Govt. of Bihar

PATNA SMART CITY LIMITED

Addresss: 5th floor, Biscomaun Bhawan, Patna- 800001,

Email: patnasmartcity.pscl@gmail.com, Website: smartpatna.co.in

SHORT NOTICE INVITING QUOTATION

(for determining rates)

RFQ No.- NIQ-06/MD/ PSCL/2020-21

Quotations are invited by Patna Smart City Ltd. (PSCL) for non SOR items, related to Integrated Command & Control Center (ICCC) in Patna latest by 17:00 hours on 07.04.2021. The detailed Technical Specifications uploaded on PSCL website smartpatna.co.in may be referred for details.

Managing Director

Patna Smart City Limited

PR. No. 15022 (NI NI) 20-21

NIQ-6/MD/PSCL/2020-21 dated 26/03/2021

Notice Inviting Quotation
for
Master System Integrator
for
Implementation of Integrated Smart Solutions
at
Patna

(*In short: ICCC Project*)

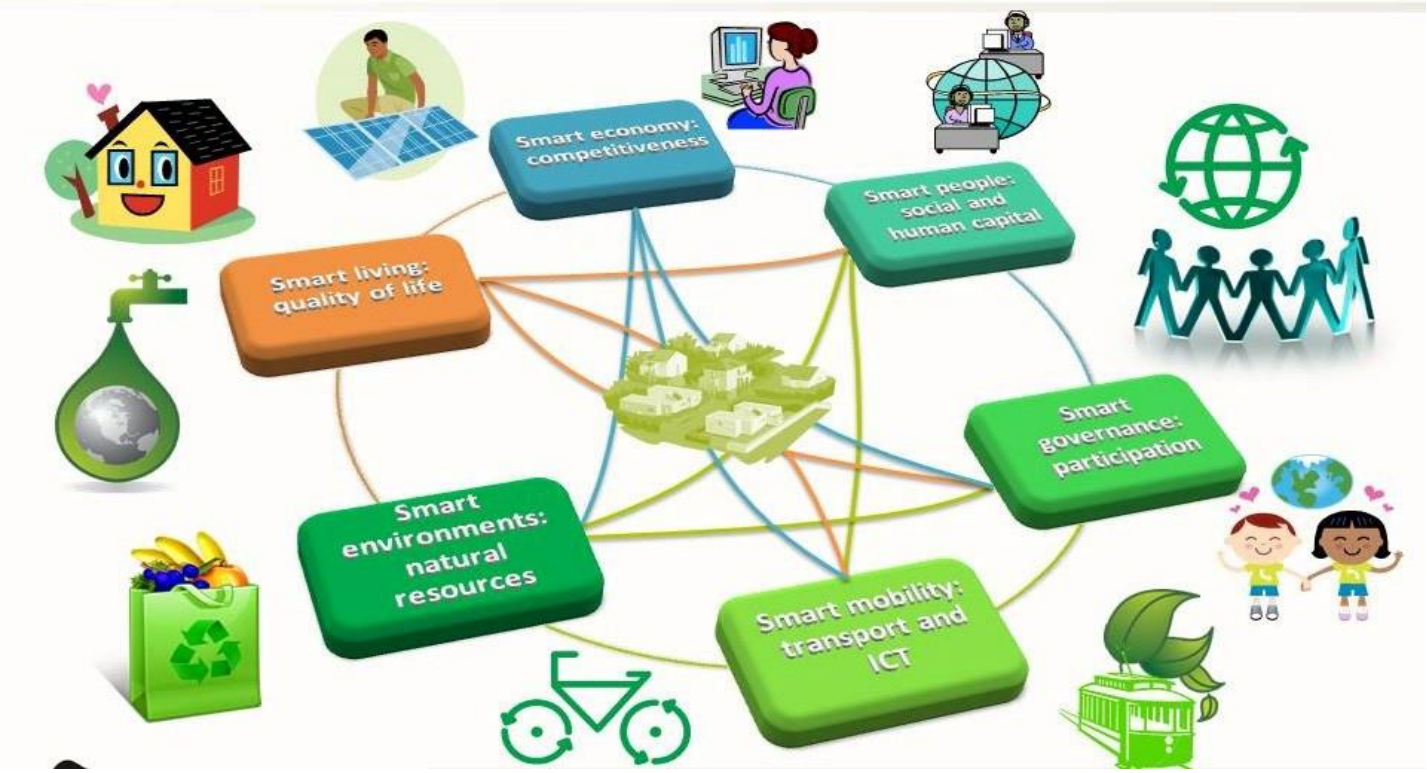


Table of Contents

ACRONYMS & ABBREVIATIONS

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
BPR	BUSINESS PROCESS RE-ENGINEERING
BSNL	BHARAT SANCHAR NIGAM LIMITED
BSRTC	BIHAR STATE ROAD TRANSPORT CORPORATION
BSWAN	BIHAR STATE WIDE AREA NETWORKS
CBD	CENTRAL BUSINESS DISTRICT
CCC	CIRCUIT CROSS-CONNECT
CCTV	CLOSED CIRCUIT TELEVISION
CMM	CAPABILITY MATURITY MODEL
COTS	COMMERCIAL OFF-THE-SHELF
CSC	COMMON SERVICE CENTRE
CSP	CLOUD SERVICE PROVIDER
CSV	COMMA SEPARATED VALUES
CTI	COMPUTER TELEPHONY INTEGRATION
DBMS	DATA BASE MANAGEMENT SYSTEM
DBO	DESIGN, BUILD, OPERATE
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
DPR	DETAILED PROJECT REPORT
DR	DISASTER RECOVERY
DRC	DISASTER RECOVERY CENTRE
DTMF	DUAL-TONE MULTI-FREQUENCY SIGNALING

1. BACKGROUND

1.1 Smart City Mission:

Main objective of Smart City Mission is to promote cities to provide core infrastructure and give a decent quality of life to its citizens, a clean and sustainable environment with application of 'Smart' Solutions

1.2 Project Objective:

The purpose of Smart Cities Mission is to drive economic growth and improvequality of life of people by enabling local area development and harnessing technology, especially technology that leads to Smart outcomes. Area-baseddevelopment will transform existing areas (retrofit and redevelop); including slums, into better planned ones, thereby improving livability of the whole City.

The objective 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.

The scope of work for the ICCC Data Center and sub -component includes

- Integrated Command and Control Center
- Disaster Recovery Center
- Intelligent Traffic Management System
- Public Wi-Fi Hotspot
- OFC Laying

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:

a) Improved visualization of ambient or emergency situation in the city and

facilitationof data driven decision making

b) Efficient traffic management
c) Enhanced safety and security
d) Better management of utilities and quantification of services
e) Asset Management
f) Disaster Management and Emergency Response
g) Efficiency improvement in public service delivery
h) Inter-departmental coordination and collaboration for faster execution of services
i) 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. Data Centre
    iv. Disaster Recovery Centre
    v. Integrated Command and Control Centre
    vi. ICT Enabled Solid Waste Management
    vii. Intelligent Traffic Management System
    viii. E-Challan System
    ix. Public Bike Sharing
    x. Smart Water Supply System
    xi. Smart Education
    xii. Smart Health Management System
    xiii. Intelligent Public Transport Management
    xiv. Smart Pole
    xv. Smart Energy Management System

The objective of the proposed project is to:

i. Ensure, through use of technology, prompt availability of professionally equipped personnel to reach to authority
ii. Increased and demonstrative presence/visibility in public places through installation of CCTV cameras
iii. Quick and effective response system to address the needs of citizen of Patna

iv. 24x7 CCTV monitoring of public areas frequently visited by people and susceptible to crime or abnormal behaviour of human.

v. Integration of location-based services existing databases of applications running in state level data centre with CCTV feeds for prompt and effective resolution of any issues at public places.

vi. Analysis of video and creation of actionable warnings/alerts for preventive and curative actions.

Following are the key objectives and intended outcomes:

i. **Security and Safety- Quick and effective emergency response system**

a. Live surveillance and alerts in case of an incident through a network of cameras

b. Greater coverage and surveillance of public places frequently used by people within the city, with more eyes on the streets

c. Supporting operations to meet any contingency situation

d. Prevention and detection of street crimes and apprehending offenders to deter criminal activities.

e. Enhancement in prediction capability through Ai based analytics, which will help in preventive and predictive measures

f. Providing surveillance in areas having higher concentration of women residences based on Hot Spots, especially of students and working women (e.g. localities having women hostels, paying guest accommodations, etc.)

g. Identification of Areas prone to crime against women or crime targeting women such as snatching incidences, eve teasing etc.

h. Identification of areas frequented by women, such as girls' Schools/Colleges, Market places, transport hubs, etc.

i. Provide emergency service assistance to women in distress.

ii. **Improved Management**

j. Decision making tool in maintaining law and order in the city

k. Acting as a tool for Police and other government agencies in monitoring and maintaining their functions

l. Providing a framework to all the stakeholders, so that there is proportionality and transparency in their use of surveillance

m. Ensuring scalability and interoperability of systems

iii. **Integrations and scalability**

n. Integration of various existing database which help in training of data and implementing AI algorithm for smart city project

o. Identification of sensitive, accident prone area and hot spots in the city

p. Disciplined traffic system

q. Ensures scalability and interoperability of systems

r. Integration of existing / proposed different CCTV projects

iv. **Process Commissioning through ICT (Information and communication Technology)**

s. Installation of CCTV surveillance covering the priority hot spot areas

t. Automated number plate recognition i.e. ANPR to be deployed in extremely sensitive areas around hotspots of crime

u. Provides greater coverage of surveillance within the city

v. **Skill enhancement**

v. The system as envisaged, will enhance the skills of operations through ICT interventions, which will enable officers to effectively utilize technology to monitor and reduce crime and with efficiently achieving the objectives.

1.3 Key components of solution :

a. City Surveillance:

Protecting citizens and ensuring public safety is one of the topmost priorities for any Government agency. It requires advanced security solutions to effectively fight threats from activities of terrorism, organized crime, vandalism, burglary, random acts of violence, and all other forms of crime. CCTV based video surveillance is a security enabler to ensure public safety. This includes a combinationof various types of cameras including fixed, PTZ, panoramic, ANPR cameras with dayand night capabilities, along with edge based video analytics for incident based monitoring of the key locations of the city.

b. City Wi-fi:

The citywide public Wi-Fi enables the citizens to access internet Wi-Fi serviceson their

handheld devices in designate public spaces. The city enables this facility using aservice provider and creating the required infrastructure at the field level. These servicescan be monitored and managed through the Integrated Command and Control Centre.

c. Smart Lighting:

This intervention requires the replacement of the current street lighting system with Smart LED street lights. In case the city has already installed LED Street Lights within the identified streetlights, these lights to be integrated with intended Smart Light System. This smart lighting system ensures an energy efficient LED based Street Light System bundled with motion & ambient light sensors with Smart controllers which delivers the following:

- Minimize energy usage
- Operate the street lights in three states (Dual DIM/Bright/Off) automatically as per the real time field requirement
- Automated controls that make adjustments based on conditions such as occupancy or daylight availability
- Policy driven central controlling mechanism to regulate the street lighting intensity and energy consumption
- Real time tracking and management of street lights
- Automatic illumination adjustment based on human presence by triggering multiple lamps to surround the person with a safe circle of light
- Automatic status updates or failure alerts to remote server
- Learn the existing occupancy pattern and predict occupancy patterns for future planning

d. Smart Traffic:

Traffic management is one of the key functions of city management. Regulating and managing the entire road network and traffic signals in the city ensures smooth traffic flow. Smart traffic system includes advanced ICT enabled Traffic Management and communication. The Smart Traffic system include implementation of a smart signaling system, automatic traffic law enforcement systems, and an information dissemination system to achieve the following functionalities:-

- Minimize the traffic congestions and waiting time
- Centrally controlled traffic management system to ensure smooth movement ofemergency services like ambulance, police etc.
- Managed and coordinated VIP movements

- Availability of traffic data to further analyze and optimize the traffic flow
- Real Time Incident Message and Advisory Messages to citizens
- Improved Traffic Regulation

e. Smart Governance and Citizen Services :

This solution will be centrally developed under Patna ICCC project and will be replicated to other cities to optimize the cost and seamless integration. Smart Governance captures the important attributes of Good Governance i.e. Simple, Measurable, Accountable, Responsive and Transparent governance. ICT in governance has been experienced in the form of e-Governance, which redefines the way Governments work, share information, engage citizens and deliver services to external and internal clients for the benefit of both Government and the clients that they serve.

f. Network Backbone:

The network backbone serves as a medium through which the field sensors communicate with the Integrated Command and Control Centre. The connectivity may be through a leased network provided by a telecom service providers or a city may decide to lay its own network fiber backbone. The network availability is monitored through a Network Operations Centre, which may be housed along with the Integrated Command and Centre.

g. Cameras:

There is Approx. 2500 (Two Thousand Five Hundred) at various locations in Patna City to be deployed.

h. DC & DR:

IT infrastructure in new Data Centre (**DC**) which will be at Patna Smart City Office and the Disaster Recovery **(DR)** which will be on Cloud.

i. ICCC (Integrated Command & Control Centre):

Viewing of video feeds at Patna Smart City Control & Command Centre where the operators can view all the video feeds and for the alerts, they can validate, transfer to the respective authorities for appropriate actions, the video Feeds can also be viewed by Police Area Offices, Railway Offices, SP-Offices for their respective jurisdictions. All viewing centers will also be connected to mobile app for video feed to supervise, manage & conclude the incidents

j. Storage:

Storage for all the video feeds and alerts of Video analytics, FRS (Facial Recognition System) & ANPR cameras

k. Collaborative Monitoring & Integration:

With other existing CCTV Surveillance systems of Patna City on through Edge Gateway device

l. Viewing Centers:

Various mentioned authorities will be given viewing rights of the feeds of the cameras corresponding to their respective coverage areas.

m. GIS Maps:

Layers and Resources. It provides functionality to allow the operator to manage the view of the facility in order to provide better situational awareness during an incident.

n. Integration of Existing Cameras:

Implementation and Integration with all existing CCTV Cameras to establish a medium of quick data gathering from multiple sources and make faster decisions.

o. Integration of various databases:

Integration of various existing databases which shall help in operation and implementing AI algorithm

2. INSTRUCTION TO QUOTATIONERS/MSIs

A. Prequalifying Criteria :

a. The annual turnover of sole bidder in each of the last 03 financial year shall be Rs 200/- Crores.

b. Sole Bidder or Lead Partner of JV shall have minimum 30% average annual turnover of 200 Cr into in the areas of Supply, Implementation and Integration of City Surveillance System and/or, Data Centre infrastructure, ICT, IT & ITeS in last three (03) financial years.

c. The Sole Bidder or JV Lead partner shall have positive net-worth in the last 03 Financial Year.

d. All the JV members should have positive net worth as per the audited consolidated financial statements in each of the last 03 financial years.

e. Bidder's solution shall adhere to the model framework of cyber security guidelines issued by MeitY (Ministry of IT)

f. The Bidder shall have any one of the following ISO Certifications valid at the time of Bidding:

- ISO 9001:2008/ 2015
- ISO 20000:2015 for IT Service Management or equivalent certification
- ISO 27001:2015 for Information Security Management System or equivalent certification.

g. The Sole bidder / any JV members should have CMMI level 3 or better certification

h. The Sole Bidder / Any member in case of JV shall have successfully executed minimum 2 similar nature of Project of minimum of 100 cr.

i. The solution offered must comply with the provisions of Order No P-45021/2/2017- PP (BE-II). Dated 4th June, 2020 issued by Public Procurement Division, Department of Investment and Internal Trade, Ministry of Commerce, GoI read with order number W-43/4/2019-IPHW- MeitY, dated 7th September, 2020 issued by IPWH division of MeitY, GoI

B. Special condition to the Quotaioners/MSIs:

- Keeping in view the scope of work the system integrator, OEM, authorized sellers/resellers and vendors in this field are required to quote the rates inclusive of all taxes which should be competitive so that the same can be utilized for framing the estimate for Integrated Command and Control of Patna Smart City. Even if the quoted rates are adopted, PSCL is not bound to give the work order to any quotationers at this stage because this is being collected only for finalization of estimates.

- The quotations are being invited by the **Managing Director, PSCL, 5th Floor, Biscomaun Bhawan, Patna – 800001** in two parts, CAPEX and OPEX. The quotationers may fill as much items as possible so that these can be used for the intended purpose mentioned above.

C. Pre-Qualification Criteria for OEMs

I. OEMs of Camera, VMS, ICCC, AI based Video Analytics Platform, FRS, ANPR should

have Presence in India for last 3 years as on the bid issuance date.

II. The OEM(s) of Camera, VMS, ICCC should be a profit-making company and should have a positive net worth for last 03 years.

III. OEM of Server, Storage and networking components should have TAC support centre In India and with Toll Free TAC helpdesk Number.

IV. The sole bidder (the Lead bidder and members – in case of JV) must comply with the requirements stipulated in Office Memorandum: F/No/6/18/2019-PPD dated 23rd July, 2020, issued by Public Procurement Division, Department of Expenditure, Ministry of Finance and GoI.

a. Camera OEMs

i. OEM should have a minimum cumulative turnover of Rs. 200 Crores in last 02 financial years from the date of opening of tender.

ii. OEM of IP CCTV cameras should have supplied at least 20,000 IP CCTV cameras in India or globally during the last 05 years

iii. OEM of IP CCTV camera should have successfully completed at least one order for supply and installation of 1,000 IP CCTV cameras during the last 05 years.

iv. OEM should have authorized service centre in India

v. OEM should have ISO certifications: ISO 9001; ISO 14000 & OHSAS 18001;2007/ISO 45001

vi. Cameras; Camera Firmware; SDK; APIs etc. shall not contain any embedded malicious code which may: -
- Inhibit the desired and designed functions of the equipment's and Solution.
- Tap information regarding network
- There are / will no Trojans, Viruses, worms, Spy wares
- OEM shall be liable under Information Technology Act, 2000 and Indian Penal Code 1860 in case any Such malicious code in offered / developed software

vii. Any component/ hardware / parts / assembly / software including firmware used in the offered solution (hardware / software) MUST NOT comply to - GB28181, GB/T 28181-2011; GB/T28181-2011; GBT 28181- 2011; GBT28181-2011 standards. Also, the IP CCTV System MUST NOT have CCC.

viii. OEM should have its own Repair/Service-Support center in the country and

must own its RMA set up in India for a minimum of 05 years from the date of submission of bid (not as joint venture, partnership firms or through any other association). In case of product failure OEM should replace malfunction product with equivalent working product immediately till the repaired or alternate product received.

ix. IP CCTV System OEM for Cameras & VMS must be a member &/or listed in the ONVIF website. The quoted products must be ONVIF compliant not conformant. Online verification of OEM in ONVIF website must be available. No OEM should be banned or suspended by ONVIF within the last five years from the date of publishing the bid.

b. OEM of ICCC

i. OEM of ICCC should have Installation base of at least 05 Safe City Projects / Smart Cities in India or globally during the last 05 years

ii. OEM of ICCC should have supplied at least 3 + Sub System Integration in single order during the last 05 years in India or globally.

iii. ICCC should have cyber-Security certifications from UL or equivalent from any Indian certifying laboratory (Suggestion: ISO 27001)

c. OEM of VMS

i. OEM of VMS should have supplied at least 20,000 cameras Licenses in India or globally in qualifying orders during the last 05 years

ii. OEM certifications

- VMS Should be ONVIF Profile S & G.
- Should also roadmap of ONVIF Profile T/Q. Declaration for the same to be provided.

d. AI Based Video Analytics/FRS/ANPR/Video Summarization Platform

i. OEM must have supplied AI based Video Analytics platform in minimum 02 Safe Cities/Smart Cities/Surveillance project at Defense, Transport Segment, with a minimum 100 Cameras in a single city, single project with AI based Video Analytics use- cases projects in India or globally from last 05 Years.

e. OEM of Server

i. OEM must have supplied servers in minimum 02 Safe Cities/Smart Cities projects in India

ii. OEM of server should be validated with offered ICCC and VMS software with minimum one year of existence

f. OEM of Storage

i. OEM should have successfully completed at least one order for supply and installation of minimum 04 PiB scale out NAS Storage in India.

g. OEM of Switches

i. OEM of Switches should have supplied at least 1000 field switches in India into any Smart City/Safe City projects during the last 05 years

ii. OEM should have authorized service center in India

iii. OEM should have its own Repair/Service-Support center in the country and must have RMA set up in India for a minimum of 05 years from the date of submission of bid (not as joint venture, partnership firms or through any other association). In case of product failure OEM should replace malfunction product with equivalent working product immediately till the repaired or alternate product received.

iv. OEM for Switches must offer IPv6 ready switches having full capabilities to ensure Quality of service, Security for CCTV cameras streams**.**

h. OEM of UPS

i. Offered Product should be OEM own Designed, Developed & Manufactured, OEM should have certificate of incorporation in INDIA for >10 Years

ii. At least one order covering minimum installation base of 1000 outdoor UPS for a project.

iii. OEM Should have ISO 9001 and ISO 14001 certificate for Manufacturing facility from reputed Agency.

iv. OEM Should have annual turnover of > 100 CR for consecutive 03 Years and same should be authorize from Reputed Agency.

v. OEM should have its own Repair/Service-Support center in India from the date of submission of bid (not as joint venture, partnership firms or through any other association). In case of product failure OEM should replace malfunction product with equivalent working product immediately till the repaired or alternate product received.

