1
65	Rajendra Nagar Pul South Golamber	1		1
66	Tempo Stand Kankarbagh	1		1
67	RajenderNagar Station gate opp commerce coll	1		1
68	Kanti Factory Mod		1	1
69	Kanti Factory Mod		1	1

Sr. #	Location for City Surveillance	PTZ Camera	Fixed Camera	Total
70	Bhoothnaath Mod		1	1
71	Bhoothnaath Mod		1	1
72	Rajendra Nagar North Golamber	1		1
73	Sipara Gumti		1	1
74	Sipara Gumti		1	1
75	Raja pur pul-1		1	1
76	Raja pur pul-1		1	1
77	Bibi Gang Chowki Danapur		1	1
78	Thakurbadi Rosi Sweets	1		1
		35	45	80

Existing installed ANPR location:

S.No	ANPR Location	Camera Lanes
1	Rukanpura Fly over (Rukanpura flyover, Patna, Bihar, India)	3
2	Fulwarisharif AIIMS (NOLSA, Muhammadpur Korji, BR 801105)	2
3	Sipara Gumti (railway crossing) near Fatuah Marg bypass road.. Patna.	2
4	Rajapur Pul ke end par	3
5	ChiraiyaaTad Pul	3
6	Rajendra Nagar Pul	6
7	90 Feet Road - Kali mandir road, T point.	2
8	GaiGhat	2
9	Gandhi Setu	3
10	Zero Mile	3
11	Meetha pur Bus stand road &bypass T point.	3
	Total	32

10.7. Annexure 7 : Existing Locations of Installed cameras for Patna Police on PPP Mode

Sr. #	Camera Type	Indicative no. of locations
1	PTZ Camera (including Critical Locations)	54
2	FIXED Camera (including Critical Locations)	49

Existing Location of CCTV Surveillance from Patna Police under PPP

Sr. #	Location for City Surveillance	PTZ Camera	Fixed Camera
1	Patna Junction, East	1	
2	Hadtali more (East)	1	
3	Hadtali more (West)	1	
4	Chiraiyatad Pul, Exhibition Road Trijunction		1
5	Mithapur Karbigahiya Park	1	
6	Gola Road, Near Petrol Pump		1
7	Boring road Chouraha, Sumati Palace (Nageswar Colony More)		1
8	Postal Park, Kankarbagh (Middle of chiryatad overbridge)		1
9	Old Bypass (R.Nagar ROB)	1	
10	Zoo, Bailey Road	1	
11	Boring Canal Road (Guinee Motors)		1
12	Patliputra Golamber	1	
13	Engg. College More , Ashok Raj Path	1	
14	Tandoor Hut, Fraser Road	1	
15	Boring Canal Road (Reliance Trends)		1
16	Malahi Pakhri More	1	
17	Kargil Chowk	1	
18	Veer Chand Patel Path, Party Karyalya	1	
19	Budha Smriti Park near Patna Junction		1
20	Chidren Park, Gandhi Maidan		1
21	Shubhash Park, Gandhi Maidan	1	
22	IGIMS, Bailey Road (UP)		1
23	IGIMS, Bailey Road (DOWN)		1
24	Colony More, Kankarbagh		1
25	Income Tax, East	1	
26	Police Office,Gandhi maidan	1	
27	Boring Road Chouraha	1	
28	Vishal Mega Mart, Fraser Road		1

Sr. #	Location for City Surveillance	PTZ Camera	Fixed Camera
29	Biscoman Bhawan (SBI, Chajju Bagh)	1	
30	Adarsh Thana (South Gandhi Maidan)		1
31	S.P Verma Road	1	
32	Ashok Cinema Flyover	1	
33	Kotwali Police Station	1	
34	Tripolia		1
35	Rukanpura, Bailey Road		1
36	Kumhrar Park	1	
37	Gola Road (Opp.Petrol Pump)		1
38	Pir muhani		1
39	Opp. Big Bazar, Exhibition Road, East Flag		1
40	Shalimar Sweets,Kankarbagh		1
41	Golghar		1
42	Bhattacharya more	1	
43	Baripath Nala Road Trijunction	1	
44	Agamkuawa Flyover Turning, Dhanuki More	1	
45	Budhmurti, Kadamkuwa (Near Apsara Hotel)		1
46	Exhibition Road, West Flag (Front of Big Bazaar)		1
47	Thakurbadi Road	1	
48	Prem Chand Golamber	1	
49	S.K puri (Police Check post)		1
50	Middle of Kanti NMCH	1	
51	Anisabad golamber	1	
52	New Market, Station Road		1
53	Bhootnath Dominos More		1
54	Bikaner Sweets, SK Puri		1
55	Patna Museum		1
56	Mc Dowells Golamber		1
57	Ramnagari More (Ashiana-Digha Road)	1	
58	Dinkar Golambar		1
59	Kankarbagh (Chiryatar Overbridge End)		1
60	Bhikhna Pahari (B.M.Das Road)	1	
61	Kendriya Vidhyalya, Kankarbagh		1
62	Munna Chak	1	
63	Rajendra Nagar Overbridge		1
64	Karbigahiya-mithapur Turning		1
65	Hanuman Nagar More		1
66	Dominos Pizza, Kankarbagh		1
67	Panch Shiv Mandir Infront		1
68	Bhootnath Road, Shani Mandir		1

Sr. #	Location for City Surveillance	PTZ Camera	Fixed Camera
69	Bajar Samiti 1		1
70	Bazar Samiti 2		1
71	New Police Line	1	
72	Passport Office (Ashiana-Digha Road)		1
73	Tempo Stand, Kankarbagh	1	
74	Rajendra Nagar Sabji Mandi		1
75	Manpura Pul		1
76	Khanjachi Road		1
77	Machua Toli	1	
78	Bakerganj More	1	
79	Buddha Colony PS, Bans Ghat	1	
80	Khetan Market	1	
81	P&M Mall	1	
82	Patna Market, Ashok Raj Path		1
83	Nala Road, Hanumaan Mandir	1	
84	IPS MESS	1	
85	Mc. Dowel Golamber PTZ	1	
86	Gandhi Setu End PTZ	1	
87	90' Bypass PTZ	1	
88	Exhibition Road PTZ	1	
89	Mithapur Bus Stand PTZ	1	
90	Dakbanglow PTZ	1	
91	Gandhi Setu Pillar 46		1
92	Chitkohara Goloumber		1
93	Gandhi Maidan Thana	1	
94	Sai Mandir Patliputra		1
95	Pirbohar Thana	1	
96	Kurji More	1	
97	Beaur More	1	
98	Saguna More	1	
99	High Court More	1	
100	Income Tax Golamber West	1	
101	Jagdeo path		1
102	Jagdeo Path Big Bazar		1
103	Jagdeo Path, Tanishq	1	
		54	49

10.8. Annexure 8 : Existing VASUDHA CENTRES in Pan City

S. No.	Block	Locality	No. of VLEs
1	Phulwari	Anishabad	4
2	Patna Sadar	Bakarganj	1
3	Phulwari	Beur	2
4	Patna Sadar	Bhootnath Road	1
5	Patna Sadar	Birla Colony	1
6	Patna Sadar	Boring Road	1
7	Patna Sadar	Patna city	4
8	Patna Sadar	Quaseem Colony	1
9	Danapur	Danapur	7
10	Danapur	Digha	1
11	Patna Sadar	East Boring Canal Road	1
12	Patna Sadar	West Boring Canal Road	2
13	Patna Sadar	Ram Krishna Nagar	3
14	Danapur	Gola Road	2
15	Patna Sadar	Hanuman Nagar	2
16	Patna Sadar	Jaganpura	2
17	Patna Sadar	Karbigahiya	1
18	Patna Sadar	Kumhartoli	1
19	Patna Sadar	Kumhrar	1
20	Patna Sadar	Langartoli	1
21	Patna Sadar	Lodipur	1
22	Patna Sadar	Mahatma Gandhi Nagar	1
23	Patna Sadar	Mahesh Pur	1
24	Patna Sadar	Mithapur	3
25	Patna Sadar	Marchhi Road	1
26	Patna Sadar	Nandgola Malsalami	1
27	Patna Sadar	Saristabad	1
28	Patna Sadar	Nehrutola	1
29	Patna Sadar	Pragati Nagar	1
30	Patna Sadar	Rajiv Nagar	1
31	Patna Sadar	Ramnagar, Bangalitola	1
32	Patna Sadar	Rukanpura	1
33	Patna Sadar	Machhuatoli	1
34	Patna Sadar	Kadam Kuan	2
35	Patna Sadar	South Mandiri	2
36	Patna Sadar	Ashok Rajpath	1
37	Patna Sadar	Patliputra	1
38	Patna Sadar	Gandhi Maidan	1
39	Patna Sadar	Patel Nagar	1
40	Patna Sadar	Ashiyana	2
41	Patna Sadar	Fraser Road	1
42	Patna Sadar	Police Line	1
43	Patna Sadar	Kurji	1
44	Patna Sadar	Rajapur	1
45	Patna Sadar	Budha Colony	1
46	Patna Sadar	Jagdev Path	1

47	Danapur	Nasriganj	1
48	Patna Sadar	Mahendru	1
49	Patna Sadar	Kankarbag	2
50	Patna Sadar	Postel Park	1
51	Danapur	Lekhanagar	1
52	Phulwari	Phulwari	4
53	Danapur	Khagaul	1
			81

10.9. Annexure 9 : Services being offered by VASUDHA CENTRE

S. No.	Services Portfolio
G2C Services (Government to Citizen Services)	
1	Pan Card Services
2	Passport Services
3	e-Aadhar (UID) card Services
4	FSSAI services
5	Banking Services – Financial Inclusion/Business correspondent services
6	Jeevan Praman Patra (For Pensioners) and PFRDA (Pension Fund services)
7	NIELIT Services(DOEACC)
8	NIOS Services (National Institute of Open School)
9	IRCTC services (Rail Ticket booking)
10	Electoral Services
B2C services	
1	Mobile and DTH Services
2	Skill Development Services
3	Insurance Services
4	Travel Services
5	Apollo Tele Health
6	Income Tax filing
7	Order Devices from CSCs
8	E-Pashu Chikitsha
9	LED KIT

10.10. Annexure 10 : IT Infrastructure Installed in existing Bihar State Data Center

S. No.	Description	Qty.
INSTALLED SERVERS		
1	DATABASE SERVER	5
2	APPLICATION SERVER	5
3	WEB SERVER	4
4	BACK UP SERVER	1
5	DIRECTORY SERVER	2
6	MANAGEMNET SERVER	1
7	EMS SERVER	8
INSTALLED NETWORK EQUIPMENTS		
8	Internet Router	2
9	Core Switch	2
10	Application Switch(24 Port)	4
11	Application Switch(48 Port)	4
12	External Firewall	2
13	Internal Firewall	2
14	Server Load Balancer	5
15	NIPS	2
16	Web Gateway	2
17	Messaging Gateway	2
INSTALLED STORAGE AND BACKUP EQUIPMENTS		
18	SAN Storage	2
19	SAN Switch	2
20	VTL	1
21	Autoloader	2
22	EML Series	1

10.11. Annexure 31 : Application Hosted on existing State Data Center

S. No.	Department	Name of Application	URL
1	Directorate of Provident Fund, GoB	eGPF Management system (Intranet Application)	Intranet
2		eGPF Portal	e-gpf.bihar.gov.in
3		e-Receipt	e-receipt.bihar.gov.in
4			
5	State Welfare Department	BC/EBC Application	http://bcebcwelfare.bihar.gov.in/
6		SC&ST Application	http://mahadalitmission.bihar.gov.in/
7	Department of Industries	Udyog Samwad	http://udyog.bihar.gov.in/
8		Startup Bihar	http://www.startup.bihar.gov.in/
9	State Health Society	ASHA Web Portal	http://192.168.21.125:8081/index.html
10		DHIS-2 Web Portal	http://bihardhis.nhsrhc-hmis.org/
11		HR Job Application	http://164.100.130.11:8081/
12		HRIS Web Portal	http://healthhrisbihar.org/
13		SHSB Website, Portal & Application	Not Applicable

REQUEST FOR PROPOSAL
Master System Integrator for Implementation of
Integrated Smart Solutions, under Smart City
Mission in Patna

14	Urban Development & Housing Department	e-Municipality e-Gov Solution	https://nagarseva.bihar.gov.in/
15		Urban Development & Housing Department	http://urban.bih.nic.in/
16	DIT	e-Office	https://eoffice.bihar.gov.in/
17		e-Office Demo	https://eofficedemo.bihar.gov.in/
18	Department of Social Welfare	Web Portal	ipSlcds.bihar.gov.in
19	State Election Commission	Website	http://sec.bihar.gov.in
20	Bihar State Films Development & Finance Co. Ltd.	BSFDFC	http://film.bihar.gov.in
21	P&D	Student Credit Card	http://7nishchay-yuvaupmission.bihar.gov.in/
22	Cabinet Secretariat	Loksamvad	http://www.loksamvad.bihar.gov.in
23	BSNL(Inspectorate for Prison & Correctional Services, GoB)	Prison Calling	URL not assigned
24	High Court	Patna High Court	http://patnahighcourt.gov.in/
25	BSEDC	SDC Private Cloud	https://cloud.bihar.gov.in/
26	L&T	Wi-Fi	Campus-Wifi.bihar.gov.in
27	Finance Department	CFMS	e-nidhi.bihar.gov.in

10.12. Annexure 42 : Application Hosted on existing State Data Center Cloud Platform

S. No.	Department	URL
1	IT Department	dit.bihar.gov.in
2	Food & Consumer Protection Dept	ePDS.bihar.gov.in
3	Home Department	home.bihar.gov.in
4	Bihar State Electronic Development Corporation Ltd.	www.bsedc.bihar.gov.in
5	State Appellate Authority	stateappellateauthority.bihar.gov.in
6	Public Health & Sanitation Mission	nnp.bihar.gov.in
7	Election Department (E.R.M.S., Office of Chief Electoral Officer, Bihar)	ceo.bihar.gov.in
8	Election Department	ele.bihar.gov.in
9	Department of Industries	lokshikayat.bihar.gov.in
10	Finance Department	nbfc.bihar.gov.in
11	Bihar Public Service Commission Department (BPSC)	onlinebpsc.bihar.gov.in
12	CM Secretariat	www.dashboard.bihar.gov.in
13		cm.bihar.gov.in
14		cmsonline.bihar.gov.in
15		cmsmoodle.bihar.gov.in
16	BCECE Board	bceceboard.bihar.gov.in

10.13. Annexure 53 : IT & Non IT Equipments in existing State Data Center

S. No.	Description	Model	QTY.
1	DESKTOP PC	HP-PRO-XL80	13
2	HONEYWELL SOFTWARE	EBI R410.2	1
3	BACnet IP NETWORK CONTROLLER	CP-IPC	1
4	BACnet MSTP NETWORK CONTROLLER	CP-SPC	3
5	ACCESS CONTROL PANEL	TEMALINE	1
6	SMART CARD READER	R-10	15
7	BIOMETRIC FINGER PRINT	V-SMART	1
8	EXIST SWITCHES	CABTREE	4
9	16-CHANNEL VIDEO DVR	HD-DVR-1016	1
10	29" COLOR MONITOR	SAMSUNG	1
11	42" LCD MONITOR	42CS560.ATR	1
12	DOME CAMERA (CCTV)	HDC-890P-36	16
13	FIRE TONE GENERATOR PAS	BOSCH	1
14	GOOSENECK MICROPHONE	LBB 1956/00	1
15	CELLING MOUNT SPEAKER	LBC 3099/41	12
16	WATER LEAK DETECTION PANEL	JAYFIRE	1
17	WATER LEAK DETECTION SENSOR	WD-CS	8
18	RODENT REPELANT MASTER CONSOL	VHFO	3
19	RODENT REPELANT SATELITE UNITS	MASER	32
20	P & T TELEPHONE	BSNL LANDLINE	1
21	DIGITAL EPABX SYSTEM	SIGMA INDX	1
22	DIGITAL TELEPHONE	BPL	20
23	CAC (1.5 TR)	3HW18VB	2

24	CAC (2 TR)	3HW24SVB	14
25	PAC (12 TR)	Pex 2045 EC	8
26	20KVA UPS	EMERSON	2
27	300KVA UPS	EMERSON	2
28	BATTERY BREAKER	STANDARD	1
29	320KVA DG	KIRLOSKER	3
30	ELECTRICAL PANEL	STANDARD	5
31	TEMP CUM HUMIDITY SENSOR	GREYSTONE	6
32	FIRE GAS RELEASE PANEL	RE120GR	2
33	FIRE GAS CYLINDER	NOVEC-1230	2
34	5 KG ABC TYPE FIRE EXTINGUISHER	FIRE SHIELD	9
35	VESDA	8100	1
36	FIRE ALARM SYSTEM PANEL	MS-9200UDLS(E)	1
37	SMOKE DETECTOR	SD 355	58
38	HEAT DETECTOR	H355	6
39	RESPONSE INDICATOR	REPUTED	25
40	ADDRESSABLE CONTROL MODULES	CMF 300	20
41	ADDRESSABLE MONITOR MODULES	MMF 300	10
42	MANUAL PULL STATION	BG-12LX	3
43	ELECTRONIC STROBE CUM HOOTER	MHR/MHW	5
44	SERVER RACK	CYBER RACK 36U	1
45	20KVA UPS BATTERY (12V)	EXIDE (12V-65AH)	1
46	300 KVA UPS BATTERY(2V)	UNISAFE(2V-1000AH)	1
47	LAPTOP	N.A.	5
48	PRINTER	N.A.	1
49	SWITCH	N.A.	2
50	LAN SWITCH	N.A.	1
51	REMOTE CONTROL OF CAC	N.A.	5
52	EARTH PIT	N.A.	17

10.14. Annexure 64 : Block Diagram of existing BSWAN Network

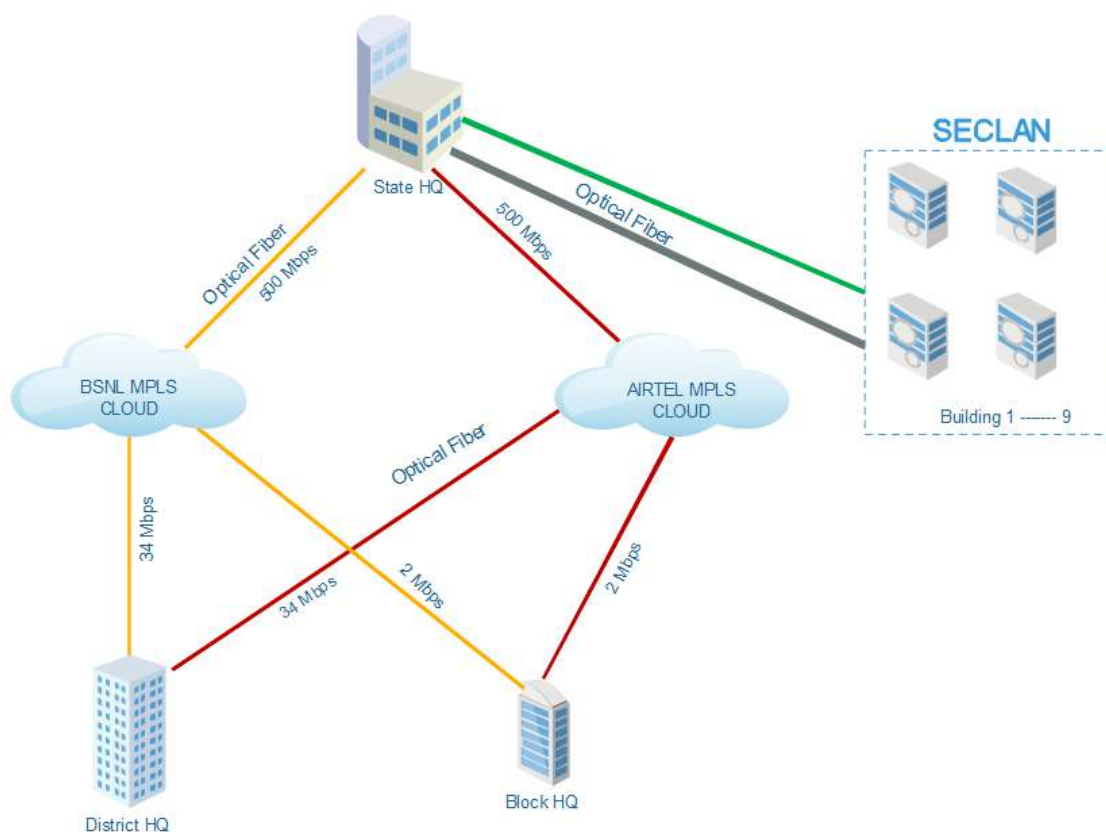


Figure 122 : Block Diagram of BSWAN Network

10.15. Annexure 75: Existing e-Governance Services offered by e-Municipality

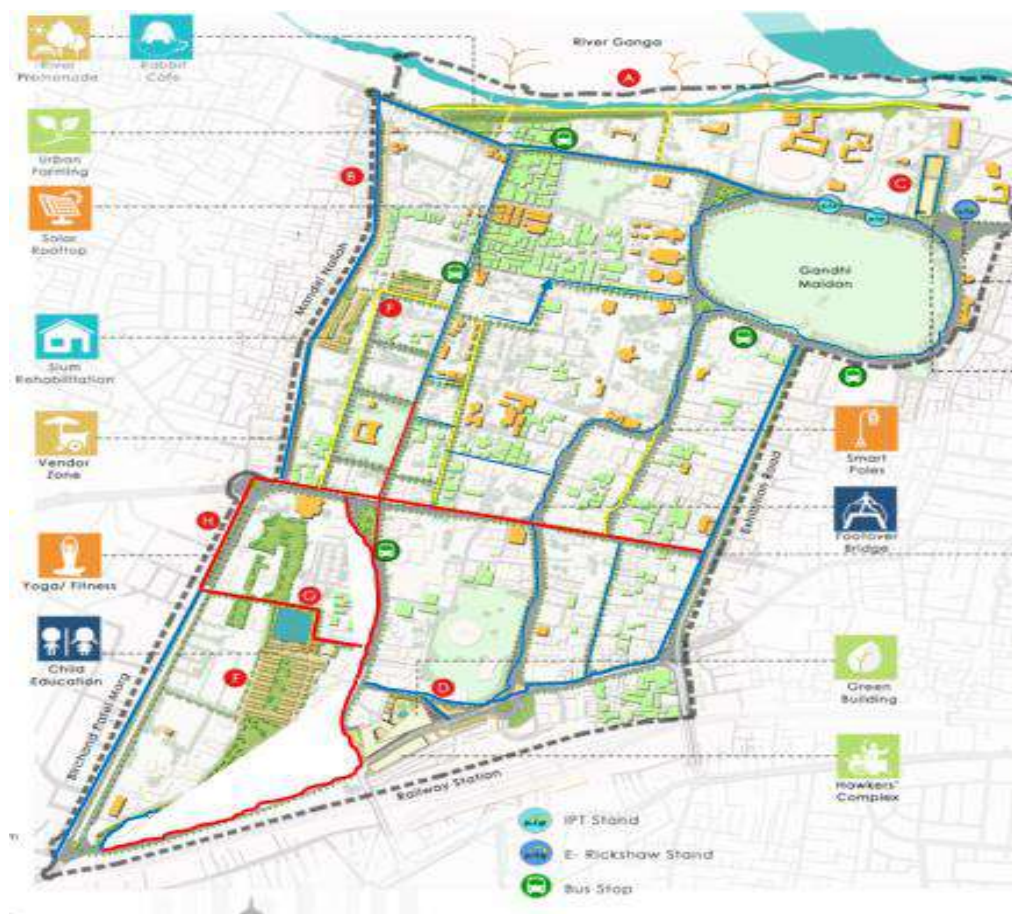
S. No.	Services Portfolio
G2C Services (Government to Citizen Services)	
1	ULB Website
2	Citizen Facilitation Center (CFC)
3	Birth and Death Certificates
4	Building Plan Approval
5	Property Tax
6	Trade License
7	Rent, Lease and Sairat
8	Advertisement and Hoardings
9	RTI (General Administration)
G2G services	
1	Personal Management System
2	General Administration (IT Support / Audit / Q&A/Legal/RTI)
3	Workflow and Document Management System

10.16. Annexure 86 : BSNL Optical Fiber Network in ABD Area

S.No.	Road	Location	Quantity	Colour
			(m)	Code
1	Exhibition road	Ram Gulam Chowk to Frazer road	360	Blue
2	Station Road	Chiryatnad Overbridge to Railway Station	470	Blue
3	Dak Bunglow Road	Exhibition road to income tax Roundabout	1200	Red
4	Amarnath Road	Budha Marg to Birchand Patel Marg	510	Red
5	New Market road	Station round about Budha Marg along	330	Blue
6	Veer Chand Patel Path	R-Block to BJP Office	905	Blue
7	Budha Marg	Tara Mandal to GPO Golambar	905	Red
8	Harding Park	GPO Golambar To R-Block	791	Red
9	Vidyapati Marg	Singha library road turning to planetarium 860	855	Yellow

10	Sinha library	Ludje house to Dak Bungalow road	634	Yellow
11	Gandhi Maidan Road	Road all along the gandhi maidan-kargil chowk to pir ali children park	2200	Blue
12	Ashok Rajpath	pir ali Children park to bas ghat	650	
13	SP Verma Road	Dak bungalow road to frazer road	354	Yellow
			10164	

10.17. Annexure 97 : Existing BSNL OFC Layout Diagram for ABD area of Patna City



DUCT _____

OFC _____

Proposed OFC _____

10.18. Annexure 108 : Analytics Use Cases Required with the Type of Locations

The SI shall implement all the use cases in such a way that the require video analytics can be deployed on any commercial off the shelf camera/device/computer/server. The AI functionality could be achieved through Camera (and other edge devices) and/or Server systems (VMS, ITMS, third party analytics etc) & ICCV or their combinations in any manner to achieve the result.

S. No.	Type of Analytics and Location	Location/Channels	Video Analytics Use case
1	Vehicle Related	150	Vehicle Classification/ Vehicle Detection and Video Capture Module
			Vehicle Detection by Color
			Hot Listing and Alert Generation
			Use of Mobile phones by Driver while driving /Red Light Violation Detection
			Wrong side driving detection/ Vehicle Behaviour Activity: •Vehicle Collision (such as Car, Bus, Truck, Motorcycle etc.) •Vehicle Park on sidewalks or at no-parking areas. (Illegal Parking)
			No helmet violation detection
			Triple ride Violation Detection
			Speed Violation Detection /Vehicle Wrong Direction Violation Detection/ Vehicle Left Side Violation Detection
2	Video Analytics Use Cases	100	Violence & Violent Behaviour Activity: •The human fighting. •The human firing a weapon. •The human throwing the stone. •Person Tracking.
			Women Safety Behaviour Activity: •The women / person in distress raising his/her hand(s) for HELP. •Chain / Mobile / Purse snatching •The human lies or falls on the ground •The human abandons an object.
			Grouping Behaviour Activity: •The Human or Humans group running. •Humans Gathering in a group. •Violation of Section 144 as per IPC
			Tracking of garbage truck movement

3	Surveillance Related at Property of interest/Other Analytics (Bus Stop, Important Buidings, Monuments, Parks, Stadium, Tourist Locations, Education Institutes, etc.)	200	Overcrowding Detection/confilcts in crowd
			Abandoned Object Detction
			Vandalism Detection
			Intrusion Detection/ Camera Health Monitoring
			Person Collapsing
			Loittering
			People Counting
			People Tracking across cameras

10.19. Annexure 19 : ICCC Design Considerations

Key Design Considerations

- Designed for 24x7 online availability of application.
 - Scalable solution on open protocols; no propriety devices/ applications
 - API based architecture for Integration with other web applications and Mobile applications.
- Key guiding principles considered for building the integrated solution are the following:
- Continuous adoption of rapidly evolving Technology - Technology evolves too fast and Government projects similar to Smart City with its long procurement cycles do not align naturally to adapt to this trend. Also, any changes to existing implementations require contract changes etc. Hence the entire system would be built to be open (standards, open API, plug-n-play capabilities), components coupled loosely to allow changes in sub-system level without affecting other parts, architected to work completely within a heterogeneous compute, storage, and multi-vendor environment.
 - Selection of best solution at best rate as and when required - Large integrated systems of Smart City operations should be designed to get best cost and performance advantages of natural technology curve (constant increase of speed and decrease of cost) and still aligned to open procurement practices of the Government. For this to happen, architecture should be open and vendor neutral, use commodity hardware, and designed for horizontal scale. This allows buying of commodity compute, storage, etc. only when needed at best price.
 - Distributed Access and Multi-channel service delivery -With high penetration of mobile devices and very large percentage of internet usage using mobile devices, it is imperative that the Smart City applications provide multiple channels of service delivery to its stakeholders. An important consideration is that the access devices and their screen capabilities (including browser variations) are numerous and constantly evolve. Hence, it is imperative to design the system such that the ecosystem of Smart City-integrated mobile apps also evolves.
 - Security and privacy of data - Security and privacy of data within the integrated Project will be foundational keeping in view of the sensitivity of data and critical nature of the infrastructure envisioned to be built for Smart City operations. Security and privacy of data should be fundamental in design of the system without sacrificing utility of the

system. When creating a system of this scale, it is imperative that handling of the sensitivity and criticality of data are not afterthoughts, but designed into the strategy of the system from day one.

- Provision of a Sustainable, Scalable Solution - The motive of the technological enhancements to provide a system that would be sustainable for the next few years. The expectation is that the system should sustain at least 5 years from GO-Live. The solution would be done keeping in mind the scalability of the system. The simplified procurement processes and ease of compliance is expected to lead to huge growth in contract's base. Every component of PSCL system needs to scale horizontally to very large volume of data.

The Application Software will have the capability to scale up to future requirements given below:

- Managing the entire Property Life Cycle (Data Collaboration between various govt. departmental systems)
- Maintaining Information on Citizen Life Cycle (Right from Birth to Marriage, Health, Education, Driving License, Interactions with PSCL)
- API Approach- PSCL has decided to adopt Open API as the guiding paradigm to achieve the above goals. Though PSCL system would develop a portal but that would not be the only way for interacting with the PSCL system as the stakeholders via his choice of third party applications, which will provide all user interfaces and convenience via desktop, mobile, other interfaces, will be able to interact with the PSCL system. These applications will connect with the PSCL system via secure PSCL system APIs. This architectural approach has been taken as the UI based integration through a ubiquitous web portal requires manual interaction and does not fit most consumption scenarios. The following benefits are envisaged from API based integration,
 - Consumption across technologies and platforms(mobile, tablets, desktops, etc.) based on the individual requirements
 - Automated upload and download of data
 - Ability to adapt to changing taxation and other business rules and end user usage models
 - Integration with customer software (GIS, Accounting systems).
- Business Rule Driven Approach-All configurations including policy decisions, business parameters, rules, etc. shall be captured in a central place within the system. The system shall provide facility to the decision makers to add new or edit/delete existing policies or make changes with appropriate permission control and audit trace. Managing these in a central repository ensures only once source of truth is used across many application servers and reduces issues of inconsistent application behavior. Decoupling of the business parameters/rules/master data from the rest of the solution architecture and making them configurable allows for a great deal of flexibility.
- Data Distribution Service-As a future roadmap it is envisaged that the functionalities provided by the PSCL Project should be available as services that could be offered to other stakeholders on request. Keeping this in mind the system shall be able to provide data on subscription-publication basis. The organization of the information exchange between modules is fundamental to publish-subscribe (PS) systems. The PS model connects anonymous information producers (publishers) with information consumers (subscribers). The overall distributed application (the PS system) is composed of processes. The goal of the

DDS architecture is to facilitate efficient distribution of data in a distributed system. Participant using DDS can ‘read’ or ‘write’ data efficiently and naturally with a typed interface. Underneath, the DDS middleware will distribute the data so that each reading participant can access the ‘most current’ values.

Guiding Architecture Principle

The IT architecture principles defined in this section are the underlying general rules and guidelines that will drive the subsequent development, use and maintenance of architectural standards, frameworks and future state target architecture.