3. PATNA CITY - AN OVERVIEW

3.1 Regional Profile

Patna is the capital of Bihar and the largest urban area. Patna is located on the southern bank of the river Ganges in Eastern India. The total area of Patna is 136 km2 (53sq.mi), Out of this, the municipal area constitutes 99 km2 (38 sq. mi), while the sub- urban area constitutes 36 km2 (14sq.mi). The cartographic co-ordinates of Patna are 25.6°N 85.1°E. It has an average elevation of 53 m (174 ft.). Maximum Summer Temp & Minimum Winter temp are 43°C and 7.3°C. A characteristic feature of the geography of Patna is at the

confluence of rivers. A narrow strip of somewhat high land about 8 kilometres in width along the southern bank of the river Ganges having very fertile soil and alluvial fertile plains in remaining portions.

The modern city of Patna is situated on the southern bank of river Ganges. The city also straddles the rivers Sone, Gandak and Punpun. The city is approximately 35 kms (22 miles) in length and 16 to 18 kms (9.9 to 11.2 miles) wide. In June 2009, the World Bank ranked Patna second in India (after Delhi) for ease of starting a business. As of 2015, Patna's per capita gross domestic product is 1, 06,000 ($1581). Using figures for assumed average annual growth, Patna is the 21st fastest growing city in the world and 5th fastest growing city in India. According to a study by the City Mayor's Foundation. Patna registered an average annual growth of 3.72% during 2006–2010. Patna also has lowest slum population of any city in India.

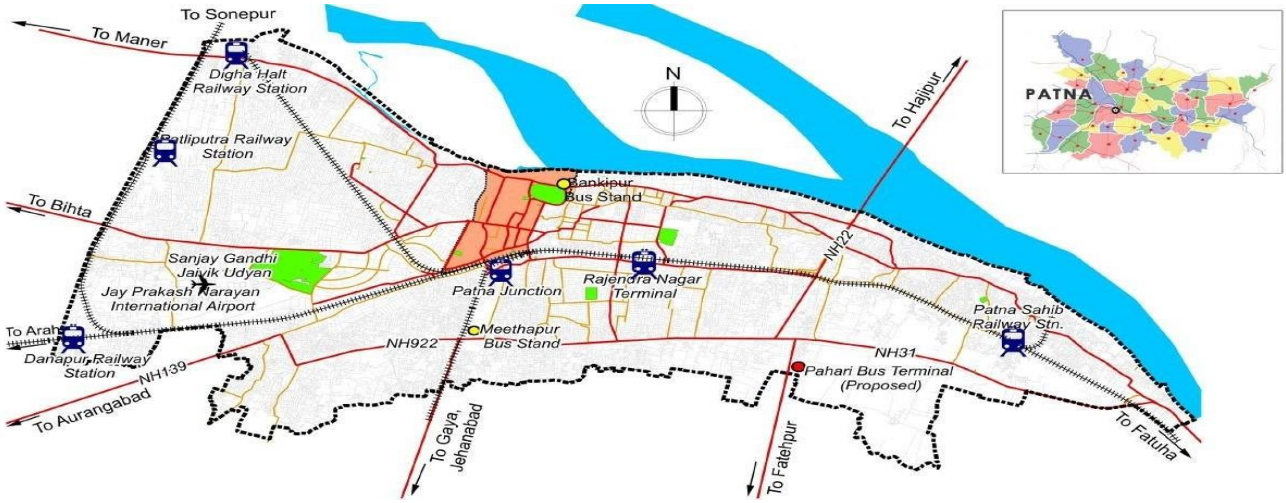


Figure 1. Patna Location Map

3.2 Linkage & Connectivity

Patna is located about 100 km south of national East – West Highway corridor.The NH 30, NH 31 and NH 2 passes through the town. The Ashok Rajpath, Patna Danapur Road, Bailey Road, Harding Road and Kankarbagh old bypass Road arethe major corridors.

Patna was one of the first places in India to use horse-drawn trams for public transport. Public transportation today is provided for by buses, auto rickshaws and local trains. Auto rickshaws are said to be the lifeline of the city. BSRTC has started City bus service on all

major routes of Patna.

ROAD CONNECTIVITY: The district of Patna is well served by a network of roads. National Highway No. 31 passes through Danapur, Patna and Patna City. While one branch goes to Barauni via Barh, another proceeds to Nawada via Bihar. Bodhgaya, Rajgir, Ranchi, Siliguri are conveniently located by road to Patna. Intra-city road transportation is also good in Patna.

RAIL CONNECTIVITY: The main line of the East Central Railway passes through the entire length of the district running parallel to the Ganga. There are three railway lines running across the district from north to south viz., the Patna Gaya Branch linethe Fatuahh-Islampur Light Railway and the Bakhtiarpur-Rajgir Branch line.

Patna Junction is the principal railway station which is located in the town and linksall the key cities of India through the network of express and super fast trains. The various cities connected with Patna are Delhi, Mumbai, Kolkata, Guwahati, Varanasi, Amritsar, Bangalore, Lucknow and Chennai.
The Howrah-Delhi railway line traverses through the entire city length in the east- west direction. Major railway stations along main line within Patna City are as follows:

- Patna Junction
- Rajendra Nagar Terminus
- Patna City
- Danapur

Minor railway stations along main line within Patna City are as follows:

- Gulzarbag
- Deedargang Halt
- Sachiwalya Half
- Phulwarisharif

There are 4 stations along Patna-Digha within Patna City area

- Digha
- Rajeev Nagar

- Secretariat
- R. Block

AIR CONNECTIVITY: Patna has excellent air connection to many important Indian cities like, Delhi, Mumbai, Kolkata. Several Airlines serve this airport with regular flights. Patna Airport is known as Jaiprakash Narayan International Airport.

RIVER CONNECTIVITY: The Ganges is navigable throughout the year and there is considerable boat traffic for transporting cargo. The smaller rivers, e.g., Punpun and Dardha become navigable only during the rains when they are used for transporting agricultural produce to the grain market at Fatuahh.

3.3 Economy

Patna has long been a major agricultural hub and centre of trade. Its most active exports are grain, sugarcane, sesame, and medium-grained Patna rice. There are several sugar mills in and around Patna. it is an important business and luxury brandcentre of eastern India.

In 2009, the World Bankstated Patna as the second best city in India to start up a business. As of 2015, GDP per capita of Patna is ₹1,06,000 ($1581) and its GDP growth rate is 7.29 per cent.

Patna is the 21st fastest growing city in the world, and the fifth fastest growing city in India, and is expected to grow at an average annual rate of 3.72%

3.4 Land Use Pattern

Patna is growing and emerging as trade and business centre in last ten-fifteen yearsand witnessing rapid in migration from immediate hinterland and different part of the state of Bihar. It resulted in to rapid urbanization in neighbouring areas of PatnaMunicipal Area become outgrowths of Patna City. In the absence of planning interventions since 1981, rapid growth led to haphazard development in the city of Patna. Haphazard development resulted into deterioration of open space and forestarea (only 2.34 sq.m. per capita), uncontrolled and unregulated construction activities and brick Kilns in and along the riverbed of Ganga, formation of slum and unregulated construction within core city.

3.5 Smart City Need in the Patna

Patna Smart City, is a mission project of Patna Municipal Corporation for providing security & safety services to the citizens of Patna, Despite the best efforts of law enforcement agencies, such as helpline Number, PCR Vans, special police unit for women and children, anti-stalking helpline and mobile applications designed for safety of citizens, people in the Patna tend to feel unsafe in many public spaces.

While smart city is a concept, which is evolving, the Ministry of Urban Development has issued advisories, where effective measure to be taken to make city smart & safe. Some of the important features prescribed for increasing security for citizens in rural and urban places, inter-alia, include (in terms of Smart City):

a. Surveillance through CCTV and technology based interventions;

b. Safety in Public Transportation systems

As part of its endeavors to safety in Patna by providing quick information & awareness, quick actions with use of all possible means and resources with utmost efficiency, PMC intends to undertake a Smart City City Project with various analytical and Artificial Intelligence tools on cameras in public places in Patna.

The use of state-of-the-art CCTV monitoring, helps to ensure a cityscape that is safe and secure for Citizen, is a technology model that has been widely demonstrated across the globe. To ensure safety and security in places frequently visited by citizen of Patna, such as market places, highways, bus terminals, metro stations, railway stations, recreational areas, areas around schools/colleges/institutions, etc., the need for such a technology enabled surveillance is more imperative, therefore, PMC has recommended to introduce a 24x7 real-time Smart City Project in Patna for citizen protection.

3.6 Current/existing/running initiative by Patna City

3.6.1 Hosting and managing the e- Governance applications of State and its constituent departments

Presently under the National e-Governance Program (NeGP), State Government had implemented the State Data Centre (SDC) in 2008. SDC was envisioned as the 'Shared, reliable and secure infrastructure services centre for hosting and managing the e-

Governance applications of State and its constituent departments'. It was envisaged to establish a robust infrastructure to enable the Government to deliver the services quickly and effectively to its stakeholders. The State Data Centre is connected to the Bihar State Wide Area Network (BSWAN), to provide the access to the e-Governance applications & Services to Government employees through Intranet and to the citizens through public Internet / CSCs etc.

3.6.2 Existing IT Infrastructure installed at Data Centre-

SNo	Item/Description	QTY
	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
	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
	STORAGE EQUIPMENTS	
18	SAN Storage	2
19	SAN Switch	2
20	VTL	1
21	Autoloader	2
22	EML Series	1

3.6.3 Existing Applications Hosted on State Data Centre

SNo	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.	State Welfare Department	BC/EBC Application	http://bcebcwelfare.bihar.gov.in/
5.		SC&ST Application	http://mahadalitmission.bihar.gov.in/
6.	Department of Industries	Udyog Samwad	http://udyog.bihar.gov.in/
7.		Startup Bihar	http://www.startup.bihar.gov.in/
8.	State Health Society	ASHA Web Portal	http://192.168.21.125:8081/index.html
9.		DHIS-2 Web Portal	http://bihardhis.nhsrc-hmis.org/
10.		HR Job Application	http://164.100.130.11:8081/
11.		HRIS Web Portal	http://healthhrisbihar.org/
12.		SHSB Website, Portal & Application	Not Applicable
13.	Urban Development & Housing Department	e-Municipality e-Gov Solution	https://nagarseva.bihar.gov.in/
14.		Urban development & Housing Department	http://urban.bih.nic.in/
15.	DIT	e-Office	https://eoffice.bihar.gov.in/
16.		e-Office Demo	https://eofficedemo.bihar.gov.in/
17.	Department of Social Welfare	Web Portal	ipmsicds.bihar.gov.in
18.	State Election Commission	Website	http://sec.bihar.gov.in
19.	Bihar State Films Development & Finance Co. Ltd.	BSFDFC	http://film.bihar.gov.in
20.	P&D	Student Credit Card	http://7nishchay-yuvaupmission.bihar.gov.in/
21.	Cabinet Secreteriat	Loksamvad	http://www.loksamvad.bihar.gov.in

22.	BSNL(Inspectoratefor Prison & Correctional Services, GoB)	Prison Calling	URL not assigned
23.	High Court	Patna High Court	http://patnahighcourt.gov.in/
24.	BSEDC	SDC Private Cloud	https://cloud.bihar.gov.in/
25.	L&T	Wi-Fi	Campus-Wifi.bihar.gov.in
26.	Finance Department	CFMS	e-nidhi.bihar.gov.in

3.6.4 Applications Hosted on 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

3.6.5 Diagram of Existing State Data Centre

3.6.5.2 Existing Control Rooms

Presently control room is used for monitoring vehicle movement and city situation withoutany apps or smart alert system.

3.6.5.3 Existing ITMS Cameras installed at different locations:

Total Detection Cameras – 208

Total Survellience Cameras – 208

Total PTZ Cameras – 52

3.6.5.4 Existing sttaus of Dial 100 & Survellience by Bihar Police :

Fixed Box Cameras including Critical Locations - 41

PTZ Cameras Including Critical Locations – 39

3.6.5.5 Common Services centres (CSC) scheme is one of the Mission Mode Projects (MMPs) under the Digital India Programme

81 number of CSCs are the access points for delivery of essential public utility services, social welfare schemes, healthcare, financial, education and agriculture services, apart from host of B2C services to citizens in rural and remote areas of the country. It is a pan-India network catering to regional, geographic, linguistic and cultural diversity of the country, thus enabling the Government's mandate of a socially, financially and digitally inclusivesociety.

3.6.5.6 Each CSC Centre has the following minimum Infrastructure :-

- CSC Infrastructure: - 100 – 150 sq. ft space
- Minimum 1 PC with UPS, OS and other application software
- Minimum 1 Printer & Scanner
- Digital / Web Camera
- Power Backup thru Genset / Inverter/ Solar
- Internet Connectivity with at least 128 Kbps speed for browsing & data uploading

4. Project Proposal: Proposed Smart City Solution

4.1 Integrated Command and Control Center for Patna

An Integrated Command and Control Centre (ICCC) is envisaged as an epicentre for all the technology initiatives for the city. Approach for designing the ICCC is to ensuring survivability in the event of distress due to weather, accident, or deliberate attack. All the technology interventions like surveillance camera feeds, solid waste collection data,water SCADA, city utility maps, traffic statistics, parking availability, etc. would integrateat ICCC.

The Command and Control Centre is equipped with large Video wall and operator workstations where city level operators and department officials manage and monitor the various city utilities. The Command and Control Centre application platform is the heart of the system. It is the platform on which all systems known as the modules integrate, this ensures seamless transaction of information obtained from the sensors, which are deployed through various subsystems.

The Command Centre Platform provides the city authorities with tools such as Artificial

Intelligence for deep data mining, data correlation, event prediction, decision support, and Standard Operating Procedure based Incident Response. The command centre Platform provides a user friendly Graphical User Interface, and array of reports includingasset tracking and management on GIS maps. The Platform is designed to ensure that the system is scalable, with interoperability, and adhering to open standards for future integration.

Bihar state has envisioned implementing Hub and Spoke model to enable data sharing across various control rooms and command centres across the City or a State. In the huband spoke model, Command Centre at the hub may be treated as the Central CommandCentre, which will be implemented in Patna , which will be having bi-directional integration between Hub (State level at Patna) where primary decision making can happen and is connected to the other City Level command centers as Spoke. Each city level command centre manages the operations of the respective city/utility operation, while data of the city may be shared through the network backbone with the CommandCentre at the Hub.

The hub in Patna will be implemented in scalable way where it will be expanded to integrate other cities and all the ULB's with existing and upcoming IT services in the State.Other State Department services will also integrate on this common platform. This platform includes IoT device integration, Artificial Intelligence where field device cancommunicate to system via internet based on configuration defined by operator.

This innovation includes following functions to provide City Services and Governance:

- Departmental collaboration
- Coordination
- M2M communication with IoT
- Co-relation of events
- Analytics for prevention and proactive operations

The Integrated Command and Control Centre (ICCC) will be an enterprise class IP-enabled application, will support the seamless unification of various Public Safety elements including Video Management System (VMS), Integrated Video Analytics System, Automatic Number Plate Recognition system (ANPR), Facial Recognition System (FRS), Picture Intelligence Unit, Incident management, Emergency Response System, Criminal tracking, Community Surveillance, Record management and integration with other Govt. databases under a single

platform. The ICCC 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 edge devices.

The ICCC 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.

The ICCC Platform will maximize real-time monitoring and control efficiency from one workstation through the synchronized control of high-resolution blueprints, images, streaming camera data and system alerts which allows for interaction between all relevant data. There will be 20 Workstations for operators who render the services of ICCC Platform to showcase the video feeds (live streaming) along with the triggers and alerts generated by Analytical servers on the Video wall.

The ICCC will be open architecture based, highly scalable and able to integrate multiple disparate systems seamlessly on a common platform. The ICCC will provide a real time Common Operating Picture (COP) of the area involving all agencies using a simple Operator / User friendly interface.

The ICCC platform will support various sensors like Cameras, GPS, Voice devices, Storage devices, Sensor inputs from other Utility applications/ systems. The ICCC platform will provide a dashboard functionality to manage workflows by integrating information from different agencies and systems to facilitate responsive decision making in City.

The ICCC platform will provide a cross-agency collaboration tool to support instant communication between various user groups and authorities. It will facilitate an Intelligent Fusion Center to conduct all Big Data Co-relation among various integrated datasets for interoperability.

The ICCC platform will be an IP enabled solution. All communication between the servers and other clients will be based on standard TCP/IP protocol and will use TLS encryption with digital certificates to secure the communication channel. The ICCC platform will protect against potential database server failure and continue to run through standard off-the-shelf solutions. The ICCC platform will support native and off-the-shelf failover options without any dependency on external application for both Hardware and Application level fail over.

Proposed components/requirements of Integrated Command and Control Centre for Smart City, Patna:

a) Integrated Command and Control Center (ICCC) Platform

b) Integrated Dashboard – Provision for generating configurable reports through dashboard and also real time monitoring and Alert Systems.

c) Video Wall & Controller System & Workstation for Operators

d) Operator Workstation and Accessories ex. Telephone, fax, inter-com etc.

e) Alerting system service through SMS gateway, IP Phones etc.

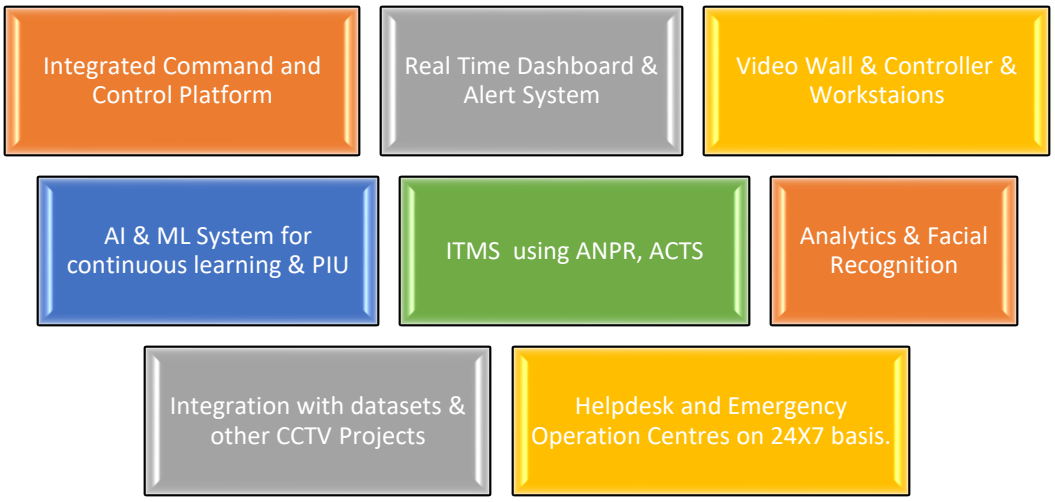
f) Integration with datasets of existing application of different projects of Patna Smart City

g) Helpdesk Service and Emergency Operation Centres on 24X7 basis.

h) Integrated Traffic Management System with ANPR, Red Light Violation, Speed Vehicle Detection

i) ACTS & Traffic Signal Management

j) Necessary Civil, Electrical work including furniture, acoustics design including Air-conditioning for Data Centre, fire safety, and Command & Control Centre.



3.2 Video Management System

The proposed Video Management System (VMS) shall provide a complete end-to-end solution for security & surveillance application. The VMS shall be an enterprise class IP based application with Server-client architecture. The VMS shall support cameras using the industry standards ONVIF Profile S, and Profile G. The VMS shall have Management Servers, Recording Servers and Client Interface as integral part of the solution.

The VMS will be accompanied with the stack of recording servers is capable to record the live streaming flow of HD videos with appropriate codec and certifications in place. The recording servers under the supervision of VMS will render SDK services through media gateway upon the unicast stream of video per camera entered in DC in order to provide dedicated encrypted stream to the analytical servers, FRS servers and ANPR servers.

The Analytical platform will revert back the derived outcomes to the VMS which will be forwarded to the VMS clients located in the user workstations at ICCC, Police Station and Police Area Offices, Railway Offices, SP-Offices Offices as per the defined jurisdictions. Also, the MCCV will be equipped with one of the VMS client of the central VMS platform to receive triggers for necessary and immediate field actions.

The VMS and ICCC servers will conduct Out-of-Band Management (OOBM) Operations with the Analytical platform to enable users to be facilitated with triggered based structured outcomes at the video wall.

The Surveillance System shall not have any limit on the number of cameras to be connected for Surveillance, Monitoring and Recording. Any increase in the no. of cameras shall be possible by augmentation of Hardware components.

Police personnel/ operators/Smart City Officers shall have following access to the video feeds of the cameras according to the role-based access assigned to them:

a. Viewing of the live Camera Video Streams (Approx. 30% of 1000 Camera) based on access rights
b. Viewing rights to the stored feeds, stored on Primary / Secondary Storage
c. Viewing of video feeds from collaborative public CCTV surveillance system
d. Viewing of video feeds basis upon the Alerts / Exceptions / Triggers raised by Video Analytics, FRS, ANPR,ATCS system
e. Trail Report on specific person / object / vehicle for a specific period / location
f. Personalized Dashboard (depending upon role-based access level defined to the police personnel/ operators/Smart City officials , detailed requirement finalization will be done during Pre-Implementation stage)
g. Provide search of recorded video. Advanced search should be possible based on various filters like alarm / event, area, camera, etc.
h. Export rights of video / other critical incident data based on appropriate rights and privileges
i. Ability to back up data stored in DC to DR on demand/ schedule based

3.2.1 VMS Functional Specification

a. The Police Stations, Railway Offices, SP-Office, Smart City Office will be provided with Video Management System with necessary computing and controllers to manage all the raw data feeds coming from the cameras of the respective territories under jurisdiction through multi-cast enabled MPLS network.
b. The Video Management System at Smart City ICCC will be equipped with Control & Command computing with all media servers regulated with central management server aligned with Database servers and adequate storage requirement. The envisaged multi-cast cameras will be equipped with in-built Network Video Storage (edge level storage) which will serve for continual storage pattern in case of failure or downtime with respect to any server as a part of this essential architecture.
c. There will be a provision of the single master server at ICCC that will handle approx. 2500 new cameras, recording servers and unlimited users to access data. The ICCC server will capable to

handle many more camera feeds as per scalable requirements however the integration of such scenario in our system will require additional compute and storage. The Master Server will have manual and automatic mode for assigning cameras to the available recorder servers as per Police Area Offices, Railway Offices, SP-Offices or PATNA SMART CITY OFFICE requirements. In automatic mode, the cameras will be assigned based on the compute capability of the recorder server. In manual mode, the system will allow the operator to assign the cameras. In both cases it will be possible to utilize all the recorder servers including the redundant one.

d. The Video Analytic and Artificial Intelligence tools will be capable to conduct real time analyses of the video feed and post data analyses of the triggered or tagged data from the big data pool. The Post Data Analyses will be provisioned with video summarization tool and methodologies by reducing timeframe of actual video substantially. This video synoptic and summarization methodology will support Police Personal in investigation studies with minimal time consumption based on customized search facility. In order to keep the real time streaming and recording uninterrupted with possible downtime during Post Data Analyses when multiple users access same feed, a streaming server will be provisioned to route the accessibility without hampering the real time input efficiency.

e. VMS will be camera agnostic. The IP details of each camera linked with the VMS so that the segregation of the real time streaming from respective cameras will be maintained and facilitate to store the continuous data feeds in the logical units of pre-defined virtualizations in the servers. Subsequently, the storage will also be linked with the same pattern indexing which will be helpful while retrieval during post analyses.

f. The viewing of the feeds will cater up to 30% of 2500 cameras at a given point of time. This will enable the optimum and efficient use of provisioned bandwidth to minimize the recurring bandwidth expenditure. The VMS will periodically check the gaps in live recording of the cameras based on broken time periods of continuous feeds and will check with the on-board storage of the camera. In case of a gap, the VMS will synchronize the video recording on the on-board storage with the VMS storage through ONVIF Profile G standards.

g. The VMS will support multi-site deployments with centralized monitoring of the videos, video analytics and system health alerts.

   i. will support matrix view at full frame rate

   ii. Support digital zoom of the cameras from central site.

   iii. Control PTZ cameras from central monitoring client application

iv. Ability to pick and choose the selected cameras from remote sites.

v. Ability to search and retrieve the archived video from the remote site with intelligent motion-based search

vi. Download multiple video segments from multiple sites efficiently

vii. Multi-layer maps support

viii. System health dashboard for all connected systems. The VMS will ensure performance checks of all cameras to alert upon the deficiency in flow of camera feeds, if any.

ix. User and rights management with audit trail and logs

x. The VMS will ensure calibration of the camera feed to show case on the video wall or monitor displays.

3.2.2 Video Management Server Plan for Cameras

The Video Management Server will provide centralized management of all IP cameras in the city. The database will support more than 5000 cameras / IP end points in a single server. The Management Server will provide with 1:1 redundancy. The Fail over and Fall-back Management Server will be on hot standby, ready to take over during the primary Management Server fails. No manual action from the user will be required. The fail over time will not be beyond 1 Min and there should not be any loss in the Live and Recorded Videos of the connected cameras.

The Video Management Servers shall be capable to be running in virtualisation / Physical server environment in the DC. The Standby VMS server will support data recovery scenarios where a server can be in another building and only take over if Primary server become offline. Both Primary and Secondary must be based on a single instance Active – Active architecture. The Standby Server will support real-time synchronization of the configuration databases for high reliability.

3.2.3 Video Recording Server Plan for Cameras

In the centralized scheme of solution, the Video Recording Servers will be running centrally in virtualisation environment in DC. Each Video Recording Server Host will be able to handle at least 960 Mbps of Video bandwidth in virtualized environment. The recording Servers will have N:1 redundancy. The Fail over and Fall-back Recording Server will be on hot standby, ready to take over during the primary Recording Server fails. No manual action from the user will be

required. There should not be any loss in the Live and Recorded Videos of the connected cameras due to failover. We have included 30% additional servers to handle the interim storage / database /failover requirements.

3.2.3 Storage Plan for Camera Video Streams

In the centralized scheme of solution, there will be centralized storage for all cameras at DC. The centralised storage has been planned at DC to store all camera feeds for 30 days 24/7 at 4MP resolution or at the highest resolution available from the camera at 25 FPS with H.265 video compression.

The recordings of all cameras will happen at DC. In Case DC goes down, data of 30% critical camera location will travel to DR, which has provision of scalability. 30% of Analytics and ANPR feeds and 100% storage of Tagged Data will be stored in active-active mode at Data Recovery Centre. DC & DR will have storage capacity of 30 days and 7 days respectively.
The video feeds related to incidents and important in nature and which may be required for evidence purposes will be flagged by the operator. The flagged video feeds will be archived in the storage for at least 90 days or as defined SOP by the police officials. A pool of mixed drive to form a tier to keep video data for 24/48 hours during playback is recommended.

3.2.4 CCTV Monitoring plan at Control &Command Centre

The VMS shall support Multicast of video streams from the Cameras. The application shall redirect video streams to active viewing clients on the network using multicast UDP directly from cameras and the architecture shall not use multicast streaming via recording servers or any other servers. This will achieve bandwidth usage optimization in the city-wide network and increase the overall compute capacity of recording servers.

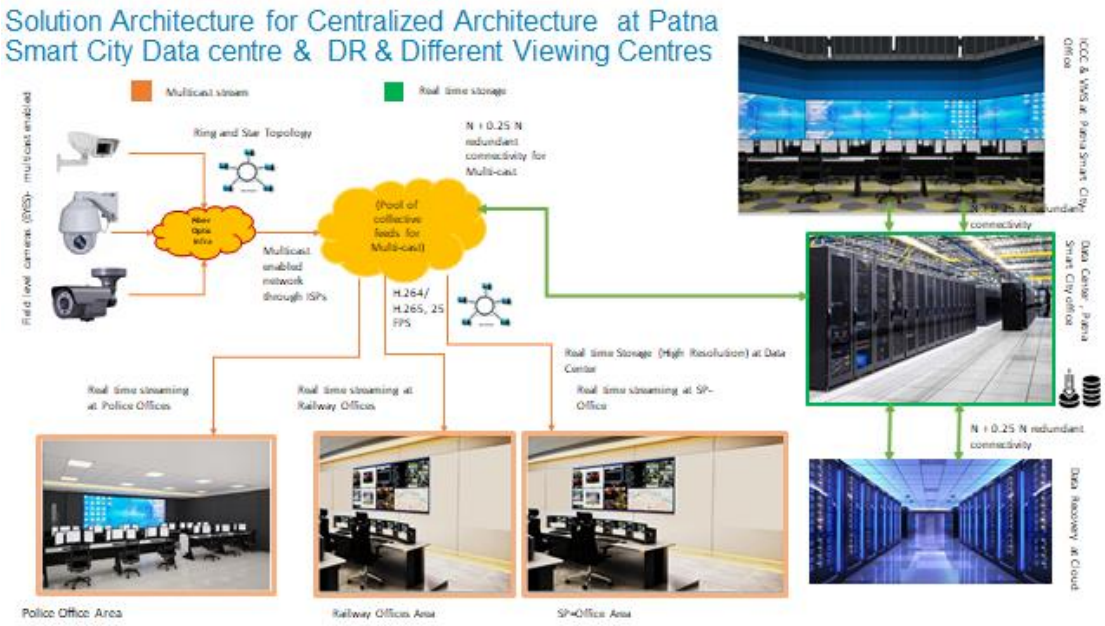
The VMS client workstations must support GPU based decoding for open standard video compression like H.265 etc. The failover for VMS client workstations between the management servers hosted at DC must be seamless during any of the Management server of ICCC or VMS goes down.

At ICCC, 30% cameras that is approx. 750 cameras to be monitored live.

At Police Area, 30% of the cameras of that Police Area Offices, Railway Offices, SP-Offices, to be monitored live sequentially. 30% will have matrix of 55” monitor displays along with operator workstations with 3 nos. of monitors.

At Railway Area, the operators will be able to monitor up to 30% cameras on operator workstation(s) per police station, LED screens are provisioned for the view as well.

Project data flow of Patna Smart City – An Overview of design



3.2.5 Edge Community Surveillance / SWAT teams Gateway

a. 10 edge gateway devices will be procured as an integral part of the Project Solution. It will be used for connecting the feeds of existing cameras reporting to other control room. The Edge Gateway appliances will connect the external set of cameras that will be used as per the requirement.

b. The primary purpose of the gateway is to provide critical situational awareness solution by accessing live video camera feeds during any crisis operations or in the community surveillance solution requirements.

c. The gateway with embedded software will have the ability to connect with 3rd party VMS software / NVR systems deployed in the private and public institutions and act as a gateway to get the live cameras feeds in to ICCC VMS application.

d. The gateway will have an ability to stream at least 200 cameras from each of the deployment site live into the Command centres or any other locations where the ICCC / VMS application is made available.

e. Live video feed streaming should not have any dependency in any format on the 3rd party VMS or NVR solutions deployed in the private or public institutions where such gateways would be deployed.

f. The communication between Edge gateway and VMS / ICCC application at command centers or any other location will be secured and encrypted.

g. The gateway will have the native intelligence to stream live video with dependency only on the network infrastructure of the 3rd party system and under no circumstances the solution should depend / intervene on the 3rd party solution deployed except accessing the live video feeds from the CCTV cameras deployed at sites.

h. The device / software will be Cyber securely hardened.

3.3 Video Analytics – Functional Requirement

The Video Analytics shall offer a suite of analytics rules with Artificial Intelligence to provide automatic detection of a range of motion and non-motion behavior of persons, objects and vehicles.

There shall be a provision of Analytics and Artificial Intelligence through Machine and Deep learning solutions on video feeds received from at least 2500 cameras out of total envisaged number of cameras. There should be provision of 2 use cases (minimum) per camera.

3.3.1 AI based brief Video Analytics process flow

a. Each of the video analytics use case shall be able to run on a unified video intelligence platform. Where the platform shall have the capability to support several multi-vendor/OEM video analytics applications that can be deployed on any camera or video-feed seamlessly.

b. Each of the video analytics use-case shall be structured as an independent module that can be deployed on any camera using a simple user interface utility, providing a complete

visibility of the use cases and which cameras they are running on. The platform should have utility of scheduling each use case on individual camera.

c. The user should be able to easily select the camera by tag, groups or locations and schedule applications on any camera.

d. System will ingest Petabytes of Data in Storage Repository (Ingest) –

I. Intelligence inputs from field officers
II. Internet Data
III. Interrogation Reports
IV. Criminal Records
V. Videos and Images from CCTV cameras, etc.

e. Custom Predictive Models trained on client's training set (AI and ML Models) –

I. Similar criminal profiles
II. Similar events clusters
III. Alerts for specific crimes
IV. Identify themes and trends
V. Track hotspots and dangerous areas
VI. Force deployment
VII. Sensitive Locations

f. Visual and Analytical platform to carry out analytics (Analysis) –

I. Track the complete profile of an individual
II. Track compromised assets
III. Track events and main suspects
IV. Track organizations and their actions
V. Identify linkages between events and individuals
VI. Identify chronology of an event
VII. Charts and Reports to identify upcoming trends

g. Performance Indicators for the Video Analytics:

I. Detection Rate (> 99%)

II. True Positive Rate + True Negative Rate (>95%)

III. False Positive Rate (<5%)

IV. False Negative Rate (<5%)

3.3.2 Video Analytics (Use-Cases)

Video Analytics will be performed on metadata fields on a data lake of the envisaged system. The data will also be gathered from different datasets to be integrated. Big Data solution with its built Artificial Intelligence (AI) and Machine Learning (ML) algorithms will be capable of assisting Police Officials to work in tandem and collaborative manner in all three following scenarios:

- Retrospective (Post Incident),
- Preventive
- Predictive measures.

The various Analytic solutions as envisaged as an effective outcome of the system includes:

a. People detection

The most important priority of city surveillance systems is on the people themselves focusing upon the prime objective of this project i.e. safety of Women and Children. The objective is to keep people safe and prevent accidents or criminal activities. Not all activities are easy to detect. For example, it is very difficult to detect if two people are fighting as this can take many different forms. However, many associated behaviors can be detected. For instance, if a person enters in any restricted area or any unattended baggage or kept beyond some threshold time etc. If crowds gather suddenly, this could be a symptom of some unusual activity as well. Having a system that can monitor various types of human behavior can help the city's officials ensure the safety of their citizens. The following can be the people driven use-cases:

b. Crowd Detection & Headcount

The analytic should have the capability of detection of a crowd within the Field of View of the camera. It should be possible for the operator to define the number of persons including gender identification within the crowd scenario. The analytic should generate the crowd formation alert with estimate of the number of persons in the crowd based on the headcount. Based on the trend evaluations for the defined area on the criminal and suspicious activities, predictive analyses should be performed for effective forecasting towards possible threat bearing activities towards people.

c. Person Falling Detection

The analytic should detect the person falling all of a sudden in the field of view of the mera and does not get up within the pre-configured duration of time. The analytic should be able to detect one or more persons falling simultaneously.

d. Protection and security towards women in isolation

The analytics will ensure suspicious behavior activity for women in isolation/ deserted area or possibly when traced surrounded by men in such identified places.
Also, the women raising and waving hand in such aforementioned situations will be tracked and alert will be generated at ICCC Platform for immediate extension of SoS help.

Apart from above used cases; the SI can also add Below is a list of our recommended / Suggested Video Analytics based on Artificial Intelligence, Machine learning based algorithms which is need of a smart and secure City :

- **Alone female /child present in a frame:** - Alert if a single women / child (based upon age and gender identification algorithm) is found in the video frame on real time on schedules hours and at identified locations. If a woman is identified to be gathered by multiple men, system shall alert on immediate / real time basis.
- **People Fighting**: Alert if at least 2 or more people hitting each other
- **A person with Weapon:** Alert if a person holding one of the weapons systems recognizes such as Gun, Rifle, Bat, etc visible for 05 seconds
- **Human Raising Hands for Help:** Alert if a person raising his both hands above the shoulder for at least 10 seconds.
- **Abandons Object:** Alert if a person abandoned a bag in public areas for more than 05 minutes.
- **People Throwing Stones**: Alert if a person or group people aggressively throwing an object/stones

- **Chain / Mobile Snatching**: If a pedestrian's personal property by employing rob-and-run tactics.
- **Fire or Smoke:** Alert on the event of fire/smoke originated in view of the configured cameras
- **Vehicle Collison:** Collision between two or more cars / vehicles in the configured view of the camera
- **Crowd Gathering / Unrest:** Alert if more than the defined group of people start gathering or panicky running.