PSCL system will be built on the following core principles:

Platform Approach

It is critical that a platform based approach is taken for any large scale application development, to ensure adequate focus and resources on issues related to scalability, security and data management. Building an application platform with reusable components or frameworks across the application suite provides a mechanism to abstract all necessary common features into a single layer. Hence the ICCC system is envisaged as a system with 100% API driven architecture at the core of it. PSCL portal will be one such application on top of these APIs, rather than being fused into the platform as a monolithic system.

Open APIs designed to be used form the core design mechanism to ensure openness, multi-user ecosystem, specific vendor/system independence, and most importantly providing tax payers and other ecosystem players with choice of using innovative applications on various devices (mobile, tablet, etc.) that are built on top of these APIs.

Openness

Adoption of open API, open standards and wherever prudent open source products are of paramount importance for the system. This will ensure the system to be lightweight, scalable and secure. Openness comes from use of open standards and creating vendor neutral APIs and interfaces for all components. All the APIs will be stateless. Data access must be always through APIs, no application will access data directly from the storage layer or data access layer. For every internal data access also (access between various modules) there will be APIs and no direct access will be there.

Data as an enterprise asset

Information is a high value asset to be leveraged across the organization to improve performance and decision making. Accurate information would ensure effective decision making and improved performance.

Effective and careful data management is of high importance and top priority should be placed on ensuring where data resides, that its accuracy can be relied upon, and it can be obtained when and where needed.

Performance

A best of breed solution using the leading technologies of the domain should be proposed in the solution ensuring the highest levels of performance. It will also ensure that the performance of various modules should be independent of each other to enhance the overall performance and also in case of disaster, performance of one module should not impact the performance other modules.

The solution should be designed in a manner that the following can be achieved:

- Modular design to distribute the appropriate system functions on web and app server
- Increase in-memory Operations (use static operations)
- Reduce number of I/O operations and N/w calls using selective caching
- Dedicated schemas for each function making them independent and avoiding delays due to other function accessing the same schema.
- Solution should provide measurable and acceptable performance requirements for users, for different connectivity bandwidths.
- The solution should provide optimal and high performance Portal Solution satisfying response time for slow Internet connections and different browsers.

Scalability

The component in the architecture will be capable of being scaled up to more user requests or handling more no. of input resources in various modules. Even inclusion of additional application functionalities can be catered to by upgrading the software editions with minimal effort.

The design of the system to consider future proofing the systems for volume handling requirements

- The application functions to be divided logically and developed as Modular solution.
- The system should be able to scale horizontally & vertically.
- Data Volume- Ability to support at least 20 % projected volume growth (year on year) in content post system implementation & content migration.
- Functionality – Ability to extend functionality of the solution without significant impact to the existing functional components and infrastructure.
- Loose coupling through layered modular design and messaging - The architecture would promote modular design and layered approach with clear division of responsibility and separation of concerns at the data storage, service and integration layer in order to achieve desired interoperability without any affinity to platforms, programming languages and network technologies. The architecture has to be scalable, maintainable and flexible for modular expansion as more citizen and business services are provided through the Project. Each of the logical layers would be loosely coupled with its adjacent layers
- Data partitioning and parallel processing - Project functionality naturally lends itself for massive parallel and distributed system. For linear scaling, it is essential that entire system is architected to work in parallel within and across machines with appropriate data and system partitioning. Choice of appropriate data sources such as RDBMS, Hadoop, NoSQL data stores, distributed file systems; etc. must be made to ensure there is absolutely no “single point of bottleneck” in the entire system including at the database and system level to scale linearly using commodity hardware.
- Horizontal scale for compute, Network and storage – Project architecture must be such that all components including compute, network and storage must scale horizontally to ensure that additional resources (compute, storage, network etc.) can be added as and when needed to achieve required scale.

No Vendor lock-in and Replace-ability

Specific OEM products may only be used when necessary to achieve scale, performance and reliability. Every such OEM component/service/product/framework/SI pre-existing product or work must be wrapped in a vendor neutral API so that at any time the OEM product can be replaced without affecting rest of the system. In addition, there must be at least 2 independent OEM products available using same standard before it can be used to ensure system is not locked in to single vendor implementation.

Security

The security services will cover the user profile management, authentication and authorization aspects of security control. This service run across all the layers since service components from different layers will interact with the security components. All public contents should be made available to all users without authentication. The service will authenticate users and allows access to other features of the envisaged application for which the user is entitled to.

The system should be designed to provide the appropriate security levels commensurate with the domain of operation. Also the system will ensure data confidentiality and data integrity.

The application system should have the following

- A secure solution should be provided at the hardware infrastructure level, software level, and access level.
- Authentication, Authorization & Access Control: 3 factors (User ID & Password, Biometric, and Digital Signature) security mechanisms should be implemented to enable secure login and authorized access to portal information and services.
- Encryption Confidentiality of sensitive information and data of users and portal information should be ensured.
- Appropriate mechanisms, protocols, and algorithms necessary to protect sensitive and confirmation data and information both during communication and storage should be implemented.
- Data security policies and standards to be developed and adopted across the Smart City departments and systems
- In order to adequately provide access to secured information, security needs must be identified and developed at the data level. Database design must consider and incorporate data integrity requirements.
- Role based access for all the stake holders envisaged to access and use the system
- Appropriate authentication mechanism adhering to industry good practice of Password Policies etc.
- Ability to adopt other authentication mechanism such as Electronic Signature Certificates
- Authorization validity to be ensured for the users providing the Data to the system. Data should be accepted only from the entity authorized
- Data should be visible only to the authorized entity
- Audit trails and Audit logging mechanism to be built in the system to ensure that user action can be established and can investigated if any can be aided(e.g. Logging of IP Address etc.)
- Data alterations etc. through unauthorized channel should be prevented.
- Industry good practice for coding of application so as to ensure sustenance to the Application Vulnerability Assessment

System must implement various measures to achieve this including mechanisms to ensure security of procurement data, spanning from strong end-to-end encryption of sensitive data, use of strong PKI national standards encryption, use of HSM (Hardware Security Module) appliances, physical security, access control, network security, stringent audit mechanism, 24x7 monitoring, and measures such as data partitioning and data encryption.

Activities such as anti-spoofing (no one should be able to masquerade for inappropriate access), anti-sniffing (no one should be able get data and interpret it), anti-tampering (no one should be able to put/change data which was not meant to be put/changed) should be taken care for data in transit, as well as data at rest, from internal and external threats.

User Interface

The architecture and application solutions to be designed should promote simplicity and ease of use to the end users while still meeting business requirements. It should provide a simpler and more cost-effective solution. Reduces development time and makes the solution easier to maintain when changes in requirements occur.

This will be accomplished by the implementation of rich User Interfaces along with its integration with the DMS, Relational Data Store, Messaging and other external applications.

- Efficient and layout design are the key considerations that enhance usability which should be factored in while designing the application. Standard and consistent usability criteria must be defined. An intuitive, user friendly, well-articulated navigation method for the applications greatly enhances the usability of the application.
- Effective information dissemination
- Enhanced functionalities including personalized delivery of content, collaboration and enriching GUI features
- The load time for all web page user interfaces must satisfy both the following response time targets on 1 mbps connection:
 - 3 sec for welcome page
 - 5 sec for static pages
 - 10 sec for dynamic pages
- Ability to perform a simple search within 10 seconds on 1 mbps connectivity and a complex search (combining four terms) within 15 seconds regardless of the storage capacity or number of files and records on the system.
 - Mobile Application Platform
 - Applications and services including all appropriate channels such as SMS/USSD/IVRS and development of corresponding mobile applications to the applications and services leveraging the Mobile Service Delivery Gateway (MSDG) and Mobile App Store.
 - Application platform should support the following smart phone mobile OS (Android 4.0 and above, iOS 4, 5 and above, Windows Phone OS 8.0 and above, Mobile Web App)
 - Support the target packaging components like (Mobile Website, Hybrid App, Native App, Web App and Application Development, Eclipse tooling platforms)
 - Support the ability to write code once and deploy on multiple mobile operating

systems

- Support integration with native device API
- Support utilization of all native device features
- Support development of applications in a common programming language
- Support integration with mobile vendor SDKs for app development and testing
- Support HTML5, CSS3, JS features for smartphone devices
- Support common protocol adapters for connection to back office systems (i.e. HTTP, HTTPS, SOAP, XML for format)
- Support JSON to XML or provide XHTML message transformations
- Support multi-lingual and language internalization
- Support encrypted messaging between server and client components

Reliability

This is a very crucial system and data are of high sensitivity, the data transfer and data management should be reliable to keep the confidence of the stakeholders. The system should have appropriate measures to ensure processing reliability for the data received or accessed through the application.

It may be necessary to mainly ensure the following

- Prevent processing of duplicate incoming files/data
- Unauthorized alteration to the Data uploaded in the PSCL system should be prevented
- Ensure minimum data loss(expected zero data loss)

Manageability

It is essential that the application architecture handles different failures properly; be it a hardware failure, network outage, or software crashes. The system must be resilient to failures and have the ability to restart, and make human intervention minimal.

All layers of the system such as application, infrastructure must be managed through automation and proactive alerting rather than using number of people managing manually.

The entire application must be architected in such a way that every component of the system is monitored in a non-intrusive fashion (without affecting the performance or functionality of that component) and business metrics are published in a near real-time fashion. This allows data centre operators to be alerted proactively in the event of system issues and highlight these issues on a Network Operations Centre (NoC) at a granular level. The solution should be envisaged to utilize various tools and technologies for management and monitoring services. There should be management and monitoring tools to maintain the SLAs.

Availability

The solution design and deployment architecture will ensure that the application can be deployed in a centralized environment offering system High Availability and failover.

The solution should meet the following availability requirements

- Load Balanced across two or more Web Server avoiding single point of failure
- Deployment of multiple application instances should be possible
- Distributed or load balanced implementation of application to ensure that availability of services is not compromised at any failure instance.
- Network, DC, DR should be available 99.99 % of the time.

SLA driven solution

Data from connected smart devices to be readily available (real-time), aggregated, classified and stored, so as not to delay the business processes of monitoring and decision making, and will enable appropriate timely sharing across the Smart City organization.

Readily available and consumed device data will facilitate timely access of analytics reports at every level and department of the Smart City and provide timely analysis of data as well as monitoring of KPIs through SLAs resulting in effective service delivery and improved decision making.

Integration Architecture

This section recommends the proposed integration architecture aligning with the overarching architectural principles.

The following are the integration specifications for the various integration scenarios -

Real-time integration

All the Smart City applications will be deployed in the Data Centre while any external application of the Smart City ecosystem will reside in outside premises.

The need for an OPC Unified Architecture (OPC- UA) is felt that will facilitate PSCL in defining an enterprise integration platform. An OPC platform will help in data exchange across applications in real-time mode (both synchronous and asynchronous), promote loose coupling with ease of maintenance and change, facilitate rapid composition of complex services, achieve scalability through modularity, and improved business visibility.

The OPC UA architecture is a service-oriented architecture (SOA) and is based on different logical levels. It is an architectural style that allows the integration of heterogeneous applications & users into flexible service delivery architecture. Discrete business functions contained in enterprise applications could be organized as layers of interoperable, standards-based shared "services" that can be combined, reused, discovered and leveraged by other applications and processes.

The following are the various integration modes and techniques that could be leveraged:-

- OPC Base Services are abstract method descriptions, which are protocol independent and provide the basis for OPC UA functionality. The transport layer puts these methods into a protocol, which means it serializes/de-serializes the data and transmits it over the network. Two protocols are specified for this purpose. One is a binary TCP protocol, optimized for high performance and the second is Web service-oriented.
- SOAP web service based interfacing technique will be leveraged as the real-time point

to point synchronous integration mode with external or third party systems. The following integration points could be considered for SOAP web service based interfacing:-

- Payment gateway of the authorized banks to enable authorized users make financial transactions for the Smart City services availed by them. This should support a unified interface to integrate with all Payment Service Providers using web services over secured protocols.
- SMS application, acting as the SMS Gateway, will make use of APIs for SMS communication to GSM network using the GSM modem, which can be both event-driven as well as time- driven. The API will be exposed to initiate the broadcasting or alert notification.
- Social Media Apps and NoSQL data stores to exchange photos, videos and message feeds, based on interactions with Citizens and Business as well as comments/posts to inform stakeholders.
- IVR/Customer Support solution with ERP and Transactional Data Repository to exchange citizen and business demographic, registration and payment data as well as transactional data related to citizen services and municipal operations.
- Message based interfacing technique will be leveraged for real-time asynchronous integration mode. The following integration points could be considered for message based interfacing -
 - Central LDAP with ERP to synchronize member and employee user registration data
 - Payment solution and ERP to exchange payment data for tracking of beneficiary's payment transactions against different services (citizen, workers, transporter, vendor), master data (employee, vendor/supplier, location, facilities, price table)
 - Employee attendance data with ERP (HR Module) to capture data pertaining to employee location and attendance
 - Departmental applications with ERP (Asset Management module) to exchange data for procurement and maintenance of any assets or infrastructure items for each department.
 - Municipal operations application with ERP (Material Management module) to capture materials related transaction and inventory data for public works
 - Other Government Applications with Smart City application to exchange data for Government procurement, public health schemes, welfare schemes, citizen health, etc.
- RESTful API service based interfacing technique will be leveraged for the following integration areas-
 - Access and use of various services provided by the different departments for citizens and business community will be done through a RESTful, stateless API layer.
 - Access and use of various internal functions related to operations and administration of Smart City for departmental and PSCL employees will be done through a RESTful, stateless API layer

- Data integration in batch mode will be through ETL. The following integration points could be considered for ETL based data integration -
 - Initial data migration to cleanse, validate and load the data extracted from source systems into target tables.
 - Data load from all the individual transactional systems like ERP, Grievance Redressal to central enterprise data warehouse solution for aggregation, mining, dashboard reporting and analytics.

Process Integration layer of the PSCL solution will automate complex business processes or provide unified access to information that is scattered across many systems. Process Integration will provide a clean separation between the definition of the process in the process model, the execution of the process in the process manager, and the implementation of the individual functions in the applications. This separation will allow the application functions to be reused in many different processes.

An enterprise service bus (ESB) is a software architecture model used for designing and implementing the interaction and communication between mutually interacting software applications in Service Oriented Architecture. As software architecture model for distributed computing it is a variant of the more general client server software architecture model and promotes strictly asynchronous message oriented design for communication and interaction between applications. Its primary use is in Enterprise Application Integration of heterogeneous and complex landscapes. Following are the requirement for an ESB system:

- The solution should support static/deterministic routing, content-based routing, rules-based routing, and policy-based routing, as applicable in various business cases.
- The solution should have capabilities to receive input message in heterogeneous formats from various different systems, interpret those messages, process and transform those messages to generate output and feed them to various different clients as per formats applicable.
 - The solution should have features to communicate across different services, process them and expose as single aggregate service to facilitate business functionality
 - ESB should support SOA standards such as XML, XSLT, BPEL, web services standards and messaging standards.
 - ESB should support all industry standards interfaces for interoperability between different systems

There are four integration gateways envisaged as part of the solution design. The key requirements with respect to each of these are mentioned below:

SMS Gateway: SMS services are envisaged to be made available as part of the solution design. The service provider may integrate the solution with MSDG, and use the services available through it, or deploy its own SMS Gateway services at no extra charge to PSCL, but it is a mandatory requirement that all the SMS based services (alerts and notifications) should be available as part of the solution. Following are some of the key requirements for the SMS services through the solution:

- Should contain required details/information and targeted to the applicant or designated officers of tax departments and other stakeholders and users as per prevailing TRAI norms

- Facilitate access through access codes for different types of services
- Support automated alerts that allows to set up triggers that will automatically send out reminders
- Provide provision for International SMS
- Provide provision to receive messages directly from users
- Provide provision for personalized priority messages
- Resend the SMS in case of failure of the message
- Provide messaging templates

Email Services: Email services are envisaged to be made available as part of the solution design to send alerts/intimations/automated messages to registered email ids, based on preferences set up/opted by individual users. An authenticated SMTP mail service (also known as a SMTP relay or smart host) is envisaged to be integrated with the solution for sending mail from the solution, and delivered to intended inbox. Support anti-spam features.

Payment Gateway: The solution is envisaged to have integration with payment gateways, to enable authorized Users make financial transactions, as per rights and privileges provided to him/her. The service provider is required to make the provisions for integration with such third party gateways and provide payment services, as per requirement of the PSCL. Some of the key features of payment gateway are mentioned below:

- Should support secure integration with Payment Service Providers
- Should support a unified interface to integrate with all Payment Service Providers
- Should support integration with Payment Service Providers using web services and over HTTP/S protocol
- Should manage messages exchange between UI and payment service providers
- Should support beneficiary's payment transactions tracking against various services
- Should support bank accounts reconciliation
- Should provide logs for all transactions performed through the Payment Gateway for future financial dispute resolution that might arise between entities and either beneficiaries or Payment Service Providers
- Should maintain and keep transactions logs for time period required and specified by the financial regulations followed in country
- Should support redundant Payment Discovery
- Should submit Periodic Reconciliation Report to Government entities
- Should support transaction reports to monitor and track payments
- Should support real-time online credit card authorization for merchants
- Should support compliance with emerging trends and multiple payment options such debit card, credit card, cash cards and other payment gateways
- Should provide fraud screening features
- Should support browser based remote administration

- Should support multicurrency processing and settlement directly to merchant account
- Should support processing of one-time or recurring transactions using tokenization
- Should support real time integration with SMS and emails

IVR Services: IVR services are envisaged as part of Call Centre facility, which will be integrated with the solution, to provide information and services to the people who would contact the Call Centre: Some of the key features of the IVR services are mentioned below:

- Should provide multi-lingual content support
- Should facilitate access through access codes for different types of services
- Should support Web Service Integration
- Should support Dual Tone Multi Frequency (DTMF) using telephone touchpad - in-band and out-of-band
- Should support redirection to human assistance, as per defined rules
- Should be able to generate Data Records – (CDRs) and have exporting capabilities to other systems

There are multiple ways of integration of the solution with other systems is envisaged. These may be through Web Services, Message Queuing, File based or API based. The integration and data sharing mechanism may be either in Batch Mode or Need basis (synchronous or asynchronous). Some of the key requirements of the interface/integration are mentioned below:

- Interface Definition
- Interface Owner
- Interface Type
- Interface Format
- Frequency
- Source System
- API/Service/Store Procedure
- Entitlement Service
- Consuming System
- Interface Layout (or) Schema
- Should have provision for exceptional scenarios
- Should have syntax details such as data type, length, mandatory/option, default values, range values etc.
- Error code should be defined for every validation or business rule
- Inputs and outputs should be defined
- Should be backward compatible to earlier datasets
- Data exchange should provide transactional assurance

- Response time and performance characteristics should be defined for data exchange
- The failover scenarios should be identified
- Data exchange should be auditable

Note: Bidder is free to proposed their own design to be meet the scope and SLA requirement

aa) Security

Data exchange should abide by all laws on privacy and data protection Security Architecture. Proposed solution shall adhere to the guidelines & frameworks issued by Bihar Government/Gol from time-to-time for security for smart city solutions.

This section recommends the proposed security architecture aligning with the overarching architectural principles. The basic tenets of Smart City security architecture are the design controls that protect confidentiality, integrity and availability of information and services for all the stakeholders.

User Security and Monitoring Authentication & Authorization

A strong authentication mechanism should be considered to protect unauthorized access to the Smart City applications. Consider use of at least two of the following forms of authentication mechanism:

- Something you know, such as a password, PIN etc.
- Something you have, such as a smart card, hardware security token etc.
- Something you are, such as a fingerprint, a retinal scan, or other biometric methods

Levels of Authentication

Based on the security requirements the following levels of authentication should be evaluated.

- For applications handling sensitive data it is recommended that in the least one factor authentication key in the form of a password is essential. Strong password complexity rules should be enforced to ensure confidentiality and integrity of the data
- For applications handling highly sensitive data it is recommended that two factor authentication mechanisms should be considered. The first line of defense is the password conforming to the password complexity rules'. Along with the password next user has to provide a one-time password which varies for each session. One time passwords are valid for each session and it is not vulnerable to dictionary, phishing, interception and lots of other attacks. A counter synchronized One-Time Password (OTP) solution could be used for this purpose.

Authorization

Authorization of system users should be enforced by access controls. It is recommended to develop access control lists. Consider the following approach for developing access control list -

- Establish groups of users based on similar functions and similar access privilege.
- Identify the owner of each group

- Establish the degree of access to be provided to each group

Data Security

PSCL should protect Integrated Project information against unauthorized access, denial of service, and both intentional and accidental modification. Data security, audit controls and integrity must be ensured across the data life cycle management from creation, accessed, viewed, updated and when deleted (or inactivated). This provides a proactive way to build defense against possible security vulnerabilities and threats, allowing errors to be corrected and system misuse to be minimized.

The implications for adhering to an effective data security and integrity guideline related to the Project are the following –

- Data security policies and standards to be developed and adopted across PSCL Smart City applications and stakeholders
- Data security controls to be put in place to restrict access to enterprise data based on roles and access privileges. Data audit logs should be maintained for audit trail purposes. Security controls will be able to be reviewed or audited through some qualitative or quantitative means for traceability and to ensure that risk is being maintained at acceptable levels.
- In order to adequately provide access to secured information, security needs must be identified and developed at the data level, not the application level. Database design must consider and incorporate data integrity requirements.
- Procedures for data sharing need to be established. Data integrity during data synchronization needs to be ensured across the enterprise.
- Audit Capabilities: The system provides for a system-wide audit control mechanism that works in conjunction with the RDBMS.
- Maintaining Date/Time Stamp and User Id: Every transaction, with a date and time and User ID, is captured. The system allows generating various audit reports for verification.
- Access Log: The PSCL Project should have extensive inbuilt security and access control mechanisms. Based on this, the system keeps track of the various functions accessed by any users.

Audit Trail & Audit Log

Audit trails or audit logs should be maintained. Log information is critical in identifying and tracking threats and compromises to the environment.

There are a number of devices and software that should be logged which include hardware & software based firewalls, web servers, authentication servers, central/domain controllers, database servers, mail servers, file servers, routers, DHCP servers etc.

It is essential to decide what activities and events should be logged. The events which ideally should be captured include

- Create, read, update and delete of confidential information;
- User authentication and authorization activities in the system, granting, modification or revoking of user access rights;
- Network or service configuration changes;

- Application process start up, shutdown or restart, abort, failure or abnormal terminations, failure of network services;
- Detection of suspicious activities such as from Intrusion Detection and Prevention system, anti-virus, anti-spyware systems etc.

Application Security

- Project must comply with the Application Security Plan and security guidelines of Government of India as applicable
- Secure coding guidelines should be followed. Secure coding guidelines should include controls against SQL injection, command injection, input validation, cross site scripting, directory traversal, buffer overflows, resource exhaustion attacks etc. OWASP Top 10 standard should be mapped in the secure coding guidelines to cover all major vulnerabilities.
- Validation checks should be incorporated into the application to detect any corruption of information through processing errors or deliberate acts.
- Data output from an application should be validated to ensure that the processing of stored information is correct and appropriate to the circumstances
- Should implement secure error handling practices in the application
- Project should have Role based access, encryption of user credentials. Application level security should be provided through leading practices and standards including the following:
 - Prevent SQL Injection Vulnerabilities for attack on database
 - Prevent XSS Vulnerabilities to extract user name password (Escape All Un-trusted Data in HTML Contexts and Use Positive Input Validation)
 - Secure Authentication and Session Management control functionality shall be provided through a Centralize Authentication and Session Management Controls and Protect Session IDs from XSS
 - Prevent Security Misconfiguration Vulnerabilities (Automated scanners shall be used for detecting missing patches, misconfigurations, use of default accounts, unnecessary services, etc. maintain Audits for updates
 - Prevent Insecure Cryptographic Storage Vulnerabilities (by encrypt off-site backups, ensure proper key storage and management to protect keys and passwords, using a strong algorithm)
 - Prevent Failure to Restrict URL Access Vulnerabilities (By providing authentication and authorization for each sensitive page, use role-based authentication and authorization and make authentication and authorization policies configurable
 - Prevent Insufficient Transport Layer Protection Vulnerabilities (enable SSL for all sensitive pages, set the secure flag on all sensitive cookies and secure backend connections
 - Prevent Id Redirects and Forwards Vulnerabilities
 - For effective prevention of SQL injection vulnerabilities, SI should have monitoring feature of database activity on the network and should have reporting mechanism to restrict or allow the traffic based on defined policies.

Infrastructure Security

The following focused initiatives to discover and remedy security vulnerabilities of the IT systems of PSCL Smart City should be considered to proactively prevent percolation of any threat vectors -

- Deploy anti-virus software to all workstations and servers to reduce the likelihood of security threats;
- Deploy perimeter security technologies e.g. enterprise firewalls to reduce the likelihood of any security threat;
- Deploy web content filtering solutions to prevent threats from compromised websites to help identify and block potentially risky web pages;
- Install enterprise-level e-mail anti-security software to reduce vulnerability to phishing and other e-mail security spams. This would check both incoming and outgoing messages to ensure that spam messages are not being transmitted if a system becomes compromised.
- Perform periodic scanning of the network to identify system level vulnerabilities
- Establish processes for viewing logs and alerts which are critical to identify and track threats and compromises to the environment. The granularity and level of logging must be configured to meet the security management requirements.
- Deploy technology to actively monitor and manage perimeter and internal information security.
- Deploy network Intrusion Detection System (IDS) on the perimeter and key points of the network and host IDS to critical systems. Establish process to tune, update, and monitor IDS information.
- In case of cloud deployment, cloud services can be disrupted by DDoS attacks or mis-configuration errors which have the potential to cascade across the cloud and disrupt the network, systems and storage hosting the cloud application.
- Deploy security automation techniques like automatic provisioning of firewall policies, privileged accounts, DNS, application identity etc.

Network Security for Smart Devices

The core principles of security for any smart device network rest on the three most important data security concerns of confidentiality, integrity and authentication. Hence the security for smart device networks should primarily focus on the protection of the data itself and network connections between the nodes. From a network perspective, following are to be considered for designing the smart devices network -

- Protection of fair access to communication channels (i.e. media access control)
- Concealing of physical location of the nodes
- Defense against malicious resource consumption, denial of service, node capturing and node injection
- Provision for secure routing to guard the network from the effects of bad nodes
- Protection of the mobile code

Smart devices have a triple role in most networks - data collectors, processors and traffic

forwarders for other devices in the network. The typical attacks for which countermeasures are to be defined and implemented are: Radio Jamming, Nodes Reporting Wrong Data, Data Aggregation Attacks and Battery Attacks.

The following guidelines need to be considered for security enhancement of smart devices and their networks:

- Use of IP-based network for smart devices
- Use of Link Layer Security for password-based access control and encryption
- Protection of smart devices nodes behind a firewall for carrying out SSL-based application data transfer and mechanism to avoid distributed DoS attacks
- Public-key-based authentication of individual devices to the network and provisioning them for secure communications
- Conformance of the security solution to the standards of IETF, IEC and IEEE to ensure maximum security and interoperability, with support for the following commonly used protocols at a minimum - IPSec/IKE, SSH and SSL/TLS

Software Development Lifecycle Continuous Build

The PSCL Project should be highly modular and parallel development should be carried out for faster execution using industry's best Software Development Lifecycle practices. All application modules within the same technology platform should follow a standardized build and deployment process.

A dedicated 'development / customization' environment should be proposed and setup. SI must provision separate development and testing environment for application development and testing. Any change, modifications in any module must follow industry standard processes like change management, version control and release management in large and complex application development environment.

Application source code could be maintained in source control and could be broken up into a number of projects. Source control projects are created to abstract related set of modules or feature that can be independently included in another application.

It is a mandatory to create, update and maintain all relevant documentation throughout the contract duration. Also it should be ensured that a bug tracking tool is maintained for proper tracking of all bugs fixes as per various tests conducted on the application.

Quality Assurance

A thorough quality check is proposed for the PSCL Project and its modules, as per standard Software Development Life Cycle (SDLC). SI is expected to lay down a robust Quality Assurance program for testing of the developed application for its functionality, performance and security before putting in production environment. The program must include an overall plan for testing and acceptance of system, in which specific methods and steps should be clearly indicated and approved by PSCL. SI is required to incorporate all suggestions / feedback provided after the elaborate testing of the system, within a pre-defined, mutually agreed timeline. SI must undertake the following:

- Outline the methodology that will be used for testing the system.
- Define the various levels or types of testing that will be performed for system.
- Provide necessary checklist/documentation that will be required for testing the

system.

- Describe any technique that will be used for testing the system.
- Describe how the testing methodology will conform to the requirements of each of the functionalities and expected outcome.
- Indicate / demonstrate to PSCL that all applications installed in the system have been tested.

Performance and Load Testing

SI is expected to implement performance and load testing with following features:

- Testing workload profiles and test scenarios based on the various functional requirements should be defined. Application as well as system resource utilization parameters that need to be monitored and captured for each run also needs to be defined.
- Should support application testing and API testing including HTTP(s), web services, mobile applications and different web 2.0 frameworks such as Ajax/Flex/HTML5.
- SI should perform the load testing of PSCL Project for multiple workload profiles, multiple scenarios, and user loads to handle the envisaged users of the system.
- Different activities before load testing i.e. identification of work load profiles, scenarios, information capturing report formats, creation of testing scripts, infrastructure detailing and workload profile should be prepared before the start of actual load testing exercise.
- Solution parameters needs to be tuned based on the analysis of the load testing reports. The tuning process could be iterative until the issues are closed. Multiple load runs needs to be executed for users to simulate different scenarios, such as peak load (year end, quarter end, etc.), load generation within the LAN, Load generation across WAN or mobile network simulator while introducing configurable latency/jitter/packet loss etc.
- Should eliminate manual data manipulation and enable ease of creating data-driven tests.
- Should provide capability to emulate true concurrent transactions.
- Should identify root cause of performance issues at application or code level. Include code performance analysis to quickly pinpoint component-level bottlenecks: Slowest classes and methods, most frequently called methods, most costly (aggregate time spent for each method), response time variance etc.
- Should allow selection of different network bandwidth such as analog modems, ISDN, DSL, or custom bandwidth.
- Should be able to monitor various system components e.g. Server (OS, Web, Application & Database) Monitoring, Network (between Client & Server) Delay Monitoring, Network Devices (Firewall, Switch & Router) Monitoring during the load test without having to install any data capturing agents on the monitored servers/components
- Should correlate response times and system performance metrics to provide quick insights in to root cause of performance issues.

- Reports on following parameters (but not limited to) such as transaction response time, transaction per second (Passed), user interface rendering time, transaction per second (Failed), web transaction breakdown graphs, hits per second, throughput, HTTP responses per Second, pages downloaded per second, system infrastructure performance metrics etc.

Should provide End-to-End system performance analysis based on defined SLAs. Should monitor resource utilization including memory leakage, CPU overload and network overload. Should have the ability to split end-to-end response time for Network & Server(s) and provide drill-down capability to identify and isolate bottlenecks.

10.20. Annexure 110 : 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. In case of addition/update in number of license for the products, SI is required to meet of technical specifications contained in the RFP and for the upward revisions and/or additions of licenses is required be made as part of change order and cost would be commensurate to the itemized rate approved at the LOI issuance.
3. Any manufacturer and product name mentioned in the Tender should not be treated as a recommendation of the manufacturer / product.
4. None of the IT / Non-IT equipment's proposed by SI should be End of Life product. It is essential that the technical proposal is accompanied by the OEM certificate in the format given in Volume I of this Tender, where-in the OEM will certify that the product is not end of life product & shall support for at least 6 years from the date of Bid Submission.
5. All IT Components should support IPv4 and IPv6.
6. Technical Bid should be accompanied by OEM's product brochure / datasheet. SIs should provide complete make, model, part numbers and sub-part numbers for all equipment/software quoted, in the Technical Bid.
7. SI should ensure that only one make and model is proposed for one component in Technical Bid for example all Field cameras must belong to a single OEM and must be of the same model etc.
8. SIs should ensure complete warranty and support for all equipment from OEMs. All the back-to-back service agreements should be submitted along with the Technical Bid.
9. All equipment, parts should be original and new.
10. The user interface of the system should be a user friendly Graphical User Interface (GUI).
11. Critical core components of the system should not have any requirements to have proprietary platforms and should conform to open standards.
12. 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 PSCL.