3.4 FACIAL RECOGNITION SYSTEM

a. The FRS application shall install for the cameras positioned at the entry/ exits of public places/ city, High Security Areas, Places of Worship, etc.

b. There will be 50 cameras across all the cameras identified for FRS application at any point of time. The licenses/ channels acquired for FRS application will be used to randomly select any camera out of 50 cameras (for Video Analytics) to run FRS; The place will be communicated later as per the requirement.

c. The distance between the camera and capture area shall be 10-12 Meter and Adequate lighting at capture zone.

d. The height of the camera from Ground / Floor shall be 8-10 feet.

e. Capture zone to be channelized to capture Frontal Face of the people. Although, one caught, the application should have the capability to make minimum 15 iterations with different illumination levels and varied angles.

f. As a precautionary measure the camera should not be placed/ pointed directly to strong light sources like sunlight, headlight or spotlight.

g. Face Recognition System shall work on real time and offline mode.

h. The system shall have the best suited technology employed for 1:1 (one to one) and 1: N (one to many) matching applications for various purposes.

i. The areas for which the camera feed will be used as input for FRS module will be identified considering:

- Highly prone area for criminal activities against women, child, elderly people as per criminal records;
- Public places with substantial walking head-counts
- High Security zones and a few Government Offices under critical surveillance
- Accuracy in bad lightening and weather conditions may be evaluated using following KPIs:

- Detection Rate (> 70-80%)
- True Positive Rate + True Negative Rate (>75%)
- False Positive Rate (<25%)
- False Negative Rate (<25%)

j. FRS should be able to

- integrate with CCTNS & other databases,
- generate Alerts based on predefined parameters
- integrate with watch list
- search on-line and off-line in video and images
- Generate Reports and Manage data

3.5 Video summarization and Analysis

Artificial Intelligence based video analytics are crucial to increase efficiency of proposed Integrated Command and Control Center being built as part of Patna Smart city Project. These live video feeds and responses to incidents reported needs to be analyzed for better policing. Artificial Intelligence (AI) based analytics that can handle “Active Surveillance”. This specific section covers the technical use case aspects of “AI-based Video Review & Investigation System”

The proposed solution should help in making Video Searchable, Quantifiable and Actionable, reviewing long duration of video in short time; quantitatively analyze video to derive actionable insights for data driven safety, security and operational decision making. The proposed system should be state of the art image processing technology essentially creating condensed summaries of original, full length video recordings, while preserving all objects and events of interest. These should be presented either simultaneously or in rapid succession, regardless of the time point and sequence in which they occurred, effectively providing operators with a clear view of activities and enabling them to rapidly review and home in on events of interest.

While keeping human operators "in the loop" the system should provide operators, what they need to quickly scan through video data to find suspicious, out of the ordinary or potentially criminal aspects. The technology should enables them to set the speed and

density of event playback, focus on specific areas of interest, and toggle event markers and time stamps for detailed event tracking, while leaving it up to operator intelligence, experience and human instincts to make sense of this video data pertaining to safety and security. After detecting an object of interest, the user shall be able to select to see the object in its original form in the original video which can then be exported.

Video Summarization tool based on attributes and meta data field will facilitate to reach to relevant and meaningful content for the defined search meeting the requirements for effective post investigation analyses within shorter time span.

3.6 Automatic Number Plate Recognition (ANPR) S/W - Vehicle Surveillance

a. The System shall automatically detect a vehicle in the camera view using video detection and activate license plate recognition.

b. The System shall automatically detect the license plate in the captured video feed in real-time.

c. The system shall perform OCR (optical character recognition) on characters of the license plate (English alpha-numeric characters in standard fonts).

d. The ANPR system should work on 90% accuracy parameters for capturing and 90% accuracy of OCR on the standard fonts.

e. The System shall store JPEG image of vehicle and license plate and enter the license plate number into PostgreSQL database along with date time stamp and site location details.

f. System shall be able to detect and recognize the English alpha numeric License plate in standard fonts and formats of all vehicles including cars, HCV, and LCV.

g. The system shall be able to process and read number plates of vehicles with speed upto 120 km/hr. or above.

h. The system shall be robust to variation in License Plates in terms of font, size, contrast and color and shall work with good accuracy.

i. The system shall support Black list / White list configuration: The system shall have option to input certain license plates according to the hot listed categories like “Wanted”, “Suspicious”, “Stolen”, etc. by authorized personnel

j. The system shall 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.

k. A single compressed stream shall also be sent to server for recording and general video analytics purpose

3.6.1 Automatic Number Plate Recognition & ITMS (Use Cases) :

A Smart ITMS model caters to a dual sided beneficial edge for a Smart City

- Reduced Traffic Violations and accidents in the City &
- Revenue Generation Model by e-Challan and Traffic awareness & advertisement programs

The e-Challan can be generated upon detection and validation of several Traffic Violations such as :

- Red Light Violation Detection System
- Over Speed Violation Detection System
- Dangerous / ZigZag or Rash Driving Detection System
- Wrong / Illegal Parking Detection System
- Triple riding and No-Helmet Detection for two wheelers
- Free Left Obstruction Detection
- Wrong –Way Driving Detection
-

- Through the inputs received from ANPR cameras, the system should capture the number plate of two-wheeler and four-wheeler vehicles. The analytic should be able to:
- Read and convert the license plate number into a text string of the vehicle with 95% detection accuracy.
- Store the JPEG image of the license plate in the database with other metadata such as time stamp, location, camera, etc.
- Classify the vehicles in categories such as four-wheeler light and heavy motor vehicles, three wheelers, auto rickshaws and two wheelers
- Detect colour of the vehicle (in day time)
- Set separate recording duration for event information (number plate as text), media clips (pre and post event recording) and ANPR- VEHICLE SURVEIILANCE picture snapshot.
- Software should also raise an alert in case of any vehicle not having any number plate.

3.6.1.1 Suspect Vehicle Detection

It should be possible to store the number plates of the vehicles under various lists such as stolen, suspicious, blacklisted, etc. The analytic should detect such vehicles in the field of

view of the cameras in real time by matching the number plate.

3.6.1.2 Vehicle Search

The analytic should provide the feature to search the vehicles based on the attributes that includes number plate (partial or full), class of the vehicle (four-wheeler light and heavy motor vehicles, three wheelers, auto rickshaws and two wheelers, etc.), color of the vehicle and location.

3.7 Public Address System (PA system)

The network PA works very much similarly to computer networks where packets of data are transmitted from one node to another with each of them having a unique IP address in the network system. The nodes will then only pick up the packets that solely addressed to them. The network PA can also be integrated with other building services or subsystems that are TCP/IP compliant like PA system at any office can be instructed from ICCC and other building management system to provide instantaneous voice assisted response and feedback from each system. The PA system should have at least features like:

i. All the elements of the system are IP compatible.

ii. Officewise announcements based on the selection of channel and all call emergency announcements can be made through the PA system.

iii. This IP based P A system can be accessed from anywhere and everywhere and forward required messages. It should have the capability to control individual PAS i.e. to make an announcement at select location (1:1) or multiple locations (1: many). The PAS should also support both, Live and Recorded inputs

PA system shall be connected at all offices with ICCC level.

3.8 Intelligent Traffic Management System & Public Transport

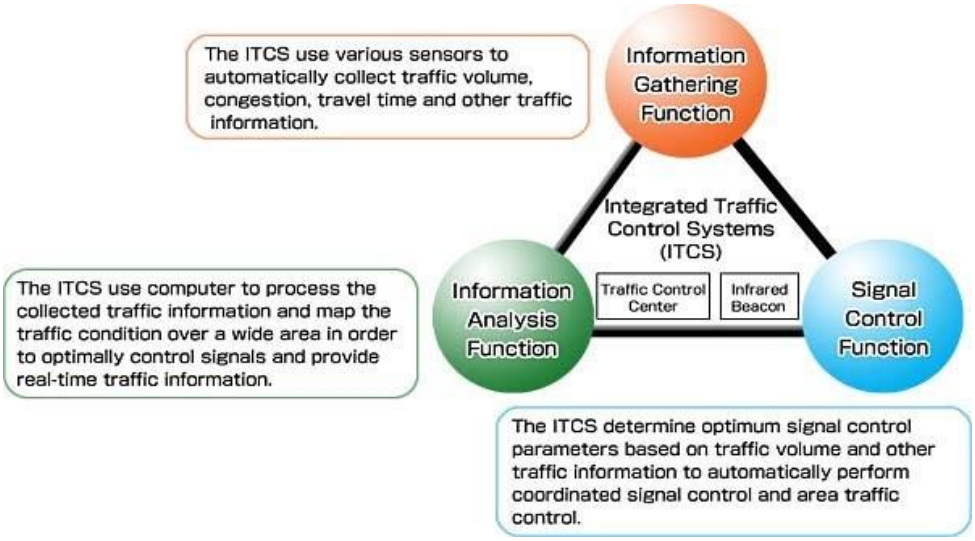
The intelligent Transport System will be established under which Automatic Signal Control System, Separate Signal System for pedestrians, Traffic Management Centreat state level, area Traffic Control System, Corridor Management, Dynamic Traffic Indicators will be established. Arrangement of Traffic Signals, Surveillance Camera, and Enforcement Camera etc will be made in the project.

Under this project with the smooth operation of traffic system its monitoring will also be done and arrangement will be made to send e-challan to those marked as violatingthe traffic rules.

Special arrangement has also been made in the project for emergency vehicles to pass without interruption. Besides, special emphasis has also been made on road safety measures
The integrated Traffic Management/Control Systems are the key components of theUniversal Traffic Management Systems (UTMS) and provide advanced traffic management By using cutting-edge technologies such as infrared beacons and computers, the ITMS achieve optimum signal control to effectively deal with ever- changing traffic flow patterns, provide real-time traffic information , and implementeach subsystem of the UTMS.

Main Benefits

- Ensure traffic safety and smooth traffic flow
- Alleviate traffic congestion
- Reduce travel time
- Minimize traffic pollution



Integrated Traffic Control System (ITCS)

5. Proposed BOQ for Smart City Project

Sl No.	Category	Line Item (Component Wise)	Unit of Measurement	Indicative Quantity

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 (Armored)	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
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 control PTZ Cameras	No.	30
13	ICC	HD LED Display (55 Inches)	No.	16

14	ICC	Workstation Desktop with three LED Monitors	No.	50
15	ICC	FRS-Master ServerDatabase (can store upto 10,00,000 Live Templates) (50 Licenses)	No.	1
16	ICC	Online UPS (sizing as per proposed solution 100KVA 2 Hrs 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
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 ICCC	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 ICCC/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 (NGFW)	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
41	Data Centre Hardware	24 Port Aggregation Switch	No.	8
42	Data Centre Hardware	42U Server Rack with necessary accessories	No.	16
43	Data Centre Hardware	Blade Chassis with Fabric Interconnect Switches	No.	10
44	Data Centre Hardware	Video Management 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
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 (siting 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	Lump sum	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
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 (Channels for Person Tracking as per clause 38 in VMS)	No.	1000
75	Software Solutions	Virtualization Software License	No.	104
76	Software Solutions	Anti-virus & Anti-Spam Enterprise software for 130 endpoints	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	No.	1
82	Software Solutions	Video Analytics Software	No.	1
83	Software Solutions	ITMS ATCS Software	No.	1
84	Software Solutions	ITMS ANPR 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 (Only for adding layers)	Lump sum	1
92	Software Solutions	e-challan software	No.	1
93	Software Solutions	Analytic Devices Type 1 with 2 GPU Cards/ 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 System with one Temperature Sensor	No.	10
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 and1 Flagged video Feed {Not for regular	TB	1

		feed) with all Security features as per MEITY guidelines.		
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 - Red, Yellow, Green Arrow	No.	240
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 Gavanised Iron Class B Traffic Signal straight pole of 6 mtr height with all accessories	No.	120
108	ITMS-ATCS	Supply Installation of Gavanised 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
113	ITMS-RLVD	Local processing unt/ Rack Servers with 3 GPUs in Data Centre (ANPR Servers)	No.	40
114	ITMS-RLVD	Mounting structure wth 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,	No.	10

		with cabling & mounting infrastructure as required		
117	Surveillance System	Outdoor Fixed Box 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 required accessories	No.	15
122	Emergency Call Box	ECB system with Mounting structure, UPS, pole etc	No.	50
123	Environmental Sensors	All type of Environmental Sensors	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	Cantllever /Gantry Poles for cameras upgradable to ANPR	No.	73

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 Workstation Desktop with three LED Monitors	No.	14
142	CCTV-Railway	IP Phone	No.	6
143	CCTV-Railway	HD LED Display (55 inches)	No.	14
144	CCTV-Railway	Managed Port L3 Edge Switches/8 Port L2 Switch	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
148	CCTV-Railway	Furniture (Table +Chair)	Pair	6
149	CCTV-SP Office	HD LED Display (55 inches)	No.	4
150	CCTV-SP Office	Workstation Desktop with three LED Monitors	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+Chalr)	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	No.	1
161	Data Centre Hardware	Backup Appliance with Backup Software	No.	1
162	DC-Software	Mail & Messaging	No.	1
163	Data Centre Hardware	Backup Appliance with Backup Software	No.	1
164	Services	Project Implementation and Commissioning Cost	SOW Enclosed	1
165	Services	Program Management During Go-Llve and O&M period & Manpower as per SLA	SOW Enclosed	1
166	Training Cost	Training Cost	SOW Enclosed	1
167	Services	Integration With Existing System(Cloud Application , Various databases)	SOW Enclosed	1
168	Services	Integration with Existing cameras (Through edge gateway)	SOW Enclosed	1
169	Services	One time Power meter installation charges (As per Junction Boxes)	SOW Enclosed	1
170	Services	Operational Charges for Power (3+2 Years)(At actuals, Will be paid directly by Smart City Office)	SOW Enclosed	1
171	Services	Billboards for poles		500
172	Services	TPA	SOW Enclosed	1
173	Services	Penta scanning & VAPT	SOW Enclosed	1

174	Services	Manpower /Operators for workstations	SOW Enclosed	1
175	Hardware	A.I Traning Servers of 2 Peta Flops	No.	2
176	Services	Endpoint Health Check for Existing Items	SOW Enclosed	1
177	Additional Software	Video Summarization	50 Camera License	1
178	Additional Software	Picture Intelligence Unit	1	1

6. Format for Commercial Offer

Offer shall be as per the format given below considering the above BOQ

Sl No.	Category	Line Item (Component Wise)	Unit of Measurement	Indicative Quantity	Warranty	Price	GST/IGST	Total

Quotationers/MSI shall prepare the quote with all applicable taxes, duties, other levies and charges etc.

Quotationers/MSI shall quote for the entire scope of contract on an "overall responsibility" basis such that the total Bid Price covers Organization's all obligations mentioned in or to be reasonably inferred from the bidding documents in respect of providing the product/services.

Prices quoted by the Quotationer/MSI shall remain firm during the entire contract period or 1 year and not subject to variation on any account.

7. Functional Requirement and Technical key Specifications

7.1 Network Backbone and bandwidth estimation

a. The network will work on a MPLS cloud. The project will adopt building own city approach to ensure high and adequate bandwidth with low operational cost. The network as envisaged will be provided by the ISP to ensure full availability of all field equipment with

99.5% minimum uptime. The MSI/SI will be responsible to establish the Last Mile Connectivity (LMC) for the Points of Presence (PoP) - location of all cameras.

b. It must ensure flexibility to create services on demand basis, more resilient and faster convergence, and multicast capabilities to ensure same feed is given at multiple receivers, future proof, no dependency on ISP open solution, better Quality of Experience, end to end Ownership by Single team as required by Smart city Project, attractive for Telecommunication market players.

c. All the cameras under the project will be linked to the Data Centre at Patna Smart City Office premises in an appropriate manner by the Network Agency to ensure adherence to SLA terms. The network will be equipped with necessary topology framework to ensure redundancy at load and bandwidth requirements for full-time availability of every camera at the Central level (Patna Smart City Office)

d. The cameras will be multi-cast enabled which will provide the feeds to the respective Police Station, Railway Offices, SP-Offices through a multi-casting enabled MPLS cloud of the identified ISP. All locations/ offices will be covered securely through redundant mechanism through the network. All the Police Stations will also be connected linearly (bi-directional) to each other to ensure redundant backing up from the adjoining Station in case of downtime condition. Same linear connectivity provision will also be available for Police Area Offices, Railway Offices, SP-Offices Offices also.

e. The consolidated data at DC will behave as a common pool of data from all field level devices from where data will be routed to ICCC (Control & Command Centre), Police Offices, Railway Offices, SP-Offices based upon the respective incident or triggers with respect to the defined jurisdiction.

f. The poles for the cameras at junction, identified areas will be provisioned with Junction boxes to cater to the Industrial grade, managed Network Access Switch (8/24 port) with PoE+ feature.

g. The Police Stations will provide their respective feeds covering consolidation of all camera feeds under its zone to the Data Centre situated at Patna Smart City Office through an MPLS cloud.

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

i. The established network must ensure minimum Recovery Point Objective (RPO) and Recovery Time Objective (RTO) without experiencing any data loss.

j. The Network for Smart City Project will be established using MPLS cloud by using the services of successful connectivity of OFC provisions can be used as and when available which shall connect all offices & Smart City office. The last mile connectivity to the new camera locations through OFC/Cat6E will be ensured by the selected MSI/SI.

k. The file sharing through the envisaged topological network must be capable of Real Time Streaming (RTS) through Block Level Transfer via HLS protocol to curtail down the delay factors and ensure better uninterrupted streaming from raw input field data.

l. With regards to monitor the feeds of existing (community surveillance) cameras reporting to respective local Police Stations, every Police office, SP-Office and Smart City office will be provided by streaming servers installed at Patna Smart City Data Centre. The streams of all the Analog cameras existing in use in different projects will be transformed to Digital casting streams through existing NAS/ DVR/ NVR using Edge Gateway through the provided streaming servers. The storage of the feeds from existing cameras will be ensured through the existing running media.

MPLS features

a. Quad Small Form-factor Pluggable /OSPF will be the chosen IGP for City MPLS network.

b. All Core and Aggregation Router will be part of Area 0 and Pre-Router will be part of Sub Area. OSPF will be carrying only Infrastructure routes. No other route will be distributed using OSPF.

c. ABR and ASBR- OSPF router will be configured based on Network requirement.

d. Network aggregation should ensure to reduce number of routes in network.

MPLS traffic engineering capabilities:

i. Enhances standard IGPs, such as IS-IS or OSPF, to automatically map packets onto the appropriate traffic flows.

ii. Transports traffic flows across a network using MPLS forwarding.

iii. Determines the routes for traffic flows across a network based on the resources the traffic flow requires and the resources available in the network.

iv. Employs "constraint-based routing," in which the path for a traffic flow is the shortest path that meets the resource requirements (constraints) of the traffic

flow. In MPLS traffic engineering, the traffic flow has bandwidth requirements, media requirements, a priority versus other flows, and so on.

v. Recovers to link or node failures that change the topology of the backbone by adapting to a new set of constraints.

e. MPLS Traffic Engineering will be used for the following application in City Network:

i. Providing bandwidth guarantee for critical real-time applications in the control plane

ii. Optimized utilization of redundant features

iii. Handling of unanticipated load in the network

iv. Fast reroute to provide fast convergence for critical real-time application traffic

v. Will use RSVP for label allocation for TE LSPs.

f. **MPLS Fast Reroute:** Fast Reroute (FRR) mechanism must be deployed to protect MPLS Traffic Engineering (TE) LSPs from link and node failures by locally repairing the LSPs at the point of failure and allowing data to continue to flow on them while the head end routers attempt to establish new end-to-end LSPs. FRR will be deployed to locally repair the protected LSPs by rerouting them over backup tunnels that bypass failed links or node.

g. **Link Protection:** Backup tunnels will be created to bypass only a single link of the LSP's path for providing link protection. This will protect LSPs if a link along their path fails by rerouting the LSP's traffic to the next hop (bypassing the failed link).

h. **Node protection and failure detection:** Fast Reroute (FRR) will be deployed to provide node protection. Backup tunnels that bypass next-hop nodes along Layered Service Provider (LSP) paths (NNHOP) will be deployed as backup tunnels to protect the primary tunnels. The backup tunnel will protect LSPs if a node along their path fails by enabling the node upstream of the failure to reroute the LSPs and their traffic around the failed node to the next-next hop. FRR must supports the use of RSVP Hellos to accelerate the detection of node failures.