13. All the Clients Machines / Servers shall support static assigned IP addresses or shall obtain IP addresses from a DNS/DHCP server.
14. The Successful SI should also propose the specifications of any additional servers / other hardware, if required for the system.
15. The indicative architecture of the system is given in this volume. The Successful SI must provide the architecture of the solution it is proposing.
16. 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 Centre 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 Tender.
17. 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.
18. 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.
19. All the hardware and software supplied should be from the reputed Original Equipment Manufacturers (OEMs). PSCL 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 tender documents.
20. All servers, active networking components (for edge level switches, please refer below for additional information), security equipment, storage systems and COTS Application.
21. Cameras, Network Video Recorder (NVR) and the Video Management / Video Analytics Software should be ONVIF Core Specification '2.X' or 'S' compliant and provide support for ONVIF profiles such as Streaming, Storage, Recording, Playback, and Access Control.
22. SI shall place orders on various OEMs directly or through distributor and not through any sub-contractor / partner. All licenses should be in the name of the PSCL.

10.21. Annexure 121 : Standards for Bio-Metrics

Bio-Metrics Standards

The Indian Government proposes to use biometric data for identification and verification of individuals in e-Governance applications. The biometric data includes fingerprint image, minutiae, face image and iris data.

The Indian e-Governance applications will have both biometric identification and verification phases, to ensure there is no duplication of identity and to verify the identity of a person for access to the services of the application.

1) Face Image Data Standard

Manual Facial recognition is not sufficient currently for de-duplication. Computer based face recognition has reasonable accuracy under controlled conditions only. Hence for de-duplication purposes, other biometrics like finger print/iris image is also recommended.

With the objective of interoperability among various e-Governance applications, the face image data standard for Indian e-Governance Applications will adopt **ISO /IEC 19794-5:2005(E)**. While the ISO standard is broad to cover all possible applications of computer based face recognition and human visual inspection, this standard is more restrictive, as it is limited to human visual inspection.

The ISO standard specifications are tailored to meet specific needs of civilian e-Governance applications by specifying certain prescriptive values and best practices suitable in Indian context.

Standard	Description
ISO /IEC 19794-5:2005(E)	<p>This standard includes capture and storage specifications of face images for human visual inspection and verification of the individuals in Indian E-Governance applications.</p> <p>It specifies a format to store face image data within a biometric data record compliant to the Common Biometric Exchange Formats Framework (CBEFF), given in ISO 19785-1. It also includes best practices recommended for implementation of the specifications in different categories of e-Governance applications.</p> <p>The scope of this standard includes:</p> <ul style="list-style-type: none"> ○ Characteristics of Face Image capturing device ○ Specifications of Digital Face Image & Face Photograph Specifications intended only for human visual inspection and verification ○ Scene requirements of the face images, keeping in view a future possibility of computer based face recognition ○ Face Record Format for storing, archiving, and transmitting the information of face image within a CBEFF header data structure for the purpose of interoperability and usage in future for computer based face recognition.

2) Fingerprint Image and Minutiae Data Standard

Fingerprint is an important and unique biometric characteristic of an individual. There are many vendors selling finger print devices for acquisition of the data in different ways. Also various algorithms are available for fingerprint features extraction and matching.

It is necessary that these vendors follow fingerprint standards and best practices to ensure interoperability of devices and algorithms to avoid vendor lock-in, and also ensure long term storage of data with technology independence.

Usually, the fingerprint image data captured during enrolment is stored / transmitted for 1:1 (verification) and 1: N (identification) in an e-Governance application life cycle.

The matching of the fingerprints is done by extracting the minutiae of fingerprint data already stored in the enrolment stage, with the minutiae of data captured at the time of verification / identification. This process may even require transmission of fingerprint image data / minutiae data among various e-Governance applications by following the best practices.

Standard	Description
ISO/IEC 19794-4:2005(E)	<p>This standard deals with usage of fingerprint image data and minutiae data for identification and verification of an individual.</p> <p>To ensure interoperability among vendors, it is required that these images be stored in a format compliant with the international standard ISO 19794-4, within the overall Common Biometric Exchange Formats Framework (CBEFF) as per ISO 19785-1.</p> <p>The Government of India would adopt ISO/IEC 19794-4:2005(E) as Fingerprint Image standard, and ISO 19794-2:2005(E) as Minutiae data format standard.</p> <p>The current version of Fingerprint image data standard has been tailored from the ISO 19794-4:2005(E) standard to meet specific needs of e-Governance applications in Indian context. It also includes best practices recommended for implementation of the specifications in different categories of e-Governance applications.</p> <p>This standard specifies fingerprint image specifications in different stages like acquisition for enrolment / verification / identification, storage and transmission. It also includes minutiae template specifications and best practices for implementation of the standard specifications in different categories of e-Governance applications based upon the volume of data, and verification/ accuracy requirements.</p> <p>The current version of the standard is applicable to all civilian e-governance applications as the present version does not include specifications for latent fingerprint data required by certain law enforcement applications.</p>

3) Iris Image Data Standard

In the recent years, Iris recognition has emerged as an important and powerful Biometric characteristic. The Indian Government anticipates that, iris biometric would be deployed for

identification and verification in e-Governance applications where identity management is a major issue.

In order to capture the Iris image, special devices are available in the market providing different formats for image acquisition and storage. Also many algorithms have been developed by vendors to extract the features of iris images to decide on a match during verification / identification stage. To ensure interoperability among the e-Governance applications requiring iris recognition, it is necessary to standardize iris specifications including the storage and transmission formats.

Thus, to allow the application developer maximum flexibility in usage of algorithms and devices from different vendors and to address interoperability requirements, the iris image must be captured and stored as per standard specifications included in this document.

This Standard would be applicable to all e-Governance applications in India as per the Government's Policy on Open Standards.

There are two types of interchange formats to represent the Iris image data. The first is a rectilinear (rectangular or Cartesian) image storage format that specifies raw, uncompressed or compressed intensity values. The second format is based on polar image specification with specific pre-processing and segmentation steps, producing a compact data structure containing only Iris information.

The Indian e-Governance applications will deal with Iris image data during multiple stages. Some of these stages are given below:

- a. Image acquisition, its processing and its storage in the Enrolment stage
- b. Image acquisition and storage for off line / on line verification of Iris image data in 1:1 matching stage
- c. Image acquisition and storage for the purpose of identification in 1:N matching stage
- d. Transmission of Iris image data to other e-Governance applications
- e. Extraction of features of Iris images (enrolment or recognition stage), their storage, and matching (Not covered in the present version of the standard).

The interchange format type of the Iris images that is defined in this standard is for rectilinear images only.

If the image is collected by a camera that captures only one eye at a time and is stored using a rectilinear coordinate system no specific pre-processing is required. Cameras that capture images of both eyes simultaneously may use the following processing steps to calculate the rotation angle of the Iris images.

Standard	Description
ISO/IEC 19794-4:2005(E)	The Government of India would broadly adopt ISO 19794-6:2005(E) Iris Image Data Standard, by tailoring the standard specifications to meet specific needs of civilian e-Governance applications in Indian context and as per the GoI Policy on Open Standards.

	<p>This Standard specifies Iris image data specifications, acquisition, storage and transmission formats. It also includes best practices for implementation of the Standard specifications in different categories of e-Governance applications, based on the volume of data and verification/ accuracy requirements. This version of the Standard does not include features extraction & matching specifications.</p>
--	---

Reference Standards:

1. GoI Face Image data standard version 1.0 published in November, 2010
2. GoI Fingerprint Image data Standard version 1.0 published in November, 2010
3. GoI Iris Image Data Standard Version 0.4, document published in March, 2011

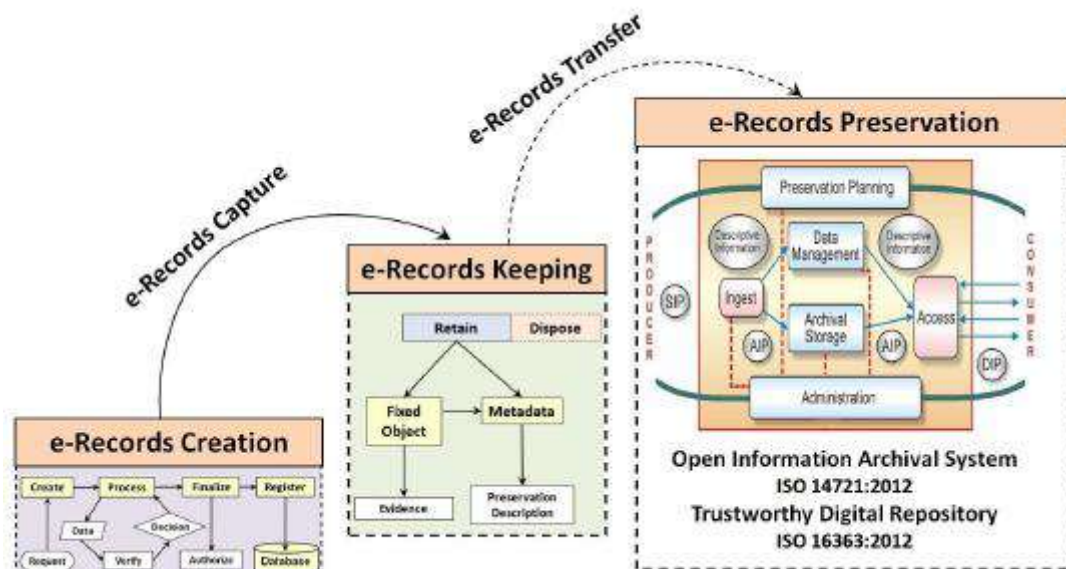
10.22. Annexure 132 : Standards for Digital Preservation Standards

The **e-Governance Standard for Preservation Information Documentation (eGOV-PID) of Electronic Records (eGOV-PID)** provides a standardized metadata dictionary and schema for describing the "preservation metadata" of an electronic record. This standard proposes to capture most of the preservation information (metadata) automatically after the final e-record is created by the e-Government system. Such preservation information documentation is necessary only for those e-records that need to be retained for long durations (e.g. 10 years, 25 years, 50 years and beyond) and the e-records that need to be preserved permanently.

The implementation of this standard helps in producing the valid input i.e. Submission Information Package (SIP) for archival and preservation purpose as per the requirements specified in the ISO 14721 Open Archival Information Systems (OAIS) Reference Model.

The eGOV-PID allows to capture the preservation metadata in terms of cataloguing information, enclosure information, provenance information, fixity information, representation information, digital signature information and access rights information.

The core concepts of 'preservability' are based on the requirements specified in IT ACT, ISO/TR 15489-1 and 2 Information Documentation - Records Management and ISO 14721 Open Archival Information Systems (OAIS) Reference Model. It introduces 5 distinct steps of e-record management i.e. e-record creation, e-record capturing, e-record keeping, e-record transfer to designated trusted digital repository and e-record preservation which need to be adopted in all e-Governance projects.



Standard	Description
ISO 15836:2009	Information and documentation - The Dublin Core metadata elements
ISO/TR 15489-1 and 2	Information and Documentation - Records Management: 2001
ISO 14721:2012	Open Archival Information Systems (OAIS) Reference Model
ISO/DIS 16363: 2012	Audit & Certification of Trustworthy Digital Repositories
METS, Library of Congress, 2010	Metadata Encoding and Transmission Standard (METS) -
InterPARES 2	International Research on Permanent Authentic Records - A Framework of Principles for the Development of Policies, Strategies and Standards for the Long-term Preservation of Digital Records, 2008
ISO 19005-1:2005 Use of PDF 1.4 (PDF/A-1b) with Level B	<p>Capture of e-records in PDF for Archival (PDF/A) format - PDF/A-1a is based on the PDF Reference Version 1.4 from Adobe Systems Inc. (implemented in Adobe Acrobat 5 and latest versions) and is defined by ISO 19005-1:2005.</p> <p>Conformance is recommended for archival of reformatted digital documents due to following reasons:</p> <ul style="list-style-type: none"> ○ PDF/A-1b preserves the visual appearance of the document ○ Digitized documents in image format can be composited as PDF/A-1b <p>PDF/A for e-governance applications</p> <ul style="list-style-type: none"> ○ Apache FOP 1.1 library can be used in the application logic for dynamically publishing the e-records in PDF/A format. <p>PDF/A for document creation</p> <ul style="list-style-type: none"> ○ Libre Office 4.0 supports the exporting of a document in PDF/A format. ○ MS Office 2007 onwards the support for “save as” PDF/A is available. ○ Adobe Acrobat Professional can be used for converting the PDF documents to PDF/A format.
ISO 19005-2:2011 Use of ISO 32000-1 (PDF/A-2)	<p>Recommended for preservation of documents requiring the advanced features supported in it.</p> <p>PDF/A-2a is based on ISO 32000-1 – PDF 1.7 and is defined by ISO 19005-2:2011.</p> <p>Its features are as under:</p> <ul style="list-style-type: none"> ○ Support for JPEG2000 image compression ○ Support for transparency effects and layers ○ Embedding of OpenType fonts ○ Provisions for digital signatures in accordance with the PDF Advanced Electronic Signatures – PAdES standard ○ Possibility to embed PDF/A files in PDF/A-2 for archiving of sets of documents as individual documents in a single file <p>PDF/A-2 does not replace the PDF/A-1 standard but it co-exists alongside with an extended set of features.</p>

	PDF/A-1a and PDF/A-1b compliance are minimum essential for e-government records as recommended in the IFEG technical standard of DeitY.
JPEG2000 (ISO/IEC 15444-1:2004) and PNG (ISO/IEC 15948:2004)	Image file formats - which support lossless compression are recommended as raster image file formats for e-governance applications as specified in Technical Standards for Interoperability Framework for e-Governance (IFEG) in India, published in 2012 by e-Gov Standards Division, DeitY.
ISO/IEC 27002: 2005	Code of practices for information security management for ensuring the security of the e-records archived on digital storage.

10.23. Annexure 143 : Standards for Localization and Language Technology

1. Character Encoding Standard for Indian Languages

The lack of availability of information in the locally understandable language is the main reason for the slow progress in the Information and Communication Technology (ICT) sector. In today's age, access to ICT plays a major role in the overall development of a country, it has become a challenge to bridge the digital divide caused by the language barrier.

Standardisation is one of the baselines to be followed in localisation. Standardisation means to follow certain universally accepted standards, so that the developers from any part of the globe could interact through the application. Standardisation becomes applicable in almost everything specific to the language – for instance, a standard glossary of terms for translation, a standard keyboard layout for input system, a standard collation sequence order for sorting, a standard font etc.

Character Encoding standard for all constitutionally recognized Indian Languages should be such that it facilitates global data interchange.

ISCII is the National Standard and Unicode is the global character encoding standard. The average data packet size is less for representation of any Indian languages using ISCII. However, being limited code space, coexistence of multiple languages within the same code page is not possible in ISCII. The migration from ISCII to Unicode has become imperative due to the following reasons:

All major operating systems, browsers, editors, word processors and other applications & tools are supporting Unicode.

- It is possible to use Indian languages and scripts in the Unicode environment, which will resolve the compatibility issue.
- The documents created using Unicode may be searched very easily on the web.
- As Unicode is widely recognized all over the world and also supporting Indian languages, it will ease Localization applications including e-Governance application for all the constitutionally recognized Indian languages.
- Since Indian languages are also used in the other part of the world, it is possible to have Global data exchange.

Unicode shall be the storage-encoding standard for all constitutionally recognised Indian Languages including English and other global languages as follows:

Specification Area	Standard Name	Owner	Nature of the Standard	Nature of Recommend Actions
Character Encoding for Indian Languages	Unicode 5.1.0 and its future up-gradation as reported by Unicode consortium from time	Unicode Consortium, Inc.	Matured	Mandatory

	to time.			
--	----------	--	--	--

Character: Character is the smallest component of any written language that has semantic value.

ISCII: Indian Script Code for Information Interchange (ISCII - IS 13194:1991) is the character-encoding standard approved by Bureau of Indian Standards (BIS). ISCII is an 8 bit-encoding scheme, catering to 128 code spaces for representation of Indian languages.

Nine Indian scripts are included in ASCII standard to represent 10 Indian languages i.e. Assamese, Bengali, Devnagari, Gujarati, Gurmukhi, Kannada, Malayalam, Oriya, Tamil and Telugu.