Automation of Network

The proposed solution should help City Network to meet the below objective:

a. Agile service deployment and rapid time to market through fully automated service provisioning and service lifetime adjustments

b. Reduce operation complexity by minimizing network protocols and enable centralized intelligence on the controller

c. Autonomic self-protected network infrastructure with autonomic segment routing and topology independent fast-reroute software features

d. Application-engineered Routing through centralized orchestration and path computation

e. Smooth migration towards SDN-enabled network fully backward-compatible with existing network protocols and services

The principle of the proposed architecture is network disaggregation i.e. moving away from integrated HW and SW, vendor specific, individual network devices toward network-as-a-platform with disaggregated open components.

Advantages of the Automation in MPLS transport

a. **Simplicity:** the network nodes only need to run a single protocol, an IGP. It doesn't need any other label distribution protocols like LDP, RSVP-TE or BGP-LU. In addition, with IP unnumbered interface support for segment routing, operators can ease the pain of the IP address management. For a fast-growing dynamic Carrier Ethernet network, this is very helpful. Operators can insert or remove the network nodes without requiring IP address changes on the adjacent links.

b. **Self-protected:** supports topology-independent fast reroute (TI-LFA) for both link and node protection. Compared with traditional RSVP-TE FRR, segment routing TI- FRR has two major advantages. One is simplicity, two lines of the interface configuration will achieve link and node protection instead of creating an RSVP-TE tunnel and manipulating the tunnel protection. The other advantage is the optimization, segment routing TI-LFA will pre- calculate the backup path based on the post-converged topology. So, it's optimized. There is not even a temporarily sub-optimal path during network re-convergence.

c. **Any cast SID for simple service node redundancy:** the redundant network nodes (such as the service nodes) can share the same any cast loopback address and SID. This simple any cast SID configuration allows for automatic service node redundancy, without requiring some complex features such as PW redundancy on the access nodes.

d. **Flexible-Algorithm is deployed** along to support Multiplane network. It supports Delay vs Cost of Transport, Intelligent Secure Path, High-BW Links Preference, Minimum delay path for each type of traffic.

e. **On demand next hop** is also deployed along with Controller to achieve the following:

- Better load-balancing: ECMP across border routers
- Better availability: sub-50msec upon remote aggregation router failure
- Better control plane scalability

f. **Data Plane Monitoring:** SR with data plane monitoring should be supported to avoid black holes in network.

Bandwidth capacity provision

a. Access layer bandwidth for Field level devices will have to be minimum at 3 Mbps per device.

b. Access/ street layer Ring bandwidth for Police Station will have to be provisioned to cater viewing of 30% of camera feeds under the specific police station jurisdiction.

c. Access/ street layer Ring bandwidth for offices will have to be provisioned minimum to cater viewing of 30% of camera feeds / police stations under respective DHQ jurisdiction.

d. Min of 10Gbps of Bandwidth to be provisioned between DC and Near DR location, preferably in a high available / failover architecture.

Planning & Execution

The detailed list of activities for laying of fibre cables for executing the network backbone works include:

1	Site survey for FTTB locations.
2	SLD submission
3	Work Order Generation.
4	ROW application to be submit in various.
5	ROW demand note received from authority.
6	DD/BG preparation.
7	DD/BG submission to authority for permission.
8	Liasioning with authority for ROW permission
9	Liasioning with authority for vehicle entry permission of HDD machine shifting.
10	Pits digging to start HDD machine

11	Manual digging or with HDD machine or trenching depends the track is hard rock/concrete/simple track.
12	Duct laying started post ROW receive
13	Cable laying started post ducting
14	Fiber termination/Cat6E work post cable laying
15	Splicing work of fiber/Cat6E
16	Pits Closer
17	Chamber installation
18	Route marker installation
19	AT offering and clearance by fiber project team
20	Ensure the availability of space and power at each node.
21	ISP material installation & commissioning.
22	Termination and integration of fiber/Cat6E
23	SFP installation
24	Patch cord installation
25	Node integration & RFS certificate for media provisioning.
26	Media provisioning.
27	Testing the circuit in presence of customer.
28	UAT at sites in presence of customer.
29	Signoff after successful completion of testing.
30	Circuit Hand over

Network Audit (Third Part Audit)

a. There will be third party network audit to be conducted on quarterly basis.

b. The Network implementation activities, which include laying of OFC and recurring bandwidth may be opted for distinct and parallel set of activities with respect to the other bundle of activities mentioned in this DPIP.

Networking Standards to be maintained

The following network standards need to be followed while implementing and operationalizing the system.

a. ANMSI/TIA-942, Telecommunications Infrastructure Standard for Data Centres

b. ANMSI/TIA/EIA/568-C.1, Commercial Building Telecommunications Cabling Standard – 2009

c. ANMSI/TIA/EIA 568-C.2, Copper Cabling Components Standard

d. ANMSI/TIA/EIA 568-C.3, Optical Fibre Cabling Components Standard

e. ANMSI/TIA/EIA-569-B, Commercial Building Standard for Telecommunications Pathways and Spaces

f. ANMSI/TIA/EIA-606-A, Administration Standard for the Telecommunications Infrastructure of Commercial Buildings

g. ANMSI/J-STD-607-A, Commercial Building Grounding (Earthing) and Bonding Requirements for Telecommunications

h. Building Industries Consulting Services International (BICMSI) Telecommunications Distribution Methods Manual (TDMM) – Preferred

7.2 INTEGRATED COMMAND CONTROL & COMMUNICATION CENTRE (ICCC)

7.2.1 70 Inches Panel for DLP based Video 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.	Individual Video Wall Resolution	
4.	Cube Depth	Less than 600 mm
5.	Light Source	Laser
6.	Light Output of projection engine	1800 Lumens or more
7.	Brightness Uniformity	95%
8.	Dynamic Contrast ratio	100,000:1
9.	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
10.	Power Supply	Dual Redundant Power Supply Built in inside the cubes
11.	Half Gain viewing angle	Horizontal ± 180°, Vertical ± 180°

7.2.2 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 of 15360 x 8640
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

7.2.3 Video Wall Management Software

Sr. No.	Item	Specifications

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: • 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.

7.2.4 IP Phone

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, 4-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

7.2.5 Keyboard Joystick for PTZ camera at Workstation

Sr. No	Specification	Description
1.	VMS Compatibility	The Joystick must be compatible with all distributed network video management components.
2.	Technology	Six-degrees-of-freedom (6DoF) sensor - Intuitively and precisely navigate digital models or camera positions in 3D space.
3.	Design	The full-size, soft-coated hand rest positions the hand comfortably, and 15 large, soft-touch, function keys allow quick access to frequently used commands.
4.	Quick View Keys	Fingertip access to 12 views makes it easier to switch cameras
5.	Function Keys	Easy access to 4 application commands for an optimized workflow.
6.	Display	Provides a visual reminder of function key assignments on your computer screen
7.	Modifier	Fingertip access to Ctrl, Shift, Alt and Esc keys saves time by reducing the need to move your hand between mouse and Joystick
8.	Numpad	Allows direct numerical input into your application using your standard mouse rather than the Joystick
9.	System flexibility	The Joystick must be part of an integrated system and shall be configured so any number can be added to the system. When combined with user interfaces (UIs), network storage managers (NSM's), encoders, IP cameras, and video consoles, the Joystick forms an integral part of a complete network-based video control system
10.	Input Connector type (power Supply)	Universal Inter changeable
11.	Joystick Interface	USB 2.0

12.	Cable	USB
13.	Joystick Module	Fully proportional PTZ, variable speed; with zoom, iris and focus controls
14.	Operating temperature	0° to 40°C

7.2.6 HD LED Display (55 Inches)

Sr. No.	Parameter	Minimum Specification
1.	Technology	LED Based
2.	Screen Size	55 inches diagonally (± 0.4 inches)
3.	Resolution	4k (3840 x 2160 at 60 Hz)
4.	Viewing Angle	178° / 178°
5.	Brightness	350 cd/m² (typical)
6.	Contrast Ratio	4000:1 (typical)
7.	Aspect Ratio	16:9
8.	Input	2 x HDMI 2.0 1 x Display Port 2 x USB Ports
9.	Remote Asset Management	1 x RJ45 1 x RS232
10.	Duty Cycle	12/7
11.	Certifications	UL/EN/CE/IEC/BIS certification for Safety and CE/FCC Certifications for EMC & Immunity.
12.	Warranty	5 years from go-ive

7.2.7 Workstation Desktop with three LED Monitors

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 able to support min 3x 55" Led Monitor mentioned above
11.	PSU	80PLUS Gold Certified Energy Star Compliant
12.	Expansion Slots	Minimum "1" PCIe x16 Gen3; "2" PCIe 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

7.2.8 Network Colour 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

7.2.9 Biometric access control System

S. No	Item	Description
1.	Finger Print Template	Open Standard Template (ISO based) Template should be compatible with aadhar database.
2.	Credential Support	Fingerprint, Card and Pin
3.	Finger Print template	10 per user
4.	Proximity Card	300 per site
5.	Sensor Type	Suprema/Morpho/Cogent
6.	Card Type Support	Proximity Card
7.	User Capacity	1000
8.	Display Unit	3.5 inch TFT Display with touchscreen
9.	Buzzer	Yes
10.	Event Buffer	500
11.	Connectivity	Ethernet and USB
12.	Power Input	12 V DC
13.	Operating Temperature	-5° to 35°C
14.	Sensor Resolution	500 dpi
15.	Timing	Fingerprint Capture: Less than 5 Sec
16.		Verification of captured finger: Less than 2 Sec
17.	Fingerprint Enrolment Software	Yes
18.	Certifications	STQC certified
19.	Installation	All conduiting / wiring /Trays /channels /trenches /pipes etc.

		for completion of Job
20.	Warranty	5 Years Comprehensive onsite OEM Warranty
	Access Control Software:	
21.	The Access Control Software should have the following Specifications:	
22.	Compatibility with any Windows Operating System	
23.	Compatibility with MYSQL / SQL / ORACLE	
24.	Support for TCP/IP Communication	
25.	Provision for Alarm Monitoring for Battery, Mains Supply, Door Opened too Long, Door Forced Opened, Unauthorized Swipe & Controller Tampering	
26.	Support for unlimited number of Card Database & Transactions	
27.	Specify Card Activation & Expiry Date	
28.	Support for Biometric, Pin & Smart Card Applications	
29.	Management of Dual Access Levels to a single Card	
30.	Remote Locking & Unlocking of Doors	
31.	Remote management of Controllers	
32.	Customization of Door User time for every card holder	
33.	One Client License	
34.	Two Stages of Alarm Management (Acknowledgement on Receipt & Closure on Investigation)	
35.	Access Privileges on the basis of Time & Date	
36.	Creation of holiday schedules to cover maintenance & Vacations / Holidays	
37.	Setting of Time / Date	
38.	Permission to activate any control output for a specific event such as alarm	
39.	Programmable Shunt time to control the door opening time	
40.	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.	
41.	Alarm Management	
42.	Automatic User Log off	
43.	Cardholder Management &Enrolment	
44.	Creation & Maintenance of User Database	
45.	Assignment of Access Privileges	
46.	Shall be capable to enroll biometric fingerprint templates	
47.	STQC certified enrolment biometric device to be provided	
48.	Warranty: 5 Years Comprehensive onsite OEM Warranty form the date of Go-Live with	

	necessary updates, upgrades and patches

7.2.10 Dome/Fixed Box Cameras for Internal Surveillance

S. No	Item	Description
1.	Video Compression	H.265 or better
2.	Type	Dome Type
3.	Video Resolution	1920 X 1080
4.	WDR	Required (>70db)
5.	Automatic Gain Control	Required
6.	Frame rate	25 fps in all resolutions
7.	Image Sensor	1/4" / 1/3" Progressive Scan CMOS
8.	Lens Type	Varifocal, IR Correction
9.	Lens	Fixed IRIS 2.8-10mm, F1.7, 3x optical zoom,10x digital zoom
10.	Minimum Illumination	0.9 lux
11.	Image settings	Compression, colour, brightness, sharpness, contrast, white balance, exposure control, backlight compensation, rotation
12.	Protocol	HTTP, HTTPS, FTP, SMTP, RTSP, RTP, TCP, UDP, RTCP, DHCP
13.	Security	Password Protection, IP Address filtering, User Access Log
14.	Operating conditions	0 to 40°C
15.	Casing	Tamper Resistant casing for Indoor Environment
16.	Standard	ONVIF Compliant
17.	Warranty	5 Years Comprehensive onsite OEM Warranty

7.2.11 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

7.2.12 Gas Based fire Suppression System

1. Gas Based Fire Suppression System (GBFSS)
   - The MSI 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 solenoid or pneumatic actuator) as the case may be, discharge pipe, non-return valveand 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 MSI 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 atotal 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 than5 days
   - be efficient, effective and does not require excessive space and high pressurefor storage
   - commercially available
   - *Key components are valves and its accessories, actuators, flexible dischargeand 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 dischargeof the agent in less than 10 seconds into the affected zone.
- The software calculation shall be approved VdS or FM / UL. The discharge timeshall 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 forunder 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 concentrationof 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 theagent'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 areashall 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 possibleto re-fill the cylinders in India itself.
   - The MSI 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 tofacilitate 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 of5m 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 orVds approved.
    - The detection of smoke by such detectors shall immediately set of 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 notbe 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 hydraulicflow calculation generated by using the agent's design software. Thecalculations shall validate the fill density assumed by the MSI.
    - The MSI shall submit copies of the datasheets of the hardware used in the system.
    - The MSI shall also submit copy of CCE approval letter for the cylinderproposed to be used.
    - The MSI shall also submit calculations to evidence the quantity of agentconsidered for the system.
    - The successful vendor must submit, along with the supply invoice, a certificateof authenticity, for the agent from the system engineering company dulychecked and verified by distributor.
    - The system engineering company should provide, as part of the handing over, the As built drawings and operation & maintenance manual.

7.2.13 Split Air Conditioner 2 Ton (5 star energy efficiency rating)

S. No	Function	Specifications
1.	Type	Cassette/high wall Type Split Type AC of suitable nominal cooling capacity operating on greener / environmental friendly refrigerant such as R407C/R410A best suitable to take care of environmental norms All indoor units shall be connected to VRV/VRF based outdoor units. Appropriate redundancy shall be maintained for rooms running 24 x 7.
2.	Rating	Operation on 230 V, 50 Hz, single phase, or 415 V, 50 Hz, three phase as required
3.	Remote	Cordless remote with centralised monitoring & control system
4.	Capability	Capable of performing - Cooling - Air Circulating - Filtering

5.		The split unit's shall be connected using Sequential controller working in periodic operations as per requirement in the area required
6.	Preferred Make	Daikin/ Toshiba/ Mitsubishi Heavy/Hitachi
7.	Warranty	5 Years Comprehensive onsite OEM Warranty from the date of Go-Live

7.2.14 ICCC Interior Specifications

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 one single solution i.e. operational control room. Main bidder to submit MAF from professional Control Room Interior Solution Provider for entire control room interior solution, MAF to be enclosed along with the bid.
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 of Preformed textured Hot dip galvanized strips and sheets of low carbon steel coated on one side with rigid polyvinylchloride (PVC) film and on the other side a coating based on cross linkable polyester resins (sheet thickness 0.6mm & PVC Coating 0.15mm).
7.	Control Room should be designed as per ISO 11064 and HFE norms, relevant Report & Control Room design animation of minimum 60 seconds must be submitted along with the bid.
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 & certified for Zone 5 Vibrations. Valid report from government approved test laboratory to be enclosed with the bid.
10.	Wall Panelling and Ceiling tiles must be Class A fire rated certified for surface burning characteristics. This is mandatory to ensure that the materials used in the interiors do not provoke fire. Valid certificate to be attached with the bid.
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 2500 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). Test report from reputed agency to be submitted along with the technical bid.
14.	UL Certificate on Load bearing capacity of Panelling - Panelling structure shall have load carrying capacity of 300 Kg to hold any display unit on. UL Certificate need to be enclosed along with the bid.

15.	**Partitions**
	• Partitions must be modular in nature.
	  ○ Straight Metal Partition
	  ▪ 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.

	○ Curvilinear Metal Partition ▪ All the properties and material of construction shall be like Metal panelling/partition but the front tiles shall be having perfect curve to meet the aesthetical requirement of the Control room and shall allow easy installation of the LVS/Screens on it. ○ Glass Partition ▪ Full glass wall partitions will be made of 12mm Toughened laminated glass with frame-less structure. The glass partition shall be supported by 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. ▪ 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. ○ The nature of installation should be replaceable, expandable and flexible to cater the future expansion/technical up-gradation. ○ 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 (Restriction of Hazardous Substance like Nickle, Cadmium etc.)
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 to be obtained from UL or Intertek 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. • Material Specification for Panelling o Factory made modular removable type self inter lockable metal panels of Preformed textured Hot dip galvanized strips and sheets of low carbon steel coated on one side with rigid polyvinylchloride (PVC) film and on the other side a coating based on cross linkable polyester resins (sheet thickness 0.6mm & PVC Coating 0.15mm). Make shall comprise of specially designed combination of perforated and non-perforated panels through CNC laser Cutting, bending & punching. Panel shall be of 0.75mm thick galvanized metal of approved color. Panels shall be designed to achieve shape and design as per the design consultant. Panels shall be fixed using hook fitting on structure. Overall system thickness for panelling shall be 70mm to 85mm and for partition shall be 85mm to 110mm. o As per design panel shall comprise of hexagonal perforation for making paneling and partitions acoustically sound. Acoustic grade fire retardant fabric (min 1.5mm thick) will be fixed at some parts of the control room. o 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: a. The cladding panels shall be made up of combination of two sheets locked and riveted together and polystyrene shall be used as infill to achieve strength and acoustics. The front tile (PVC pre-coated metal sheet) shall be perorated/ non-

	perforated as per the design requirement and the back tile (Powder coated 0.6mm GI sheet) shall be designed in such a manner that it fits on the back portion of the front tile. Once the tiles are fitted together then these will be manually riveted. These tiles shall be bend through CNC, machine punched & laser Cut to achieve perfect accuracy. b. 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. c. 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: a. For Panels: i. Front Panel: PVC pre-coated GI sheet (sheet thickness: 0.6mm and PVC coating: 0.15mm) ii. Back Cover: Powder coated GI sheet. (sheet thickness: 0.6mm with powder coating:) iii. 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. b. For Structure: i. Powder coated sheet. (sheet thickness: 1.0mm to 1.6mm with powder coating) ii. The metal sheet shall have possibility of being formed mechanically per the specific needs of the project.
21.	Material Selection: a. Available Width- 300mm to 1200mm (in multiples of 150mm). b. Available Height- 150mm to 750mm (in multiples of 150mm). c. Thickness- 10mm to 15mm for perforated tiles with acoustic fleece without back cover 25mm to 30mm for non-perforated tiles with back covers.

	d. PVC pre-coated sheet: i. Fire rating and Low flame spread: EN ISO 11925-2,/EN 13823 / ASTM E-84 e. Acoustic test: 9301/ ISO: 140/ASTM 413, ASTM C 578. f. Powder coating i. Adhesion test: EN ISO 2409 ii. Salt spray test: 600 hrs. iii. Resistance to humid atmosphere test: DIN 50017.
22.	**Acoustics Design** • 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). • 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. • 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 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.

7.3 ICT HARDWARE COMPONENTS FOR DATA CENTRE

7.3.1 Core Router

S.No.	Minimum Technical Requirements
1	**Architecture**
1.1	Router shall have Modular and distributed architecture, chassis based
1.2	Router shall have redundant management module or switching fabric.
1.3	Router shall have minimum 4 additional open slots in chassis (without any additional adaptor/module) apart from the Management/supervisor module slot
1.4	Shall be based on multi-core, multi-threaded processor
1.5	Shall have distributed forwarding architecture
1.6	The router shall be (1U/2U) Rack Mountable
1.7	Router Shall have minimum 8 nos. of 1G SFP ports & 8 x10G SFP+ portspopulated with appropriate transceivers as per solution/ design.
1.8	Router shall have 8 x 1G SFP Ports in addition to S. No. 1.5 with populated with appropriate transceivers as per solution/design.
1.9	Shall have up to 1Tbps backplane Bandwidth with redundant switching fabric
1.10	Console port, Auxiliary port/USB port/Management Port and Compact flash slots
1.11	Shall support various types of interfaces like 1G Ethernet, high-density 10 GbE WAN interface options.
1.12	Router shall have the sufficient free open slot for future scalability of 4 nos. of 10G SFP+ interface module
2	**Reliability Features**
2.1	Shall have dual routing processor/Management modules with 1:1 redundancy
2.2	Shall have redundant power supply (internal)
2.3	The Router shall support to connects multiple routers through physical ports to achieve system virtualization. All routers appears as one node on the network to allow for simplified configuration, while achieving high resiliency and increased system expandability
2.4	Support hot-swapping of interface cards, routing processor modules, power module and fan tray
2.5	VRRP/VRRPv3
2.6	MPLS TE FRR

2.7	IGP fast routing convergence
2.8	BFD: supporting collaboration with Static route/ RIP/OSPF/ISIS/ BGP/ VRRP/TE FRR
2.9	Graceful Restart: OSFP/BGP/IS-IS/ LDP/RSVP
2.10	Unified Modular operating system provides an easy to enhance and extend feature which doesn't require whole scale changes
3	**Layer 2 protocols**
3.1	ARP: Dynamic/static ARP, proxy ARP, gratuitous ARP
3.2	Ethernet, sub-interface VLAN
3.3	QinQ terminating
4	**IP services & IP Routing (any software/license required to enable these features shall be provided from Day 1)**
4.1	TCP, UDP, IP option, IP unnumbered
4.2	Policy-based routing
4.3	Static routing
4.4	Dynamic routing protocols: RIPv1/v2, OSPFv2, BGP, IS-IS
4.5	Route recursion
4.6	Routing policy
5	**IPv4 multicast (any software/license required to enable these features shall be provided from Day 1)**
5.1	IGMP (Internet Group Management Protocol) v1/v2/v3
5.2	PIM-DM, PIM-SM, PIM-SSM
5.3	MSDP (Multicast Source Discovery Protocol)
5.4	MBGP
5.5	Multicast routing
6	**Network protocols**
6.1	DHCP Server/Relay/Client
6.2	DNS Client
6.3	NTP Server/Client
6.4	Telnet Server/Client
6.5	TFTP Client
6.6	FTP Server/Client
6.7	UDP Helper
7	**IPv6 Features (any software/license required to enable these features shall be provided from Day 1)**
7.1	Basic functions: IPv6 ND, IPv6 PMTU, dual-stack forwarding, IPv6 ACL

7.2	Static routing
7.3	Dynamic routing protocols: RIPng, OSPFv3, IS-ISv6, BGP4+
7.4	IPv6 multicast:MLDv1/v2,PIM-DM,PIM-SM,PIM-SSM
8	**MPLS Features (any software/license required to enable these features shall be provided from Day 1)**
8.1	L3VPN: Inter-domain MPLS VPN (Option A/B/C), nested MPLS VPN, Hierarchy PE (HoPE), CE dual homing, MCE, multi-role host, GRE tunnel
8.2	L2VPN: Martini, Kompella, CCC, and SVC
8.3	MPLS TE, RSVP TE
8.4	Multicast VPN
9	**QoS**
9.1	Traffic classification: based on port, MAC address, IP address, IP priority, DSCP priority, TCP/UDP port number, and protocol type
9.2	Traffic policing: CAR rate limiting, granularity configurable
9.3	Rate limiting based on source/destination address (supporting subnet-based rate limiting)
9.4	Priority Mark/Remark
9.5	Queue scheduling mechanism: FIFO, PQ, CQ, WFQ, RTPQ, CBWFQ
9.6	Congestion avoidance algorithm: Tail-Drop, WRED
9.7	MPLS QoS and IPv6 QoS
9.8	HQoS/Nested QoS
10	**Security**
10.1	ACL and ACL acceleration
10.2	Time-based access control
10.3	Packet filter firewall
10.4	TCP attack prevention on local host
10.5	Control panel rate limiting
10.6	Virtual fragment reassembly
10.7	URPF
10.8	Hierarchical user management and password protection
10.9	AAA
10.10	RADIUS &TACACS
10.11	PKI Certification
10.12	SSH v1.5/2.0
10.13	RSA

10.14	IPSec, IPSec multi-instance, IKE
11	**Management & maintenance**
11.1	Configuration through the CLI, console, Telnet
11.2	Dial up configuration and remote maintenance
11.3	SNMP (v1, v2c, v3), RMON (group 1, 2, 3 and 9 MIB)
11.4	System logs, Hierarchical alarms
11.5	Ping and Traceroute
11.6	Network Quality Analysis, supporting collaboration with VRRP, policy- based routing, and static routing
11.7	Fan detection, maintenance, and alarm
11.8	Power supply detection, maintenance, and alarm
11.9	CF card detection, maintenance, and alarm
11.10	Temperature detection, alarm
11.11	Dual images
11.11	Loading/upgrading through FTP, TFTP
12	**Other Services**
12.1	Shall support Connection limit
12.2	Shall support NetStream/Slow/Netflow/equivalent
13	Regulatory Compliance
13.1	Router shall conform to UL 60950 or IEC 60950 or CSA 60950 or EN 60950 Standards for Safety requirements of Information Technology Equipment.
13.2	Router shall conform to EN 55022 Class A/B or CISPR22 Class A/B or CE Class A/B or FCC Class A/B Standards for EMC (Electro Magnetic Compatibility) requirements.

7.3.2 Core Switch

S.No.	**Minimum Technical Requirements**
1	**Architecture**
1.1	The Core switch should have chassis based, min. 6 slots for interface modules
1.2	The switch shall have Min Dual Management Modules/CPU/Supervisory Module/RoutingEngine with 1:1 redundancy
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 6 Tbps switching capacity and the chassis should support to upgrade up to9 Tbps switching capacity in feature
1.6	Shall have up to 2 Bpps switching throughput
1.7	Minimum 960 Gbps (Full Duplex) per-slot bandwidth
1.8	The chassis 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 distributed in min. 2 slots. Min. 8 ports shouldbe 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
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 through Equivalent SDN Technology. The Fabricshould be managed by a single IP Address.
3.5	The connected servers or switches should be attached using standard LACP for automaticload balancing and high availability
3.6	The virtual switching fabric shall be established over standard 10G Ethernet links
3.7	Virtual Router Redundancy Protocol (VRRP) support
3.8	Bidirectional Forwarding Detection (BFD) for RIP, OSPF, BGP, IS-IS and VRRP
3.9	Graceful restart for OSPF, IS-IS, BGP
3.10	UDLD or equivalent feature to prevent loops on detecting unidirectional links
3.11	Shall support a ring protocol to provide standard sub- 200 ms recovery for ring Ethernet-based topology
3.12	Shall support Virtual Extensible LAN (VXLAN), Software Defined Networking (SDN) architecture with OpenFlow 1.3 protocol.

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
4.11	DHCP Snooping and IP Source Guard
4.12	ARP attack protection
4.13	IEEE 802.1AE MACsec/Equivalent
5	**IPv4 & IPv6 Routing features (any software/license required to enable these features shallbe provided from Day 1)**
5.1	Static routing, RIPv1/v2
5.2	OSPFv2, IS-IS, BGPv4
5.3	Equal-Cost Multipath (ECMP)
5.4	Policy Based routing
5.5	RIPng/Equivalent OSPFv3, BGP4+, IS-ISv6
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 multicast routes.
5.9	Multicast Source Discovery Protocol (MSDP)
5.10	Unicast Reverse Path Forwarding (uRPF)
6	**Management & maintenance**
6.1	Configuration through the CLI, console, Telnet, 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**
7.1	OpenFlow protocol capability to enable software-defined networking

7.2	Allows the separation of data (packet forwarding) and control (routing decision) paths, tobe controlled by an external SDN Controller, utilizing Openflow protocol
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 or Switch Operating System should be EAL-2/NDPP certified

7.3.3 Firewall (NGFW)

S.No.	Minimum Technical Requirements
1	The next Generation Firewall should be Appliance based and have inbuilt features Firewall, IPS, Load balancing, QOS, VPN, AV, DPI, Application control for 3000+ applications
2	Support of 60 Gbps Maximum Firewall throughput
3	Support of 12 Gbps NGFW throughput all modules enabled
4	Support of 3000000 or more concurrent connections.
5	Support of 10 Gbps or more IPsec VPN throughput and Support of 10000 or more IPSec VPN Tunnels
6	The firewall should support a minimum of 8x 1G Copper Ethernet interfaces and 6x10G interface and 2x40 G Interface for future
7	For future redeployment flexibility, the firewall shall be a dedicated appliance supportingmulti product roles capable of switching between L2FW/IPS/NGFW roles without change of licenses and additional cost.
8	The Firewall should have option for URL Filtering 90+ categories and Cloud sandboxing for malware analysis if required with License upgrade.
9	The firewall shall achieve the following industry recognized security certification standards: Common Criteria EAL4+/NDPP, FIPS 140-2.
10	The firewall must include support for high availability feature - Active-Active Load Sharing or Active-Standby, Stateful failover including VPN connections.
11	The firewall must support high availability clustering within the same HA cluster.

12	The firewall must be a Next Generation firewall that includes features like Application ID, UserID and Intrusion Prevention System (IPS) as basic and not as an add-on license or subscription. The firewall must support Full QoS or DSCP/ToS Throttling with granular QoS configuration per interface and/or individual rule basis
13	The firewall shall support full stack, multilayer normalization and stream-based data inspection and detection processes to detect advanced evasion techniques. The firewall shall include anti-evasion capability.
14	The solution should have separate management console of security policies. The firewall management console should support HA and shall be capable of managing up to 20 NGFWnodes in future and integration with advance security (Web, Email and DLP console) . The firewall shall offer centralized management with integrated log server, with options to upgrade to multi domain architecture.
15	The firewall shall offer centralized management with integrated log server, with options to upgrade to multi domain architecture. The logs displayed on the firewall management console shall minimally contain the following fields on the same page: Timestamp, Sender (which Firewall sends the log), Geo Location, Source and Destination IP, Source and destination port, Service / Application, User, NAT address / Interface, Client Executable/File/MD5 hash, Rule, Event description, hit counts, action
16	The NGFW should transparently redirect HTTP and HTTPS traffic to a proxy on premises.

7.3.4 DC 48 Ports Switch for DMZ Managed

General	Descriptions
Device Type:	Switch supporting Full Enterprise Layer 3 features with Line rate non-blocking performance.
Architecture	Modular Switch to Provide 48 x (25/10/1 GbE) Ports and 6x 40 GbE QSFP28 Ports
Redundant Power supply and Fans	Should have Dual Internal Field Replaceable Hot Swappable Redundant AC Power Supply and Hot swappable Redundant Fans

Ports Requirement	Multi-rate switching :Support for 10G , 25G , 40 G and 100G from Day one
	The Switch should support below ports from Day 1
	32x 10G SR , 2x 40 G QSFP28 SR 2x 100G QSFP28 Passive Direct Attach cable 1m ,
High Availability	The switch should support HA options in Active - Active or Active Backup configuration as required, all supporting features and licenses to be provided to support the same.
Interfaces to connect Servers	The switch should support relevant 10G,10G base T , 25G , 40G and 100 G interfaces from day one
Performance	
Switching Capacity	Minimum 1.5 Tbps backplane or more
MAC Address Table Size	Minimum 96 K MAC addresses
802.1Q Vlans	4K 802.1Q vlans with 4K vlan ID support
Networking Features	
Data Link Protocol:	Ethernet, Fast Ethernet, Gigabit Ethernet, 10 Gigabit, 25 Gigabit , 40 Gigabit, 100 Gigabit
Routing Protocol:	Should support L3 routing in hardware for both IPv4 and IPv6 packets
	Should support IPv4 routes and IPv6 routes
	Should support Static Route, OSPF, BGP from Day one for both IPv4 and IPv6 considering all License, software, hardware upgrades required if any.
Link Aggregation	Should support 8 ports upto max 32 LAG groups, should be able to LAG across switches
Switching Protocol:	Ethernet
Status Indicators:	Link activity, port transmission speed, port duplex mode, power, link OK, system

Compliant Standards:	IEEE 802.3, IEEE 802.3u, IEEE 802.3z, IEEE 802.1D, IEEE 802.1Q, IEEE 802.3ab, IEEE 802.1p, IEEE 802.3x, IEEE 802.3ad (LACP), IEEE 802.1w, IEEE 802.1x, IEEE 802.1s, 802.3ae 10 Gigabit Ethernet, 802.3ba 40Gigabit Ethernet, 802.1p L2 Prioritization, 802.1Q VLAN Tagging, Double VLAN Tagging (Q in Q), GVRP, 802.1D Bridging, GARP,/ GMRP, 802.3x Flow Control, 802.1ac Frame Extension for VLAN tagging, 802.1x Port based Network Access Control Multicast : PIMSM/SSM, IGMP
Redundancy Protocols	Should support STP, RSTP, MSTP/PVST, Root Guard, BPDU Guard
	Converged network support for DCB, with priority flow control (802.1Qbb), ETS (802.1Qaz), DCBx and iSCSI TLV
	supports Routable RoCE and FIP Snooping to Enable convergence .
	Should support technologies similar to MLAG, ECMP, Stacking etc
Qos	Should support and create Policy Maps using DSCP values, QoS Rate Adjustment, Strict-priority Queueing/ Weighted Random Early Detection, minimum 8 hardwrae queues using 802.1p , DSCP
Security Features	
	Should support all AAA functions with RADIUS and TACACS integration., 802.1X
	Should support Layer 2 and layer 3 Acls
Management Function	
	Should support encrypted communication between the user accessing the device namely using all access methods CLI, GUI via NMS via features like SSHv2, SSL, and SNMPv3 and Secure FTP/TFTP , Ping,Telnet,Tracert for IPv4 and IPv6, sFlow
	Should support features like LLDP, LLDP-MED or equivalent
	Smart Scripting support through Perl/Python/Equivalent
	Software Defined Networking Support from day one without any license
Miscellaneous	

Physical parameter of switch	
Power Device:	Internal Hotswappable/redundant Power supply AC
Voltage Required:	AC 120/240 V (50/60 Hz)
Redundancy	Redundant, hot-swappable/redundant power supplies and fans
operating specifications	Operating temperature: 32°F to 113°F (0°C to 45°C)
Voltage Required:	AC 120/240 V (50/60 Hz)
Compliant Standards and Certifications	
Regulatory standrads	Should be ROHS , UL/CSA 60950 , EN550022 , EN 55024, EAL/NDcPP Compliant
Warranty and Support SLA	OEM warrant for 5 year 24x7 Next Business Day

7.3.5 24 Port L3 Edge Switches for Management

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: 212Gbps and forwarding rate of 150 Mpps
5	Should have minimum 32000 MAC address entries, minimum 4000 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 and VRF-lite from day one
8	Should have LAG load balancing, double VLAN tagging.
9	Should have dual firmware images on board. USB port for easy config & firmware image upload
10	Should support port Based ACLs, MAC based ACLs and minimum 1000 ACL rules from day 1.

11	Should have Flow based QoS, DiffServ, port based QoS, WRR, strict queue scheduling
12	Should support UDLD, 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, Private VLAN & Auto VLAN
16	Switch should be manageable through NMS on per port/switch basis. Should Support SNMP, RMON, SSH, 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, 802.3az EEE, REACH compliance, Switch should be EAL3/NDcPP certified.

7.3.6 24 Port Aggregation Switch

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.
2	Should have 24x RJ45 10/100/1000Mb POE+ auto-sensing ports, 4 x SFP+ ports. Switch should have minimum 500 watt power support for POE devices.
3	Should be able to support stacking with 40Gbps 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 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 on board. USB port for easy config & firmware image upload

9	Should support Time Based ACLs, MAC based ACLs and minimum 1000 ACL rules from day 1.
10	Should have Flow based QoS, DiffServ, port based QoS, WRR, strict queue scheduling
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, Private VLAN & Auto VLAN
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, captive portal
17	Switch should have 1GB RAM for its smooth operations
18	Should operate at 220VAC ~50Hz. Switch Should support external RPS.
19	Should be RoHS, 802.3az EEE, REACH compliance.

7.3.7 42U Server Rack with necessary accessories

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 form 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

7.3.8 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, in case of active mid plane it should be redundant
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 6 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 10G uplinks
FC Switches	The Chassis should have redundant FC switches, each switch should have 4 no. of 32Gbps FC uplinks to SAN
Management	The chassis should have a touch screen LCD display
	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. Post installation, 5-year product warranty should reflect in the support web site of the OEM.

7.3.9 Blade Server

Feature	Specification
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 OS & 4 x 1.2TB 10K RPM SAS HDD in RAID-6 for data Server should be configured with integrated RAID controller to support RAID level 0,1,5,6 on internal disks, Server should have 6 nos. of 2.5inch HDD bays
Ethernet ports	2 * 25GbE network ports for ethernet
FC ports	2 * 32Gbps 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
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.
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 root of trust
Pre-failure alert	Should provide predictive failure monitoring & proactive alerts of actual or impending component failure for fan, memory,HDD
Configuration & management	• 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
Systems Management Software	The server should come with systems management software to provide update management, configuration management, patch management and virtualization management.
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.