Unicode: Unicode is a 16-bit character-encoding standard. All the major written scripts of the world are included in the Unicode Standard. The first version of Unicode was published in year 1991.

Unicode vis-à-vis ISO10646

Unicode is a 16 bit Character Encoding standard. All the major written scripts are included in the Unicode Standard. Indian scripts are also included in the standard. There are 22 constitutionally recognised Indian Languages, written in 12 different scripts. ISO/IEC 10646 is the character-encoding scheme evolved by the International Organisation for Standardisation (ISO) in 1990.

In 1991, the ISO Working Group responsible for ISO/IEC 10646 (JTC 1/SC 2/WG 2) and the Unicode Consortium decided to create universal standard for coding multilingual text. Since then, the ISO 10646 Working Group (SC 2/WG 2) and the Unicode Consortium are working together closely to extend the standard and to keep their respective versions synchronised.

In addition to the code tables as per ISO/IEC 10646, the Unicode Standard also provides an extensive set of character specifications, character data, algorithms and substantial technical material, which is useful for developers and implementers.

2. Font Standard for Indian Languages

A single International Standard to comply with UNICODE data storage. This ensures data portability across various applications and platforms.

True Type Fonts (TTF) was used in various applications earlier by various vendors. TTF had no encoding standard due to which vendors and developers had their own encoding schemes, thereby jeopardizing data portability. ISO/IEC 14496-OFF (Open Font Format) on the other hand is based on a single International Standard and complies with UNICODE for data storage. This ensures data portability across various applications and platforms. Open type font is a smart font which has built- in script composition logic.

Most often it has been observed that the use of proprietary fonts of different standards in Government Offices, which are not compatible with each other, is causing serious problems in information exchange amongst offices. By using Unicode compliant ISO/IEC 14496-OFF (Open Font Format) for font standard, the problem relating to the exchange of documents/files is completely solved.

Open standard under the International Organization for Standardization (ISO) within the MPEG group, which had previously adopted Open Type by reference, now adopted the new standard with appropriate language changes for ISO, and is called the "ISO/IEC 14496-OFF (Open Font

Format)" for which formal approval reached in March 2007 as ISO Standard ISO/IEC 14496-OFF (Open Font Format) and it is a free, publicly available standard.

ISO/IEC 14496-OFF (Open Font Format) for font standard would be the standard for Indian Languages in e-Governance Applications. **ISO/IEC 14496-OFF (Open Font Format) for font standard is mandatory for all 22 constitutionally recognized languages.**

TTF (True Type Font)

A Font Format developed by Apple and licensed to True type, is the native Operating System Font Format for Windows and Mac operating systems.

ISO/IEC 14496-OFF (Open Font Format)

OFF fonts allow the handling of large glyph sets using Unicode encoding. Such encoding allows broad international support for typographic glyph variants.

OFF fonts may contain digital signatures, which enable operating systems and browsing applications to identify the source and integrity of font files, (including the embedded font files obtained in web documents), before using them. Also, font developers can encode embedding restrictions in OFF fonts which cannot be altered in a font signed by the developer.

10.24. Annexure 154 : Standards for Metadata and Data

Standardization of data elements is the prerequisite for systematic development of e-Governance applications.

Data Standards may be defined as the agreed upon terms for defining and sharing data. Data Standards promote the consistent recording of information and are fundamental to the efficient exchange of information. They provide the rules for structuring information, so that the data entered into a system can be reliably read, sorted, indexed, retrieved, communicated between systems, and shared. They help protect the long-term value of data.

Once the data standards are in place, there is a need to manage data, information, and knowledge. Metadata of standardized data elements can be used for this purpose.

Metadata is structured information that describes, explains, locates or otherwise makes it easier to retrieve, use or manage an information resource. Metadata is often called data about data or information about information. A metadata is a matter of context or perspective -what is metadata to one person or application can be data to another person or application.

In other words, Metadata facilitates the user by providing access to the raw data through which the user can have an understanding of the actual data. Hence, Metadata is an abstraction layer that masks the underlying technologies, making the data access friendlier to the user.

Data and Metadata Standards provide a way for information resources in electronic form to communicate their existence and their nature to other electronic applications (e.g. via HTML or XML) or search tools and to permit exchange of information between applications.

The present document “Data and Metadata Standards- Demographic” focuses on Person Identification and Land Region codifications. It includes the following:

a) **Mechanism for allocation of reference no.** to the identified Generic data elements, and their grouping.

b) **Generic data elements** specifications like:

- Generic data elements, common across all Domain applications
- Generic data elements for Person identification
- Generic data elements for Land Region Codification
- Data elements to describe Address of a Premises, where a Person resides

c) **Specifications of Code Directories** like:

- Ownership with rights to update
- Identification of attributes of the Code directories
- Standardization of values in the Code directories

d) **Metadata of Generic Data Elements**

- Identification of Metadata Qualifiers

- Metadata of the data elements

e) Illustration of data elements to describe:

- Person identification
- Address of a premises

This Standard would be applicable to all e-Governance applications in India as per the Government's Policy on Open Standards (refer [http://egovstandards.gov.in/policy/policy-onopen-](http://egovstandards.gov.in/policy/policy-onopen-standards-for-e-governance/)

standards-for-e-governance/)

Reference Standards:

4. ISO Standard 1000:1992 for SI Units
5. MNIC Coding for Person Identification
6. ISO 693-3 for International language codes
7. RGI's coding schemes for Languages
8. Top level document provided by Working Group on Metadata and Data Standards
9. EGIF (e- Government Interoperability Framework) Standard of U.K.
10. [uidai.gov.in/UID_PDF/Working Papers/A_UID_Numbering_Scheme.pdf](http://uidai.gov.in/UID_PDF/Working_Papers/A_UID_Numbering_Scheme.pdf)
11. [http:// www.dolr.nic.in](http://www.dolr.nic.in) for conversion table of units as used by Department of Land Records
12. GoI Policy on open standards version 1.0 released in November, 2010
13. UID DDSVP Committee report, Version 1.0, Dec 09, 2009
14. ANSI92 Standard

10.25. Annexure 165 : Standards for Mobile Governance

Framework for Mobile Governance (m-Governance)

Mobile Governance (m-Governance) is a strategy and its implementation to leverage available wireless and new media technology platforms, mobile phone devices and applications for delivery of public information and services to citizens and businesses.

The m-Governance framework of Government of India aims to utilize the massive reach of mobile phones and harness the potential of mobile applications to enable easy and round the-clock access to public services, especially in the rural areas. The framework aims to create unique infrastructure as well as application development ecosystem for m-Governance in the country.

In cognizance of the vast **mobile phone subscriber base, peaked to more than 1 billion users in the country**, the Government has decided to also provision for access of public services through mobile devices, thereby establishing mobile Governance (m-Governance) as a compelling new paradigm.

Government of India will progressively adopt and deploy m-Governance in a time-bound manner to ensure inclusive delivery of public services to both the urban and rural populace in the country in accordance with this framework.

The following are the main measures laid down:

- i. Web sites of all Government Departments and Agencies shall be made mobile compliant, using the “**One Web**” approach.
- ii. **Open standards** shall be adopted for mobile applications for ensuring the interoperability of applications across various operating systems and devices as per the Government Policy on Open Standards for e-Governance.
- iii. **Uniform/ single pre-designated numbers** (long and short codes) shall be used for mobile-based services to ensure convenience.
- iv. All Government Departments and Agencies shall develop and deploy mobile applications for providing all their public services through mobile devices to extent feasible on the mobile platform. They shall also specify the service levels for such services.

The success of the proposed initiative on m-Governance will greatly depend upon the ability of the Government Departments and Agencies to provide frequently needed public services to the citizens, create infrastructure for anytime anywhere mobile-based services, adopt appropriate open standards, develop suitable technology platforms, make the cost of services affordable, and create awareness, especially for people in underserved areas.

To ensure the adoption and implementation of the framework in a time-bound manner, following actions will be taken:

1. Creation of Mobile Services Delivery Gateway (MSDG)

MSDG is the core infrastructure for enabling the availability of public services through mobile devices. This will be developed and maintained by an appropriate agency within DIT. MSDG is proposed to be used as a shared infrastructure by the Central and State Government Departments and Agencies at nominal costs for delivering public services through mobile devices.

Various channels, such as voice, text (e-mail and SMS), GPRS, USSD, SIM Toolkit (STK), Cell Broadcast (CBC), and multimedia (MMS) will be incorporated to ensure that all users are able to access and use the mobile based services. The various delivery channels are expected to entail innovative ways of providing existing services as well as development of new services.

To ensure successful implementation of the platform with requisite levels of security and redundancy, following actions will be taken:

a) **End User Interface:** End-user devices include landline phones, mobile phones, smart phones, personal digital assistants (PDAs), tablets, and laptops with wireless infrastructure. Mobile applications developed shall take into consideration appropriately the wireless-device interface issues, such as bandwidth limitations, micro-browser and micro-screen restrictions, memory and storage capacities, usability, etc.

b) **Content for Mobile Services:** Due to lower-bandwidth and smaller-screen characteristics of mobile devices, successful development and deployment of m-Governance will require development of separate mobile-ready content. Similarly, to meet the needs of all the potential users, the applications will need to be developed in the relevant local languages for the various channels of delivery. Open standards and open source software, to the extent possible, will be used to ensure interoperability and affordability of the content and applications developed.

c) **Mobile Applications (Apps) Store:** A mobile applications (m-apps) store will be created to facilitate the process of development and deployment of suitable applications for delivery of public services through mobile devices. The m-apps store shall be integrated with the MSDG and it shall use the MSDG infrastructure for deployment of such applications. It is proposed that the store will be based upon service oriented architecture and cloud based technologies using open standards as far as practicable. The open platform will be developed and deployed in conjunction with the MSDG for making the additional value added services available to the users irrespective of the device or network operator used by them

d) **Application Programming Interfaces (APIs) for Value-Added Services (VAS) providers:** MSDG shall offer suitable APIs to VAS providers with appropriate terms and conditions to ensure interoperability and compliance with standards for development of applications for delivery of public services.

e) **Mobile-Based Electronic Authentication of Users:** For electronic authentication of users for mobile-based public services, MSDG shall incorporate suitable mechanisms including

Aadhaar-based authentication. This will also help in ensuring appropriate privacy and confidentiality of data and transactions.

f) **Payment Gateway:** MSDG shall also incorporate an integrated mobile payment gateway to enable users to pay for the public services electronically.

g) **Participation of Departments:** The Government Departments and Agencies both at the Central and State levels will be encouraged to offer their mobile-based public services through the MSDG to avoid duplication of infrastructure.

2. Creation of Mobile Governance Innovation Fund

Department of Information Technology (DIT) shall create a Mobile Governance Innovation Fund to support the development of suitable applications by Government Departments and Agencies and also by third-party developers including start-ups. The fund shall be created and managed by DIT for a minimum period of 3 years. The objective of this fund will be to accelerate the development and deployment of the mobile applications across the entire spectrum of public services.

3. Creation of Knowledge Portal and Knowledge Management Framework on Mobile Governance

DIT shall develop and deploy a state-of-the-art knowledge portal and knowledge management framework that acts as a platform for awareness generation and dissemination for various Central Government Ministries and the State Governments. This will enhance the absorptive as well as the service provision capabilities of various stakeholders in m-Governance. Since m-Governance is in its nascent stage both in India and globally, the knowledge portal will act as a reference and guide for Government Departments and Agencies in India.

4. Creation of Facilitating Mechanism

An appropriate facilitating mechanism will be created to ensure compliance with the standards for mobile applications and ensure seamless interoperability of services and implementation of short and long codes for public services across multiple service providers. The proposed mechanism shall be established and managed by the Department of Information Technology, Government of India.

Guidelines for Delivery Channels for Provision of Public Services through Mobile Devices

The Objective is to provide:

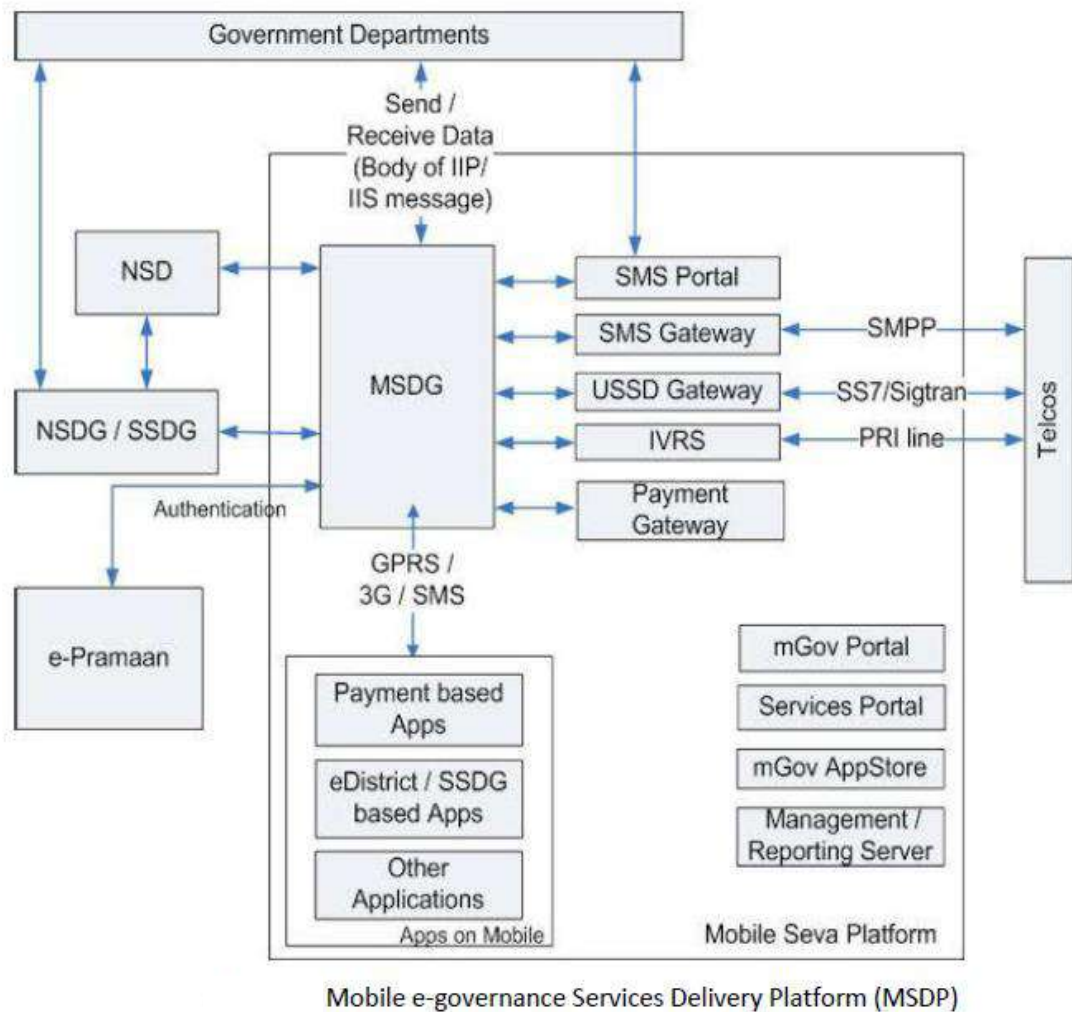
- a. Guidelines to deliver public services round-the-clock to the users using m-Governance
- b. Guidelines to develop standard based mobile solutions
- c. Guidelines to integrate the mobile applications with the common e-Governance infrastructure

As part of the initiative a shared technical infrastructure **Mobile Services Delivery Gateway (MOBILESEVA)** has been created to enable integration of mobile applications with the common e-Governance infrastructure and delivery of public services to the users.

The objective of creating the MOBILE SEVA is to put in place government-wide shared infrastructure and services to enable rapid development, mainstreaming and deployment of m-Governance services. It will enhance interoperability across various public services as well as reduce the total cost of operation of m-Governance services by providing a common pool of resources aggregating the demand for communication and e-Governance services, and act as a platform for various Government Departments and Agencies to test, rapidly deploy, and easily maintain m-Governance services across the country.