7.3.10 GPU Server

Parameter	Specifications
Rack Height	2U or lower
CPU Support	Must support 2 CPU's
Chipset	Intel C610 or better

Processors	2 x Intel Xeon processor 2.2 Ghz, 12 Core
Cache	8 MB L3 Cache per CPU or more
Memory	4x 32 GB RAM 2666 MT/s support up to 1500GB RAM, should have min. 16 DIMM slots
Hard Drives	4x3.84Tb SSD & 4x 1.2TB 10K RPM SAS
	Should support up to eight hard disk drives (SAS, SATA, nearline SAS SSD: SAS, SATA)
GPU Configured	Should be configured with 3nos. Of Nvidia tesla T4 GPU
GPU Support	Should support upto 6 single wide GPU's
RAID Card	RAID Controller Card supports RAID 1, 5, 10 with 4 GB Cache
PCI Slots (I/O)	4 x PCIe 2.0/3.0 slots
NIC ports	2x1G & 2x10G baseT ports
Redundant Power Supply	Dual, Hot-plug, Redundant Power Supply
SD Modules slots	Dual SD Module slots supporting redundant configuration
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
Management (continued)	• Automated hardware configuration and Operating System deployment to multiple servers
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	Should have a cyber resilient architecture for a hardened server design for protection, detection & recovery from cyber attacks or equivalent
	Should protect against firmware which executes before the OS boots
	Should maintain repository for firmware and should be able to rollback, if required.
OS	Windows server 2016 Standard Edition with downgrade rights to 2012R2 Std

Warranty	5 years On-site comprehensive warranty with 24x7x365 remote hardware support.

7.3.11 Continuous Learning Server A.I/Training Server

Parameter	Specifications
Rack Height	4U or lower
CPU Support	Must support 2 CPU's
Chipset	Intel C620 or better
Processors	2 x Intel Xeon processor 2.2 Ghz, 12 Core
Cache	8 MB L3 Cache per CPU or more
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 A100 32Gb GPU
GPU Support	Should support upto 6 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	• 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

Management (continued)	• Automated hardware configuration and Operating System deployment to multiple servers • Support for Redfish API for simple and secure management of scalable platform hardware
HTML5 support	HTML5 support for virtual console & virtual media without using Java or ActiveX plugins
Server security	Should have a cyber resilient architecture for a hardened server design for protection, detection & recovery from cyber attacks or equivalent
	Should protect against firmware which executes before the OS boots
	Should maintain repository for firmware and should be able to rollback, if required.
OS	Windows server 2016 Standard Edition
Warranty	5 years On-site comprehensive warranty with 24x7x365 remote hardware support.

7.3.12 AAA server

S. No.	Parameter	Specifications
AAA Server (Hardware Appliance) (for scalability upto 1000 endpoints)		
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		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:
		• 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		Policy creation tools:
		• Pre-configured templates
		• Wizard based interface
		• LDAP browser for quick look-up of AD attributes
		• 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 3rd party system to manage guest accounts.

7.3.13 8 Port PoE Ruggedized Switch

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 (IPv6 Logo Committee certified)
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 20 switches in One Single Ring and have recovery time of <30ms.

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
	ENVIORNMENTAL
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

7.3.14 Server Load Balancer

Sr No.	Minimum Technical Specification
1	The Load Balancer device should be a dedicated Hardware Appliance with the following features: 1) Should support multiple virtual network functions in which each VNF has a dedicated resourcs alloted to it like CPU, RAM, Hard Disk, SSL cores and can install & run 3rd party and open source VNFs on the same appliance for future scalability. 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. 3) The Load Balancer shall automatically synchronize configurations between the pair and automatically failover if any fault is detected with the primary unit. 4) The device should support upto 16 virtual instances. Should have internal redundant Power supply with 512 TB usable hard disk, 16 GB RAM and capability to host other 3rd party and open source virtual network functions like SSL VPN, web application firewall etc.

2	The Load Balancer shall support offloading of SSL connections and should deliver 25 Gbps of SSL throughput on 1024 key.
3	Proposed device should have minimum 4 x 10G SFP+ ports prepopulated and upto 1 x 40 QSFP ports
4	Proposed device should support upto 8 virtual instances with capability to run multiple virtual network functions like Linux-CentOS/ Ubuntu etc. in same appliance
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	The solution should support XML-RPC for integration with 3rd party management and monitoring. Should also support AAA, HOTSPOT mgmt, Domain mgmt, captive portal, 2 FA, Wireless Hotspot Gateway, SAA, SAML, Hardware binding and AAA support along with SSO. Solution must support machine authentication based on combination of HDD ID, CPU info and OS related parameters i.e. mac address to provide secure access to corporate resources.
9	Should have secure access solutions for mobile PDAs, Android, Windows and iOS based smart phones and tablets with machine authentication
10	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.
11	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.
12	The solution should support Multi-level virtual service policy routing ,-Static, default and backup policies for intelligent traffic distribution to backend servers
13	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/DNS64/NAT 64/ DNS 46/NAT 46/ IPv6 NAT
14	The solution should support advance ACL's to protect against network based flooding attacks. Administrator should able to define ACL's rules based on connections per second (CPS) and concurrent connections (CC), cookie value.

15	The solution should provide comprehensive and reliable support for high availability and N+1 clustering through standard VRRP on Per VIP based Active-active & active standby unit redundancy mode.
16	OEM should have presence in India since last 5 years and have 24 x 7 TAC in India

7.3.15 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	The switch must support Smart Zoning such that the entries in the TCAM is significantly reduced and therefore increasing the overall scalability of the SAN Fabric.

14	The switch must support Power On Auto Provisioning (POAP) and Quick Configuration Wizard for simplified operations.
15	Inter-switch links must support the transport of multiple Virtual Fabrics between switches, whilst preserving the security between Virtual Fabrics.
16	The switch must support routing between Virtual Fabric instances in hardware.
17	The switch shall support FC-SP for host-to-switch and switch-to-switch authentication.
18	ID and Destination ID. The support for load balancing utilizing the Exchange ID must also be supported.
19	The switch must be equipped with congestion control mechanisms such that it is able to throttle back traffic away from a congested link.
20	The switch must be capable of discovering neighbouring switches and identify the neighbouring Fibre Channel or Ethernet switches.
21	The switch should support IPv6.

7.3.16 Scale Out Storage

Sr. No.	Feature	Description of Scale-Out Storage Specifications
1	**Controllers and Architecture**	- Storage Should be Fully Symmetric and fully distributed clustered /federated Architecture written for Scale-Out Storage operations - Scale out storage should be configured with minimum 4 controllers of the same type -capacity enhancement, software/firmware upgrades. - The storage cluster should support linear scalability of perfomance and capacity. ie for every drive added, performance should increase by the same amount till the maximum capacity of the storage - All storage nodes/controllers must be active for all Storage shares, contributing in performance and capacity of the system
2	**Onboard Memory**	The scale out storage must be configured with minimum 512 GB DRAM based cache/memory.

3	**Operating System**	Scale-Out Storage operating system should have Fully journaled, fully distributed, specialised Operating System by OEM , dedicated for serving data efficiently and customised 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 30 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)**	'- The Scale-Out Storage should have self-optimizing architecture in the event of an ungraceful shutdown of the cluster to ensure higher uptime. - 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. - 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**	- Scale out storage should be configured with 4 PB usable capacity , using equal to or less than 12TB NL-SAS/SATA HDD. Additional 30% usable space should be reserved, or equivalent number of disks should be provided, as hot spares. Storage should be the capability of using the hot spare area for data writes, without affecting VMS data flow, in case need arises. - Offered scale out storage should be capable of providing a throughput of greater than 15GBps at 100% write on SMB2 or equivalent, for handling the camera feed and other workloads. Dimensioning tool output needs to be provided on OEM letterhead for the same - The storage should be scalable upto 2x the capacity, and performance, with same drive size
8	**Capacity/performance Expansion**	- 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 autobalance 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.
9	**Protection Levels**	- 10PB usable capacity and hot spare space should be configured with protection level which can protect data against simultaneous 2/3 disks 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, directory or file level or as per OEM Design
10	**Protocol Support**	- Network protocol Support: • Must provide access for a variety of operating systems (UNIX, Mac, Linux, Windows) using OS protocols. All protocols, supported by the storage MUST be included without additional licenses and hardware. Should support user security mechanisms like AD,LDAP/ NIS.
11	**File Locking & Filtering**	File Locking for Data protection from corruption while sharing files between UNIX and Windows users.
12	**Client Load Balancing**	Storage System should have capability to load balance client connectivity across these multiple controllers/drives so that all clients gets distributed across all existing controllers/nodes/drives to avoid any performance hotspot.
13	**Heterogenous support for end user systems**	Operating system support RedHat Linux, Suse Linux, Windows , Unix Based operating systems like SUN solaris, HP Unix, IBM AIX
14	**Management Interface software**	Support the management, administration and configuration of the whole storage platform through a single management interface along with CLI or equivalent

15	**Security**	- The system must support encrypting data at rest. - The system must support multiple multitenant access zones for different Active Directories and LDAP. Each Access zone must simultaneously support local, Active Directory and LDAP users. - The system must support Role Base Access Control with Integration with Active Directory and LDAP . - The system must be able to support System Auditing for system as well as supported protocols. - The system must support multiple DNS. - The system must be able to support Anti Virus Scanning through Internet Content Adaptation (ICAP) protocol.
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

7.3.17 Unified Storage

Parameters	Description
Type of Storage System	Storage Array (should be a purpose built appliance)should be unified storage with a single microcode / Operating system. Proposed Storage shall be the latest generation storage from the respective OEM. The storage array must support block, file services and VVOL natively or by providing addon gateway/controllers in redundant configuration.
Capacity	100 TB Usable using SSD Drive of size less than 3.84TB. Raid 5/6 can be used to provision this capacity 1900TB Usable using NL-SAS Drive ;RAID 6 must be used to provision this capacity
RAID Functionality	Storage should have RAID levels support for RAID 1/0, 5 & 6
Processors	Unified storage must have atleast 24Cores Intel Skylake x86 based processor per controller or better . Incase additional gateway is being provided than gateways to be provided in redundancy. Each Gateway must have 32Cores x86 based processors
Cache Memory	Proposed storage shall have atleast Dual active-active controllers with minimum 128 GB primary DRAM cache DRAM cache shall be protected with Cache destaging or battery backup.

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, NAS Quota Management, Anti-Virus integration for NAS, 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 or 8X8 Gbps
	b. 4 x 25 Gbps Ports. All 25GbE ports should be capable to deliver both iSCSI/NFS, CIFS/SMB/sFTP etc. In case iSCSI and NAS protocols are served from different ports then 4x 25G iSCSI and 4x 25G NAS ports should be proposed.
GUI Application	Storage management software should be configured with HTML5 based graphical user interface and it should be configured with single interface for managing all BLOCK and NAS Protocols. The storage management software should display graphical depiction of storage hardware components with capability of tracking system and state information.

File System	Storage must support 64 bit file system and allow creating multiple NAS servers for tenant isolation with each file system scalable upto 128TB. If NAS is being provided as hardware module or gateway then it must be redundant. Each of the above hardware module or gateway must have 512GB DRAM Cache/Memory Each file system must support multi-protocol access via SMB / NFS. Data must be able to access from client concurrently using these protocols. NAS must support FTP / SFTP access to File data/directory/File System. If this is not available then additional hardware with commercial FTP server with 250 concurrent users to be provided in redundancy. NAS must be able to leverage Active directory or LDAP for authentication purposes also. The File system or NAS must provide functionality for preventing modifying and deletion by user when accessed via SMB/NFS till the time lock has been set to date in future. The File system or NAS must support functionality for preventing deletion of file system having locked files by admin before the expiry of lock set to a date in future. NAS Servers must support IP Multi tenancy with each tenant has its own dedicated network namespace including VLAN domain, routing table, firewall, interfaces, DNS and more if required. or equivalent solution can be provided by providing additional software/hardware The NAS must support CAVA or equivalent feature
Snapshots	SAN should support minimum 200 snapshots . Proposed storage solution should support snapshot creation using ROW (Redirect on write) algorithm. Storage arrays should have ability to use snapshot as writable volume. Proposed system should support snapshot scheduler. Proposed storage should allow snapshot replication with different retention for source and destination.
Automatic Tiering	The proposed storage system must support SSD based cache for read and write I/Os, Atleast 200GB (SSD SAS based) cache to be provided mirror protected. If not available then atleast 128GB DRAM Cache to be provided.

WORM Support	Storage shall have capability for protecting files from modification or deletion until a specified retention date to allows customers to create a permanent, unalterable set of files and directories and ensure the integrity of data.
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 and File Protocols. This should also provide licenses for capability to complete failover and failback for NAS servers along with settings from day 1
Quality of Service	The Storage should have the capability to provide Quality of Service (QoS) feature to limit IOPS or Throughput for test/dev hosts so that they do not use beyond permitted resources
Predictive Analytics	Storage OEM shall provide software-as-a-service cloud management dashboard that provides monitoring and reporting multiple storage system, VMware environment and SAN switches. Required on-prem software and hardware should be included in the solution. Cloud based software should be accessible from any internet connected device with mobile application support for iOS and Android. The tool should provide comprehensive monitoring of system health, performance, capacity, configurations, and on-array protection metrics. Tool shall have machine learning and predictive analytic measurements by using the metrics to improve capacity planning and fix problems before they disrupt business. Tool shall provide a comprehensive and proactive health score per array to ensure that each array provides the optimal foundation for running business data with the highest availability.
Data Copy Management	A data copy management for database (oracle, SQL) with capability and license for mounting and maintaining 10 simultaneous copies

Data Archiving to Cloud	Proposed solution should include software for policy based data archiving solution to archive data from storage to secondary archival software. Software should support both NAS and Block level data archival to on-prem target or to public clouds like AWS, Azure etc. Details on supported targets to be submitted.
Investment Protection	the storage array shall support online upgrade to higher model by replacing the controllers for meeting higher performance and scalability.
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 and Backup solution should be from same OEM
	Storage software, hardware and support all should come from same and single OEM

7.3.18 300 KVA UPS

Sr. no	Parameter
	SCOPE OF SUPPLY :
	This specification is set for the design, manufacture, testing at manufacturer's works, supply, erection, testing,Installation and commissioning of 200 KVA Uninterruptible Power System (UPS) which can be connected in Parallel (Add ON) configuration and facility to connect one or two more nos. of UPS to be in parallel in future. Each UPS is with SMF / valve-regulated lead-acid batteries (VRLA) housed in one or more external racks and providing a minimum autonomy as defined under "Batteries" herein.
	The present specifications contain minimum requirements. All offers must be completed strictly in accordance therewith, either by confirming data or by filling in the spaces provided, where requirements are not met.
	Any deviations, or exceptions to, the minimum requirements must appear in the offer.
	Where no exceptions are shown, the requirements of the present specifications will be considered as accepted.

	1.1 SUMMARY
	These specifications describe requirements for an Uninterruptible Power System (UPS) optimized for maximum efficiency. The UPS shall automatically maintain AC power to the critical load within specified tolerances and without interruption during failure or deterioration of the normal power source. The manufacturer shall design and furnish all materials and equipment to be fully compatible with electrical, environmental and space conditions at the site. The UPS shall include all equipment to properly interface the AC power source to the intended load and shall be designed for unattended operation.
	1.2 VENDOR QUALIFICATION CRITERIA
	Vendor quoting should be an OEM & have manufacturing facility in India.
	Vendor should be certified for ISO 9001(QMS), ISO 14001(EMS) & ISO 18001(OSHAS).
	Vendor should have their own service setup across the country to guaranty service
	support as per service level agreements.
	1.3 STANDARDS
	The UPS and all associated equipment and components shall be manufactured in accordance with the
	following applicable standards:
	• Safety Requirements: IEC 62040-1-1, EN 50091-1-1
	• EMC: IEC 62040-2 (Class A), EN 50091-2 (Class A)
	• Performance: IEC 62040-3 (VFI SS 111), EN50091-3
	The above mentioned product standards incorporate relevant compliance clauses with generic IEC and EN standards for safety (60950), electromagnetic emission and immunity (61000 series) and construction EN standards for safety (60950), electromagnetic emission and immunity (61000 series) and construction
	• IEC 61000-3-4
	• IEC 61000-4-2, 4, 5, 6, 8, 11
	• EN60950
	• EN60529
	• IEC 60146-1-1

	The UPS is CE marked in accordance with EEC directives 73/23 “low voltage” and 89/336 “electromagnetic compatibility”. The Quality System for the engineering and manufacturing facility certificated to conform to Quality System Standard ISO 9001 for the design and manufacture of power protection systems for computers and other sensitive electronics.
	1.4 SYSTEM DESCRIPTION
	1.4.1 Design Requirements
	The UPS shall be rated to provide a minimum of 180kW on the output. The required UPS kVA rating will be set the same as the minimum kW rating. (Unity power factor) The UPS shall be able to supply all required power to full rated output kVA loads with power factor from 0.5 lagging to 0.9 leading. The UPS shall also work from 0.8 power factor to 0.5 leading power factors subject to derating.
	Load voltage and bypass line voltage shall be 400VAC, three-phase, four-wire plus ground. Input voltage shall be 400VAC, three-phase, four-wire plus ground. The AC input source and bypass input source shall each be a solidly grounded wye service. The battery shall support the UPS at the rated kW load for at least 30 minutes at 25°C at startup.
	The UPS shall have an active power factor-corrected IGBT converter/rectifier, capable of maintaining input power factor and input current total harmonic distortion (THDi) within specifications without an additional input filter.
	The UPS shall be of transformer-free design, requiring no internal ransformer in the main power path for the basic operation of the module. Optional output transformers in cabinets to the basic UPS module shall be permissible to provide isolation.
	For 200 KVA : The entire system shall be working in eco mode / Double Conversion Mode as and when selected / required .
	The parallel system shall have provision for common battery option for cost optimization purpose.
	The battery shall be sized at 180 kW load per each UPS for at least 30 minutes at 25°C per UPS .
	UPS shall have a provision for inbuilt Isolation Transformer connected at final output side (after Inverter and St. Bypass) so as to have total galvanic Isolation during both situation ,when load is either on Inverter Or Bypass .
	1.4.2 Modes of Operation

	The UPS shall operate as an on-line reverse transfer system in the following modes:
	A. Normal: The critical AC load is continuously powered by the UPS inverter. The rectifier/charger derives power from the utility AC source and supplies DC power to the DC-DC converter, which in turn supplies the inverter while simultaneously float charging the battery.
	A. Energy Optimization / Eco Mode: The critical AC load is continuously powered by the bypass with the inverter available to power the load if the bypass source voltage or frequency exceeds adjustable parameters of power quality.
	B. Emergency / Battery : Upon failure of utility AC power, the critical AC load is powered by the inverter, which, without any switching, obtains its power from the battery plant via the DC booster. There shall be no interruption in power to the critical load upon failure or restoration of the utility AC source.
	C. Recharge: Upon restoration of the utility AC source, the rectifier supplies power to the DC-DC converter and the output inverter. The rectifier powers the inverter and simultaneously recharges the battery. This shall be an automatic function and shall cause no power interruption to the critical AC load.
	A. Bypass: If the UPS must be taken out of service for maintenance or repair, the static transfer switch shall transfer the critical load to the bypass source. The transfer process shall cause no interruption in power to the critical AC load.
	B. Off-Battery: If the battery only is taken out of service for maintenance, it is disconnected from the DC-DC booster by means of an external disconnect circuit breaker. The UPS shall continue to function and meet all of the specified steady-state performance criteria, except for the power outage backup time capability.
	If multiple battery strings are used, each string shall be capable of being electrically isolated for safety during maintenance.
	1.1.1 **Performance Requirements**
	The solid-state power components, magnetic, electronic devices and over-current protection devices shall operate within the manufacturer's recommended temperature when the UPS is operating at 100% capacity, supporting critical load and maintain battery charging with the following conditions occurring simultaneously.
	· Any altitude within the specified operating range ≤1500m elevation.
	· Any ambient temperature within the specified operating range of 0°C to 40°C (32°F to 104°F). (Note: Battery life is halved for every 10°C increase above 20°C).
	· Relative humidity (RH) within 0 to 95% , non-condensing.