MSDP (Mobile e-governance Services Delivery Platform) provides an integrated platform for delivery of government services to citizen over mobile devices using Mobile Service Delivery Gateway (MSDG), SMS Gateway, m-App Store, m-Payment Services, Location Based Services (LBS), Unstructured Supplementary Services Data (USSD), Unstructured Supplementary Service Notify (USSN), Unstructured Supplementary Service Request (USSR), MMS, Cell Broadcasting Service (CBS), SIM Toolkit (STK), IVRS etc.

MSDG is a messaging middleware to facilitate e-Governance services delivery based on e-Governance Standard protocols which are IIP (Interoperability Interface Protocol), IIS (Interoperability Interface Specifications), IGIS (Inter-Gateway Interconnect Specifications) and Gateway Common Services Specifications (GCSS).



Mobile Application (m-Apps)

Mobile application software is applications software developed for handheld devices, such as mobile

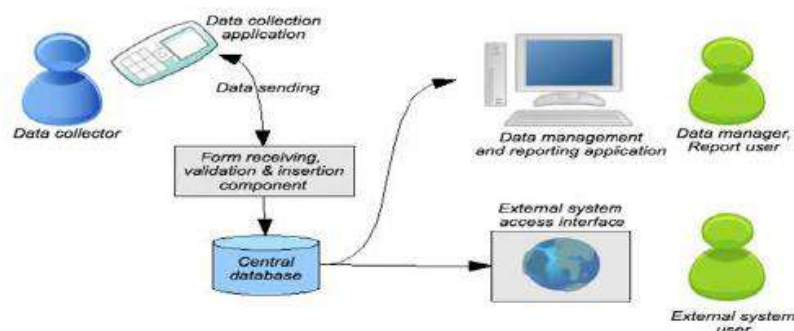
phones, tablets etc. These applications can be pre-installed on phones during manufacture or downloaded by users from various mobile software distribution platforms, or delivered as web applications using server-side or client-side processing (e.g. JavaScript) to provide an application like experience within a Web browser.

1. Mobile Application Dependency on Handset and O/S

Mobile Application software developers also have to consider a lengthy array of screen sizes, hardware specifications and configurations because of intense competition in mobile software and changes within each of the platforms.

2. Data Collection: m-forms

Mobile Application can also make use of the various forms for data collection. Many data collection systems are built from existing commercial or open source components, or even come packaged as an end-to-end solution. The components of data collection relate to each other as shown below:



The data collection may be done by various methods. Following are the most common types of data collection client applications which may be used:

1. **Fixed format SMS based Forms:** The 'client application' in this case is the phone's built-in SMS functionality. The user writes and sends SMS in a predefined format, representing answers to successive questions.

2. **Java Micro Edition Platform (J2ME) Application based Forms:** A J2ME application is written in the Java programming language, and loaded onto the phone over Bluetooth or by downloading the application from the Internet. To use the client application, the data collector navigates through questions in an application on the phone, which collects the answers and submits the completed form to a server.

3. **Mobile Operating System based Forms:** Mobile Operating Systems such as Android, Windows Mobile can also be used for developing native platform-dependent applications which can have various forms for data collection.

4. **Web-based Forms:** The 'client application' for web-based forms is the phone's web browser. The user browses to a website, where the form is published in an optimized format for mobile browsers.

5. **Voice-based based Forms:** The user dials a number and then chooses from options on a menu, useful when there are low levels of literacy among data collectors, or when a system is needed that caters for both landline and mobile phones.

6. **Wireless Internet Gateway (WIG) based Forms:** WIG uses a programming language (Wireless Markup Language, or WML) that is internal to almost all SIM cards. The menu definition is easy to write, but the size limit is 1MB, making it difficult to support long menus or multiple languages.

7. Unstructured Supplementary Service Data (USSD) based Forms: This is a real-time question-response service, where the user initiates a session and is then able to interact with the remote server by selecting numeric menu options. The phone needs to be continuously connected during the session, which needs a good, consistent signal.

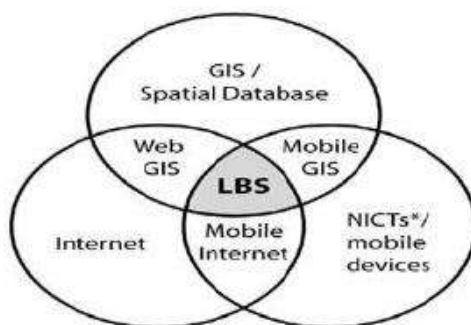
Once data has been captured on the phone, the completed form generally needs to be submitted to a central back-end server.

Other Mobile Technologies

1. Location Based Services (LBS)

Location-based services (LBS) denote services offered to mobile users according to their geographic location. LBS give the possibility of a two way communication and interaction. Therefore the user tells the service provider his actual context like the kind of information he needs, his preferences and his position. This helps the provider of such location services to deliver information tailored to the user needs. LBS enable to retrieve and share information related to their current position. For e.g. Google Latitude.

It works as an intersection of the following features in a system:



***NICT – New Information and Telecommunication technologies**

Geographical Information System (GIS) is a hardware, software and procedures designed to support the capture, management, manipulation, analysis, modelling and display of spatially referenced data for solving complex planning and management problems.

Internet is used to utilize the database dynamically so as to provide the appropriate service.

Mobile Devices as an end- device to execute the service.

2. Cell Broadcast Centre

Cell Broadcast is a mobile technology which allows text messages to be broadcasted to all mobile handsets and similar devices within a designated geographical area.

It is a one-to-many geographically focused service, in contrast to SMS which is a one-to-one or one-to-few service. It is usually used for providing location-based services, especially emergency services, as it utilizes minimum network resources for message broadcast and provides instantaneous delivery to all subscribers in a geographic area.

A Cell Broadcast message is an unconfirmed push service, meaning that the originator of the message does not know who has received the message, allowing for services based on anonymity. Mobile telephone user manuals describe how the user can switch the receiving of Cell Broadcast messages on or off.

Also known as Short message service-Cell Broadcast (SMS-CB), CB messaging is a mobile technology feature defined by the ETSI's GSM committee and is part of the GSM standard. It is also supported by UMTS, as defined by 3GPP.

a) Localization

Given that only a miniscule segment population in India can read and write English, it is important to deploy local/ regional languages to ensure all-round success of m-Governance initiatives. For detailed guidelines please refer to the Mobile Localization Guidelines.

b) Indian Language SMS

Currently, Indian language SMS services are offered by some operators but unlike the English SMS service, the language service is not necessarily interoperable across networks and cannot be availed on all types of handsets. The lack of a standard for Indian SMS comes in the way of providing scalable, interoperable and affordable SMS services in Indian languages.

To realise the goal of interoperable and affordable Indian language SMS, the following are the priority areas:

- i. **Text entry standards (i.e. keypad)**
 - ii. **Encoding standards to support all the major Indian languages**
 - iii. **Font support standardization for handsets to send and receive Indian language SMS**
- i. **Text entry methods**

The two methods in vogue are:

- a. **Mapping the Indian language characters on the handset keypad**
- b. **Screen-assisted text inputting mechanisms available from a few OEMs and vendors**

The keypad for the English language has been standardized by ITU. Although efforts on supporting the Indian languages on handheld devices are on, acceptable standards are yet to be evolved. In the absence of any national standards specifying mapping of the Hindi (and other Indian Languages) alphabets to the 12-key mobile devices, the handset vendors keen on penetrating the large Indian market are using their own mappings (which can differ across vendors).

ii. Encoding standard

The Unicode standard supports the 22 major Indian languages but uses more bandwidth (2 octets for each character) and hence the maximum size of SMS that can be sent using Unicode (70 characters) would be less than half of that of an English language SMS (170 characters).

iii. Font Support

Solutions for aesthetic display of Indian language scripts on small handset screens are being worked out. Similarly, solutions are tried out for handsets already in use so that they can receive and display messages in Indian languages, even if they cannot be used to send such messages.

3. Mobile Payment (M-Payment)

Mobile payment is an alternative payment method. Instead of paying with cash, check, or credit cards, a consumer can use a mobile phone to pay for a wide range of services; after having authenticated the user using AADHAR or any other means. The basic aim of mobile payments is to enable micropayments on low-end mobile devices which support only voice and text, in addition to higher end phones which could support web-browsing or Java application capabilities.

a. Mobile banking (M-Banking or mBanking)

M-Banking is a term used for performing balance checks, account transactions, payments, credit applications and other banking transactions through a mobile device. The earlier mobile banking services were offered over SMS, a service known as SMS banking. With the introduction of smart phones with WAP support the mobile web is also being used for M-Banking. Latter with the advancements of web technologies such as HTML5, CSS3 and JavaScript it became feasible to launch mobile web based services to compliment native and hybrid applications.

b. Immediate Mobile Payment Services (IMPS)

The Immediate Mobile Payment System (IMPS) has been developed by the National Payments Corporation of India (NPCI) to expand the scope of mobile payments to all sectors of the population. IMPS offer an instant, 24X7, interbank electronic fund transfer service through mobile phones.

An IMP provides an inter-operable infrastructure to the banks for enabling interbank real time funds transfer transactions. IMPS rides on the existing NFS Interbank ATM transaction switch infrastructure and message format making it easy for banks to adopt.

To enable the transfer of money, both the sender and the receiver of payment have to link their bank accounts with their phone numbers through their respective banks. The sender has to register for mobile banking service with her/his bank. Upon registration, the bank will provide a link to the Mobile banking software which needs to be installed in the mobile phone to enable payments.

Both the sender and the receiver will receive a Mobile Money Identifier (MMID) while the sender will also receive a Mobile PIN (MPIN) for authentication of transactions. While transacting, the sender has to input the MPIN, receiver's mobile number and MMID, and the amount of funds to transfer.

IMPS will authenticate the sender, check the receiver's mobile number and MMID, and transfer the funds to the receiver's account in real-time. Both the sender and the receiver receive messages notifying them about the success or failure of the transaction.

c. Contactless cards and Mobile Phones

These cards are based upon a technology known as NFC (Near Field Communication) that allows NFC enabled cards to be ready by taping them on or by passing them by, a card reader than swiping them through or inserting into, the POS terminal. They are now being integrated into mobile phone handset for m-Payments.

NFC enabled phones are expected to become more widely available. The NFC chip inside the phone will be connected to the secure element within the SIM card, allowing information stored in an m-wallet to be accessed by the NFC card reader. Authorization for payments involves entering a PIN.

d. Airtime balance for payment

Airtime as balance for payment was realized because of the need for the unbanked majority to easily and cheaply transfer funds around the country. The facility required is the most basic of mobile phones, an account, which can be opened at any one of vendors to start transferring and receiving money.

Since the system uses either SIM toolkit or USSD technology depending on the country, the network charges are minimal to non-existent. It has lowest entry barriers, since it works on more than 95 percent of handsets and has low transaction costs and no bank account or credit card required.

e. Mobile Wallet

A Mobile Wallet is functionality on a mobile device that can securely interact with digitized valuables thereby making payments using the mobile phone. Mobile wallet may reside on a phone or on a remote network / secure servers. It is controlled by the user of the wallet.

Using a mobile wallet to make a payment is incredibly simple. When it is time to pay, the user turns on his or her phone's screen (if the screen is off, when the phone is dormant for instance, the NFC chip will not work), opens the wallet application, enters their pin number, and passes the phone within a few inches of the contactless payment symbol. The payment transaction is then processed just like a conventional card transaction. In addition, relevant offers, discounts, and coupons can be passed from the wallet along with the payment in that same tap of the phone.

4. SIM Application Toolkit

The SIM Application Toolkit is a standard set of commands, under GSM, which defines how the card should interact with the outside world and extends the communication protocol between the card and the handset. It is designed as a client server application.

With SIM Application Toolkit, the card has a proactive role in the handset, i.e., the SIM initiates commands independently of the handset and the network. This enables the SIM to build up an interactive exchange between a network application and the end user and access, or control access to, the network. The SIM also gives commands to the handset such as displaying menus and/or asking for user input.

10.26. Annexure 176 : Standards for GIGW**Guidelines for Indian Government Websites**

India, the largest democracy in the world, is set to emerge as an ICT Superpower in this millennium. Realising the recognition of ‘electronic governance’ as an important goal by Governments world over, Indian Government has also laid a lot of emphasis on anytime, anywhere delivery of Government services. As of today, there are over five thousand Government websites in India.

Awareness about the fast changing ICT world and keenness to keep pace with the latest has ensured that almost all the State Governments in India already have their websites up and running. In fact each state has multiple websites belonging to different Departments.

However, these websites follow different Technology Standards, Design Layouts, Navigation Architecture, or, in simple terms, different look and feel as well as functionality.

The need for standardisation and uniformity in websites belonging to the Government cannot be stressed enough, in today’s scenario.

As a first step, it is suggested that the Indian Government websites adhere to certain common minimum standards which have been derived, in the form of guidelines discussed in this document, as prerequisites for a Government website to fulfil its primary objective of being a citizen centric source of information & service delivery. These guidelines could eventually form the basis for establishment of the desired standards.

Compliance to these guidelines will ensure a high degree of consistency and uniformity in the content coverage and presentation and further promote excellence in Indian Government Web space.

These Guidelines have been framed with an objective to make the Indian Government Websites conform to the essential pre-requisites of UUU trilogy i.e. Usable, User-Centric and Universally Accessible. They also form the basis for obtaining Website Quality Certification from STQC (Standardisation Testing Quality Certification) an organisation of Department of Information Technology, Government of India.

These Guidelines are based on International Standards including ISO 23026, W3C’s Web Content Accessibility Guidelines, Disability Act of India as well as Information Technology Act of India.

A. Indian Government Entity

All websites and Portals belonging to the Indian Government Domain at any hierarchical level (Apex Offices, Constitutional Bodies, Ministries, Departments, Organisations, States/UTs, District Administrations, and Village Panchayats et al) must prominently display a strong Indian Identity and ownership of Indian Government.

The above objective can be achieved through the following:

1. The National Emblem of India MUST be displayed on the Homepage of the websites of Central Government Ministries/Departments. The usage of National Emblem on an Indian

Government website must comply with the directives as per the ‘State Emblem of India (Prohibition of improper use) Act, 2005’.

Further, the State Governments should also display the State Emblem (or the National Emblem in case the State has adopted the National Emblem as its official State Emblem) as per the Code provided in the above Act. The Public Sector organisations and autonomous bodies should display their official logo on the Homepage of the website to re-enforce their identity.

2. The Homepage and all important entry pages of the website **MUST** display the ownership information, either in the header or footer.
3. The lineage of the Department should also be indicated at the bottom of the Homepage and all important entry pages of the website. For instance, at the bottom of the Homepage, the footer may state the lineage information, in the following manner:
 - i. This Website belongs to Department of Heavy Industries, Ministry of Heavy Industries and Public Enterprises, Government of India’ (for a Central Government Department).
 - ii. This Website belongs to Department of Industries, State Government of Himachal Pradesh, India’ (for a State Government Department).
 - iii. This is the official Website of Gas Authority of India Limited (GAIL), a Public Sector Undertaking of the Government of India under the Ministry of Petroleum and Natural Gas (for a Public Sector Undertaking).
 - iv. This is the official Website of the District Administration of Thanjavur, State Government of Tamil Nadu (India)’ (for a District of India).
4. All subsequent pages of the website should also display the ownership information in a summarised form. Further, the search engines often index individual pages of a website and therefore, it is important that each webpage belonging to a site displays the relevant ownership information.
5. In case of those websites which belong to Inter-Departmental initiatives involving multiple Government Departments which are difficult to list on the Homepage, the Government ownership should still be reflected clearly at the bottom of the page with detailed information provided in the ‘About the Portal/Website’ section.
6. The page title of the Homepage (the title which appears on the top bar of the browser) **MUST** be complete with the name of the country included, for instance, instead of the title being just Ministry of Health and Family Welfare, it should state, Government of India, Ministry of Health & Family Welfare.

Alternatively, in case of a State Government Department, it should state ‘Department of Health, Government of Karnataka, India ‘. This will not only facilitate an easy and

unambiguous identification of the website but would also help in a more relevant and visible presence in the search engine results. Further, it is important since the screen readers used by the visually impaired users first read the title of the page and in case the title is not explanatory enough, it may confuse or mislead them.

B. Government Domains

The URL or the Web Address of any Government website is also a strong indicator of its authenticity and status as being official. In today's era with a large proliferation of websites, which resemble Government websites and fraudulently claim to provide reliable Government information and services, the role of a designated Government domain name assumes a lot of significance.

Hence, in compliance to the Government's Domain Name Policy, all Government websites MUST use 'gov.in' or 'nic.in' domain exclusively allotted and restricted to Government websites. The military institutions and organisations in India may also use 'mil.in' domain in place of or in addition to the gov.in /.nic.in domain. The above naming policy applies to all Government websites irrespective of where they are hosted.

Those Departments and Government entities that are using and have been publicising a domain name other than the above should take appropriate early action to register official government domain names and use the existing ones as 'alias' for a period of six months. An intermediary page with a clear message notifying the visitors about the change in the URL and then auto redirecting them to the new URL after a time gap of 10 seconds should be used.

The Domain Name Conventions, as specified in the '.IN Registration' policy should be followed while registering a 'gov.in' Domain Name.

National Informatics Centre (NIC) is the exclusive Registrar for GOV.IN domain names. The use of GOV.IN Domain is restricted to the constituents of Indian Government at various levels right from Central, State/UT, District & Sub-District, block, village etc.

For detailed information and step-by-step procedure on how to register a .GOV IN Domain, one may visit <http://registry.gov.in> .

C. Link with National Portal

- 1) **india.gov.in:** The National Portal of India is a single window source for access to all information and services being provided by the various constituents of the Indian Government to its citizens and other stakeholders.

There are exclusive sections on Citizens, Business, Overseas, Government, Know India, Sectors etc. catering to the information needs. Sections targeting special interest groups such as Government Employees, Students, Senior Citizens, Kids etc. are also present.

a) Since the National Portal is the official single entry Portal of the Indian Government, all Indian Government websites MUST provide a prominent link to the National Portal from the Homepage and other important pages of citizens' interest.

b) The pages belonging to the National Portal MUST load into a newly opened browser window of the user. This will also help visitors find information or service they could not get on that particular website. It is quite common that citizens are not aware which information or service is provided by which Department.

As per linking Policy of the National Portal, no prior permission is required to link 'india.gov.in' from any Indian Government website. However, the Department providing a link to the National Portal is required to inform the National Portal Secretariat about the various sections of the National Portal that they have linked to, so that they can be informed of any changes, updations / additions therein. Also, it is not permitted that the National Portal Pages be loaded into frames on any site. These must be loaded into a new browser window.

Special Banners in different sizes and colour schemes for providing a link to the National Portal have been given at <http://india.gov.in/linktous.php>

Instructions on how to provide a link have also been given. The Government websites / portals may choose any banner from the ones provided, depending upon their site design and place the same on their Homepage.

D. Content Copyright

Copyright is a form of protection provided under law to the owners of “original works of authorship” in any form or media. It is implied that the original information put up on the website by a Government Department is by default a copyright of the owner Department and may be copied, reproduced, republished, uploaded, posted, transmitted, or distributed only if the copyright policy of the concerned Department allows so.

Hence, the information, material and documents made available on an Indian Government website MUST be backed up with proper copyright policy explaining the terms and conditions of their usage and reference by others. The copyright policy of a Department could be liberal, moderate or conservative depending upon their preferences based on the kind of information available on their website. However, since it is a duty of a Government Department to provide all the information in the public domain freely to the citizens, the Departments should aim to have a liberal copyright policy.

The Departments should also be sensitive towards publishing any information having a third party copyright. The Government Departments MUST follow proper procedures to obtain the permission, prior to publishing such information on their websites.

If any published Government Document/Report is being reproduced on any website, whether as excerpts or in full, the source of the same i.e. Full Title of the Report/Document along with the name of the concerned Department and year of publication MUST be provided.

E. Content Hyper linking

Since Government websites often receive queries and requests from owners of other websites who might want to provide a hyper link to their web pages, every Indian Government website

MUST have a comprehensive and clear-cut hyper linking policy defined and spelt out for those who wish to hyper link content from any of its sections. The basic hyper linking practices and rules should ideally be common across the websites of a State/Ministry.

The hyperlinking policy enumerating the detailed criteria and guidelines with respect to hyperlinks with other sites may be made available under the common heading of **‘Hyperlinking Policy’** and displayed at a common point on the Homepage of all sites under the ownership a State/Ministry.

- a) To create a visual distinction for links that lead off site, Cascading Style Sheets (CSS) controls or XSL or some such similar mechanism should be used. In case the link takes the user to another website of the same Department/Ministry/ State, a seamless transition should be used through appropriate CSS controls.
- b) Third party content should only be linked when consideration about the copyright, terms of use, permissions, content authenticity and other legal and ethical aspects of the concerned content have been taken into account.
- c) The overall quality of a website’s content is also dependent, among other things on the authenticity and relevance of the ‘linked’ information it provides.
- d) Further, it MUST be ensured that ‘broken links’ or those leading to ‘Page Not Found’ errors are checked on a regular basis and are rectified or removed from the site immediately upon discovery.

F. Privacy Policy

Government websites should follow an extremely cautious approach when it comes to collecting personal details/information about the visitors to the sites. It should be an endeavour to solicit only that information which is absolutely necessary.

In case a Department solicits or collects personal information from visitors through their websites, it MUST incorporate a prominently displayed Privacy Statement clearly stating the purpose for which information is being collected, whether the information shall be disclosed to anyone for any purpose and to whom.

Further, the privacy statement should also clarify whether any cookies shall be transferred onto the visitor’s system during the process and what shall be the purpose of the same.

Whenever a Department’s website allows e-commerce and collects high risk personal information from its visitors such as credit card or bank details, it MUST be done through sufficiently secure means to avoid any inconvenience. SSL (Secure Socket Layer), Digital Certificates are some of the instruments, which could be used to achieve this.

10.27. Annexure 187 : Standards for Open APIs

Policy on Open Application Programming Interfaces (APIs)

Under the overarching vision of Digital India, Government of India (GoI) aims to make all Government services digitally accessible to citizens through multiple channels, such as web, mobile and common service delivery outlets.

To meet this objective, there is a need for an interoperable ecosystem of data, applications and processes which will make the right information available to the right user at the right time.

Interoperability among various e-Governance systems is an important prerequisite for upgrading the quality and effectiveness of service delivery. For promoting Open Standards for software interoperability across various Government departments and agencies, GoI has already notified the “Policy on Open Standards for e-Governance” and “Technical Standards on Interoperability Framework for e-Governance”.

Open API is the API that has been exposed to enable other systems to interact with that system. Open API may be either integrated with the host application or may be an additional piece of software that exposes any proprietary API with an Open API equivalent. The Open API, whenever possible, may be free of charge and without restrictions for reuse & modifications.

Policy on Open APIs for Government of India” (hereinafter referred to as the “Policy”) will encourage the formal use of Open APIs in Government organizations. This policy sets out the Government’s approach on the use of “Open APIs” to promote software interoperability for all e-Governance applications & systems and provide access to data & services for promoting participation of all stakeholders including citizens.

The objectives of this policy are to:

- i. Ensure that APIs are published by all Government organisations for all e-Governance applications and systems.
- ii. Enable quick and transparent integration with other e-Governance applications and systems.
- iii. Enable safe and reliable sharing of information and data across various e-Governance applications and systems.
- iv. Promote and expedite innovation through the availability of data from e-Governance applications and systems to the public.
- v. Provide guidance to Government organizations in developing, publishing and implementation using these Open APIs.

Government of India shall adopt Open APIs to enable quick and transparent integration with other e-Governance applications and systems implemented by various Government

organizations, thereby providing access to data & services and promoting citizen participation for the benefit of the community.

The Open APIs shall have the following characteristics for publishing and consumption:

- i. The relevant information being provided by all Government organisations through their respective e-Governance applications shall be open and machine readable.
- ii. All the relevant information and data of a Government organisation shall be made available by Open APIs, as per the classification given in the National Data Sharing and Accessibility Policy (NDSAP-2012), so that the public can access information and data.
- iii. All Open APIs built and data provided, shall adhere to National Cyber Security Policy.
- iv. The Government organizations shall make sure that the Open APIs are stable and scalable.
- v. All the relevant information, data and functionalities within an e-Governance application or system of a Government organisation shall be made available to other e-Governance applications and systems through Open APIs which should be platform and language independent.
- vi. A Government organisation consuming the data and information from other e-Governance applications and systems using Open APIs shall undertake information handling, authentication and authorisation through a process as defined by the API publishing Organisation.
- vii. Each published API of a Government organization shall be provided free of charge whenever possible to other Government organizations and public.
- viii. Each published API shall be properly documented with sample code and sufficient information for developers to make use of the API.
- ix. The life-cycle of the Open API shall be made available by the API publishing Government organisation. The API shall be backward compatible with at least two earlier versions.
- x. All Open API systems built and data provided shall adhere to GoI security policies and guidelines.
- xi. Government organizations may use an authentication mechanism to enable service interoperability and single sign-on.

The policy shall be applicable to all Government organisations under the Central Government and those State Governments that choose to adopt this policy for the following categories of e-Governance systems:

- All new e-Governance applications and systems being considered for implementation.
- New versions of the legacy and existing systems.

10.28. **Annexure 198 : Standards for Internet of Things**

1. Sensor & Actuators

a. IEEE 1451

IEEE 1451 is a set of smart transducer interface standards developed by the Institute of Electrical and Electronics Engineers (IEEE) Instrumentation and Measurement Society's Sensor Technology Technical Committee describing a set of open, common, network-independent communication interfaces for connecting transducers (sensors or actuators) to microprocessors, instrumentation systems, and control/field networks.

b. Identification Technology

ISO/IEC JTC 1/SC31 Automatic identification and data capture techniques

It develops and facilitates standards within the field of automatic identification technologies. These technologies include 1D and 2D barcodes, active and passive RFID for item identification and OCR.

c. Domain Specific Compliance:

Sensors/IoT Devices/Actuators should follow the compliance to respective domain specific standards, like healthcare devices HL7, automobile/bus UBS-II (ITS sensor parameter & standards), OBD-II, Electric Vehicle Charging etc.

2. Communication Technology

a. Thread:

Networking protocol called Thread that aims to create a standard for communication between connected household devices.

b. AllJoyn:

Open source AllJoyn protocol was initially developed by Qualcomm provides tools for the entire process of connecting and maintaining devices on a Wi-Fi network.

c. IEEE 802.15.4:

It offers physical and media access control layers for low-cost, low-speed, low-power Wireless Personal Area Networks (WPANs).

IEEE 802.15.4e-2012, IEEE 802.15.4-2011, IEEE 802.15.4-2003, IEEE 802.15.4-2006

d. IETF IPv6 over Low power WPAN (6LoWPAN):

It defines encapsulation and header compression mechanisms that allow IPv6 packets to be sent to and received over IEEE 802.15.4 based networks.

6LoWPAN Frame Format

Fragmentation and Reassembly

Header Compression

Support for security mechanisms

e. IETF “Routing Over Low power and Lossy (ROLL):

IPv6 Routing Protocol for Low power and Lossy Networks (LLNs) (RPL)
 RPL Topology Formation (Destination Oriented Directed Acyclic Graphs - DODAGs)
 RPL Control Messages

f. IETF Constrained Application Protocol (CoAP):

It offers simplicity and low overhead to enable the interaction and management of embedded devices.

3. Use Case/ Application Specific:

i. Industrial IoT (IIoT): Object Modelling Group (OMG) has been active in IIoT standardization efforts. OMG IIoT standards and activities include (but are not limited to):

- Data Distribution Service (DDS)
- Dependability Assurance Framework For Safety-Sensitive Consumer Devices
- Threat Modelling
- Structured Assurance Case Meta-model
- Unified Component Model for Distributed, Real-Time and Embedded Systems
- Automated Quality Characteristic Measures
- Interaction Flow Modelling Language™ (IFML™)

(Source: <http://www.omg.org/hot-topics/iiot-standards.htm>)

ii. eHealth: IEEE has many standards in the eHealth technology area, from body area networks to 3D modelling of medical data and personal health device communications. IEEE 11073 standards are designed to help healthcare product vendors and integrators create devices and systems for disease management.

iii. eLearning: The IEEE Learning Technology Standards Committee (LTSC) is chartered by the IEEE Computer Society Standards Activity Board to develop globally recognized technical standards, recommended practices, and guides for learning technology.

iv. Intelligent Transportation Systems (ITS): IEEE has standards activities on many aspects of ITS, such as vehicle communications and networking (IEEE 802 series), vehicle to grid interconnectivity (IEEE P2030.1), addressing applications for electric sourced vehicles and related support infrastructure, and communication for charging (IEEE 1901).

4. Consortia

a. Open Interconnect Consortium:

OIC (Atmel, Dell, Broadcom, Samsung, and Wind River as members) is an open environment to support the billions of connected devices coming online.

b. Industrial Internet Consortium:

It was founded by Intel, Cisco, AT&T, GE & IBM with the goal of developing standards specifically for industrial use of the Internet of Things.

5. Architecture Technology

a. IEEE P2413: Standard for an Architectural Framework for the Internet of Things

The architectural framework for IoT provides a reference model that defines relationships among various IoT verticals (e.g., transportation, healthcare, etc.) and common architecture elements.

The standard also provides a reference architecture that builds upon the reference model. The reference architecture covers the definition of basic architectural building blocks and their ability to be integrated into multi-tiered systems.

6. Further Readings for Standards

a. ITU Standardization Roadmap

This document was released on 6 May 2016. It contains a collection of Standards/ITU-T Recommendations that fit into the scope of Joint Coordination Activity for IoT and Smart Cities. It includes Standards/ITU-T Recommendations related to Internet of Things (IoT), smart cities and communities (SC&C), network aspects of identification systems, including RFID (NID) and ubiquitous sensor networks (USN). Refer References for the link.

b. IERC Position Paper on IoT Standardization:

It presents an inventory of existing standards and provides an overview of past and current activity in relation to standardization in the area of Internet of Things, and assembles a series of examples of standardization activities in this area.

10.29. Annexure 29 : Standards for Disaster Management

The aim of the local disaster management standards and guidelines is to support local government / municipal corporations to develop a community specific disaster management system, including governance arrangements, a Local Disaster Management Plan (LDMP) using the comprehensive approach to disaster management.

This standard establishes a common set of criteria for all hazards disaster/emergency management with fundamental criteria to develop, implement, assess, and maintain the program for prevention, mitigation, preparedness, response, continuity and recovery.

International Standards used in Disaster Warning and Management

S. No.	Standards	Description
1.	ISO 22320:2011	Societal security – Emergency management – Requirements for incident response deals with overall approach for preventing and managing emergencies /disasters
2.	ISO 22322:2015	Societal security -- Emergency management -- Guidelines for Public warning deals with guidelines for developing, managing, and implementing Public warning before, during, and after incidents / disasters
3.	ISO 22324:2015	Societal security — Emergency management — Guidelines for colour-coded alerts deals with guidelines for the use of colour codes to inform people at risk as well as first response personnel about danger and to express the severity of a situation. It is applicable to all types of hazard in any location.
4.	ISO 31000:2009, <i>Risk management – Principles and guidelines</i>	It deals with principles, framework and a process for managing risk. It helps organizations / local bodies to increase the likelihood of achieving objectives, improve the identification of opportunities and threats and effectively allocate and use resources for risk treatment.
5.	IEC 31010:2009, <i>Risk management - Risk assessment techniques</i>	It helps the decision makers understand the risks that could affect the achievement of objectives as well as the adequacy of the controls already in place. It focuses on risk assessment concepts, processes and the selection of risk assessment techniques.
6.	ISO 11320:2011	Nuclear criticality safety -- Emergency preparedness and response
7.	ASCE/SEI 41-06 - <i>Seismic Rehabilitation of Existing Buildings</i>	Standards for Seismic retrofitting of existing building including steps to better protect non-structural components (suspended ceilings, non-load-bearing walls and utility systems) and building contents (furnishings, supplies, inventory and equipment)
8.	ISO 19115-1:2014	Defines the schema required for describing geographic information and services by means of metadata. It provides information about the identification, the extent, the quality, the spatial and temporal aspects, the content, the spatial reference, the portrayal, distribution, and other properties of digital geographic data and services

----- End of the Document -----