	· Environment pollution level 2
	· Any input voltage within the specified range, +30% to -15% of nominal
	1.1.1 Input
	A. Voltage: Input/output voltage specifications of the UPS shall be
	Rectifier AC Input: 380/400/415V, three-phase, four-wire-plus-ground (Also compatible with 3-wire system)
	Bypass AC Input: 380/400/415V, three-phase, four-wire-plus-ground
	AC Output: 380/400/415V, three-phase, four-wire-plus-ground
	A. Voltage Range: +20%, -15% of nominal (- 40% at half load)
	B. Frequency Range: 40Hz to 70Hz
	C. Rectifier Walk-In: 0% to 100% of full rated load over 1-30 seconds
	D. Max Inrush Current : ≤1 In
	E. Power Factor: ≥0.99 at full load with nominal input voltage
	F. Generator Ada ptability: UPS input current limit can be adjusted to suit generator power rating. Wide input frequency range is permissible.
	G. Current Distortion: ≤ 3% THD at full load, UPS in double-conversion mode
	H. Surge Protection: Sustains input surges of 4kV (Line to ground) without damage as per criteria listed in EN 61000-4-5: 1995
	1.1.1 **AC Output**
	A. Load Rating: 100% load rating at 104°F (40°C) for 8 hours for any combination of linear and non-linear loads; 100% of load rating continuous at 95°F (35°C)
	B. Voltage Regulation: <1% RMS average for a balanced three phase load in Steady State ; ±2% for 100%
	unbalanced load for line-to-line imbalances
	C. Manual Voltage Adjustment Range: ±5% for line drop compensation adjustable by factory service personnel .
	D. Frequency Regulation:
	Synchronized to bypass: ±2.0Hz default setting, (shall be adjustable by factory service personnel)
	Synchronized to internal clock 0.1%
	E. Efficiency: Defined as output kW/input kW at rated lagging load power factor ; and not less than the values listed below (figures w/o Iso. Txr.)

	>95.5% at 100% Load, > 95.5 % at 75-40% Load .
	F. Phase Imbalance:
	Balanced loads 120° ±1°
	100% unbalanced loads 120° ±2°
	G. Voltage Transients (average of all three phases):
	• 0-100% or 100-0%
	Response Meets IEC 62040-3: 2010 Figure 2 Curve 1, Class 1 Meets ITIC and CBEMA Curve Requirements
	• 10-100% or 100-30%
	Transient Voltage Deviation, RMS 5%
	A. Output Voltage Transients
	Voltage transients shall be limited to a maximum deviation from nominal system output volts of ± 5% with recovery to within 1% of the nominal output voltage within one electrical cycle (20 milliseconds) for each of the following conditions. Limits shall apply to any UPS load within the UPS rating, and frequency shall be maintained at 50 Hz ± 0.1 Hz. The system shall not transfer to bypass under these conditions (except item 3).
	1. 100% load step
	2. Loss or return of AC input power, momentary sags, surges or spikes on the input to the UPS (all three phases or single phase)
	3. Uninterrupted transfer of the critical load to and from the UPS output and bypass power line (manually initiated or automatic)
	A. Voltage Harmonic Distortion:
	Maximum <2% (100% linear load)
	Maximum <5% (100% non-linear load, per IEC 62040-3)
	A. Overload at full Output Voltage with ±1% voltage regulation:
	100% continuously
	105% - 130% of full load for 60 minutes at 40°C ambient
	130% - 125% of full load for 10 minutes at 40°C ambient
	125% - 150% of full load for 60 seconds at 40°C ambient
	>150% of full load for a minimum of 200 milliseconds at 40°C ambient
	K. Current Limit: 300% nominal current

	L. Fault Clearing:
	· **Inverter only:** 300% of normal full load current for 10 milliseconds or 150% of normal full load current for <5 seconds (when bypass is not available).
	· **Bypass available:** 1000% for 100 milliseconds in inverter pulse-parallel operation when bypass is available.
	1.4.6 Earthing/ Grounding
	The UPS chassis shall have an appropriate equipment earthing terminal.
	1.5 ENVIRONMENTAL CONDITIONS
	The UPS shall be able to withstand the following environmental conditions without damage or degradation of operating characteristics:
	A. Operating Ambient Temperature
	UPS: 0°C to 40°C (32°F to 104°F)
	Battery: 25°C (77°F), ±3°C (±5°F)
	A. Storage/Transport Ambient Temperature
	-15°C to 50°C (-4°F to 158°F)
	C. Relative Humidity
	0 to 95%, non-condensing
	D. Altitude
	Operating: ≤ 1500m; derate power by 1% per 100m between 1500m and 3000m
	Storage/Transport: To 50,000 ft. (15,000m) above Mean Sea Level
	E. Audible Noise Level
	• 65 dBA measured 1m from the surface of the unit
	1.1 WARRANTY
	1.1.1 **UPS Warranty**
	The UP S manufacturer shall warrant the unit against defects in workmanship and materials for 12 months after initial startup or 18 months after the shipping date, whichever comes first.
	1.1.1 **Warranty - End User**
	Warranties associated with buyout items shall be passed through to the end user.
	1.2 QUALITY ASSURANCE
	1.2.1 **Manufacturer Qualifications**

	A minimum of 20 years' experience in the design, manufacture and testing of solid-state UPS systems is required.
	1.1.1 **Factory Testing**
	Before shipment, the manufacturer shall fully and completely test the UPS unit to ensure compliance with the specification.
	The UPS unit shall be tested at the system-specified capacity. Testing shall be done using load banks at part-load and the full kW rating of the unit.
	Operational discharge and recharge tests to ensure guaranteed rated performance.
	System operations such as startup, shutdown and transfers shall be demonstrated.
	A certified copy of the test results shall be available for each system as indicated on the order.
	2.0 PRODUCT
	1.1 FABRICATION
	1.1.1 **Materials**
	All materials of the UPS shall be new, of current manufacture, high grade and shall not have been in prior service except as required during factory testing. All active electronic devices shall be solid-state. All power semiconductors shall be sealed. Control logic and fuses shall be physically isolated from power train components to ensure operator safety and protection from heat.
	1.1.1 **UPS Internal Wiring**
	Wiring practices, materials and coding shall be in accordance with the requirements of the National Electrical Code and applicable local codes and standards. All bolted connections of busbars, lugs and cables shall be in accordance with requirements of the National Electric Code and other applicable standards. All electrical power connections shall be torqued to the required value and marked with a visual indicator.
	2.1.3 Field Wiring
	All field wiring power connections shall be to tin-plated copper busbars for connection integrity. Busbars shall have adequate space to allow two-hole, long-barrel, compression type lugs forming a permanent connection between field wiring and field-installed lugs. Provisions shall be made in the cabinets to permit installation of input, output and external control cabling using raceway or conduit. Provision shall be made for top and bottom access to input, output, bypass and DC connections. In conformance with the NEC, connection cabinets shall provide for adequate wire bend radius.

	2.1.5 **Construction and Mounting**
	The UPS shall be in an IP20 enclosure, designed for floor mounting. The UPS shall be structurally adequate and shall have provisions for hoisting, jacking and forklift handling. Maximum cabinet height shall be 2145mm (85in.).
	2.1.6 Cooling
	Adequate ventilation shall be provided to ensure that all components are operated well within temperature ratings.
	Temperature sensors shall be provided to monitor the UPS's internal temperature. Upon detection of temperatures in excess of the manufacturer's recommendations, the sensors shall cause audible and visual alarms to be sounded on the UPS control panel.
	Air filters shall be located at the point of air inlet and shall be changeable. Recommended service and ventilation clearance of 500mm shall be required in the rear of the system.
	2.1 **EQUIPMENT**
	2.2.1 UPS System
	The UPS system shall consist of an IGBT power factor-corrected rectifier, DC-DC booster and three-phase transformer-free inverter, bypass static transfer switch, bypass synchronizing circuitry, protective devices and accessories as specified. The specified system shall also include a battery disconnect breaker and battery system.
	2.2.2 Surge Protection
	The UPS shall have built-in protection against surges, sags and overcurrent from the AC source. The protection shall meet the requirements of IEC/EN 61000-4-5 including: Level 4 (4kV) (Line to Earth), Level 3 (2kV) (Line to Line) Based on B
	2.2.3 Configurations
	The UPS system shall consist of one unit of UPS of the same kVA rating in a stand alone configuration . Systems greater than one module (at a later stage) shall be able to operate simultaneously in a Parallel configuration .
	2.2.4 System Protection
	The UPS shall have built-in protection against: surges, sags and over-current from the AC rectifier input source, over-voltage and voltage surges from output terminals of paralleled sources, and load switching as well as circuit breaker operation in the distribution system.

	The UPS shall be protected against sudden changes in output load and short circuits at the output terminals. The UPS shall have built-in protection against permanent damage to itself and the connected load for all predictable types of malfunctions. Fast-acting, current-limiting devices shall be used to protect against cascading failure of solid-state devices. Internal UPS malfunctions shall cause the module to trip off-line with minimum damage to the module and provide maximum information to maintenance personnel regarding the reason for tripping off-line. The load shall be automatically transferred to the bypass line uninterrupted, should there be an internal UPS malfunction or should the connected critical load exceed the capacity of the available on-line modules. The status of protective devices shall be indicated on a graphic display screen on the front of the unit.
	2.2 COMPONENTS
	2.2.3 Rectifier
	The term ***rectifier*** shall denote the solid-state equipment and controls necessary to convert alternating current (AC) to regulated direct current (DC) to simultaneously supply the inverter and charge the battery. The rectifier shall be of DSP (Digital Signal Processor) controlled design and utilize insulated gate bipolar transistors (IGBTs). The DC output of the rectifier will meet the input requirements of the inverter even without the battery being connected.
	A. Input Current Harmonic Distortion
	The rectifier shall actively control and reduce input current distortion over the full operating range of the UPS without the need for an additional passive input filter. Input current THD shall be less than 3% at rated load and nominal voltage in double-conversion mode.
	B. Dynamic Current Input Limit Reduction
	The rectifier, in conjunction with the other UPS controls and circuitry, shall adjust the current demanded for battery charging as a function of UPS wattage load and input voltage level
	C. Input Power factor correction: The rectifier also performs a PFC function; input power factor shall be a minimum 0.99 at 100% load and 0.98 at 50% load.
	D. AC Input Current Limiting: The maximum Input current limit can be reduced at 100% for generator operation.

	E. Input Power Walk-In: The rectifier/charger shall provide a feature that limits, during the transfer from battery mode to line mode, the total initial power requirement at the input terminals to 0% of rated load and gradually increases power to 100% of full rating over the 30-second (adjustable) time interval
	F. Fuse Protection
	Each AC phase shall be individually fused with fast-acting fuses so that loss of any semiconductor shall not cause cascading failures.
	2.2.3 DC-DC Booster
	The term DC-DC converter shall denote the equipment and controls to regulate the output of the rectifier to the levels appropriate for charging the battery and to boost the battery voltage to the level required to operate the inverter. The DC-DC converter shall be solid-state, capable of providing rated output power and, for increased performance, shall be a pulse width-modulated design and shall utilize insulated gate bipolar transistors (IGBTs). The DC-DC converter shall control charging of the battery. The AC ripple voltage of the charger DC shall not exceed 1% RMS of the float voltage.
	A. Battery Recharge
	In addition to supplying power for the load, the rectifier/charger shall be capable of producing battery charging current sufficient to replace 95% of the battery discharge power within ten (10) times the discharge time. After the battery is recharged, the rectifier/charger shall maintain the battery at full charge until the next emergency operation. Ripple voltage at the battery terminal (RMS) should be less than 1%, and ripple current must not exceed 5% (of C-10 Ah rating) nominal discharging current.
	B. Battery Equalize Charge : A manually initiated equalize charge feature shall be provided to apply an equalize voltage to the battery. The duration of equalize charge time shall be adjustable from 8 to 30 hours. A method shall be available to deactivate this feature for valve regulated battery systems.
	C. Temperature-Compensated Charging
	The UPS shall adjust the battery charging voltage based on the battery temperature reported from external battery temperature sensors. Temperature sensors shall be monitored for faulty measurements and ignored if a fault is detected to prevent over or under changing the battery. When multiple sensors are used the voltage shall be based on the average temperature measured. Excessive difference in the temperature measurements shall be reported and the charging voltage adjusted to protect the batteries from excessive current.
	D. Battery Load Testing

	The UPS shall be capable of performing battery load testing under operator supervision. To accomplish this, the rectifier shall reduce charging voltage to force the batteries to carry the load for a short time. If the curve of battery voltage drop indicates diminished battery capacity, the UPS shall display an alarm message. If the voltage drop indicates battery failure, the UPS shall terminate the test immediately and annunciate the appropriate alarms.
	E. Battery Circuit Breaker (BCB)
	Each UPS module shall have a properly rated isolator to isolate it from the battery. This isolator is to be housed in a separate enclosure for wall mounting, and must be installed as close as possible to the battery systems and UPS.
	2.2.3 Inverter
	The term *inverter* shall denote the equipment and controls to convert direct current (DC) from the rectifier or battery via the DC-DC booster to provide alternating current (AC) to power the load. The inverter shall be solid-state, capable of providing rated output power, and for increased performance, the inverter shall be a pulse-width-modulated design, Vector controlled and utilize insulated gate bipolar transistors (IGBTs). With this patented Vector control, switching at high frequency can achieve minimum output voltage distortion.
	A. Overload Capability
	The inverter shall be able to sustain an overload across its output terminals while supplying full rated voltage of up to 150% for 60 seconds. The inverter shall be capable of at least 200% current for short-circuit conditions including phase-to-phase, phase-to-ground and three-phase faults. After the fault is removed, the UPS shall return to normal operation without damage. If the short circuit is sustained, the load shall be transferred to the bypass source and the inverter shall disconnect automatically from the critical load bus.
	A. Output Frequency
	The inverter shall track the bypass continuously, providing the bypass source maintains a frequency of either 50Hz ±1%. The inverter shall change its frequency (slew rate) at less than 1Hz per second to maintain synchronous operation with the bypass. This shall allow make-before-break manual or automatic transfers. If the bypass fails to maintain proper frequency, the inverter shall revert to an internal oscillator, which shall be temperature compensated, and shall hold the inverter output frequency to 0.1% from the rated frequency for steady-state and transient conditions. Drift shall not exceed 0.1% during any 24-hour period. Total frequency deviation,

	including short time fluctuations and drift, shall not exceed 0.1% from the rated frequency.
	B. Phase-to-Phase Balance
	The inverter shall provide a phase-to-phase voltage displacement of no worse than ±3% with a 100% unbalanced load.
	C. Fault Sensing and Isolation
	The UPS shall be provided with a means to detect a malfunctioning inverter and isolate it from the critical load bus to prevent disturbance of the critical load voltage beyond the specified limits.
	D. Battery Protection
	The inverter shall be provided with monitoring and control circuits to protect the battery system from damage due to excessive discharge. Inverter shutdown shall be initiated when the battery voltage has reached the end of discharge voltage. The battery end-of-discharge voltage shall be calculated and automatically adjusted for partial load conditions to allow extended operation without damaging the battery. Automatic shutdown based on discharge time shall not be acceptable.
	2.2.3 Static Bypass
	When maintenance is required or when the inverter cannot maintain voltage to the load due to sustained overload or malfunction, a bypass circuit shall be provided to isolate the inverter output from the load and provide a path for power directly from an alternate AC (bypass) source. The UPS control system shall constantly monitor the availability of the inverter bypass circuit to perform a transfer. The inverter bypass circuit shall consist of a continuous duty bypass static switch and an overcurrent protection device to isolate the static bypass switch from the bypass utility source. The bypass static switch shall denote the solid-state device incorporating SCRs (silicon controlled rectifiers) that can automatically and instantaneously connect the alternate AC source to the load.
	A. Static Bypass Switch Rating
	The static bypass switch shall be rated for continuous duty operation at full rated load for highest reliability without the use of mechanical devices as used with a momentary rated device
	B. Manual Load Transfers

	A manual load transfer between the inverter output and the alternate AC source shall be initiated from the control panel. Manually initiated transfers shall be make-before-break by turnind the inverter OFF .
	C. Automatic Load Transfers
	An automatic load transfer between the inverter output and the alternate AC source shall be initiated if an overload condition is sustained for a time period in excess of the inverter output capability or due to a malfunction that would affect the output voltage. Transfers caused by overloads shall initiate an automatic retransfer of the load to the inverter only after the load has returned to a level within the rating of the inverter source and the alarm has been acknowledged..
	D. Momentary Overload
	In the event of a load current inrush or branch load circuit fault in excess of the inverter rating, the bypass static switch shall connect the alternate AC source to the load for at least 100 milliseconds, allowing up to 1000% of the normal rated output current to flow. Output voltage shall be sustained to the extent the alternate AC source capacity permits. If the overload condition is removed before the end of the 100-millisecond period, the bypass static switch shall turn Off and the load shall remain on inverter power. If the overload remains, then a transfer to the alternate AC source is to be completed.
	E. Active Eco Mode
	When selected, this mode of operation shall transfer the load to the bypass source and maintain it there as long as the bypass source frequency, slew rate and voltage are within the adjusted operating parameters. While in this mode, the inverter shall remain operating to demonstrate the ability to instantaneously assume the load without interrupting the output voltage. Should the bypass source go outside the adjusted limits, the bypass static switch shall turn Off, isolating the load from the bypass while the inverter assumes the full critical load. The load shall be transferred from the bypass source to the inverter while maintaining the output voltage within the ITIC and CBEMA curves.
	F. Back-feed Protection
	As required by IEC/EN 62040-1, the static transfer switch shall not back-feed UPS power to the bypass distribution system while the UPS is operating on battery during a bypass power outage. The purpose of this requirement is to prevent the risk of electrical shock on the distribution system when the normal source of power is disconnected or has failed. If a shorted SCR is detected, the static transfer switch shall

	be isolated by an internal automatic circuit breaker and an alarm message shall be annunciated at the UPS control panel. The load shall remain on conditioned and protected power after detection of a shorted SCR and isolation of the bypass static switch.
	2.2.3 Man-Machine Interface (MMI)
	A. UPS Display and Control Panel
	Each UPS module shall be equipped with a 320 x 240 dot graphic LCD display. This shall automatically provide all information relating to the current status of the UPS as well as being capable of displaying metered values. The display shall be menu-driven, permitting the user to easily navigate through operator screens.
	B. Logic
	UPS system logic and control programming shall reside in a microprocessor-based control system with nonvolatile flash memory. Rectifier, inverter and system control logic shall utilize high-speed digital signal processors (DSPs). CAN bus shall be used to communicate between the logic and the User Interface as well as the options. Switches, contacts and relays shall be used only to signal the logic system as to the status of mechanical devices or to signal user control inputs. Customer external signals shall be isolated from the UPS logic by relays or optical isolation.
	C. Metered Values
	A microprocessor shall control the display and memory functions of the monitoring system. All three phases of three-phase parameters shall be displayed simultaneously. All voltage and current parameters shall be monitored using true RMS measurements for accuracy to ±3% of voltage, ±5% AC current. The following parameters shall be displayed:
	• Input voltage, line-to-line
	• Input current per phase
	• Input frequency
	• Input Power factor
	• Battery voltage
	• Battery charging/discharging current
	• Output voltage, line-to-line
	• Output frequency
	• Bypass input voltage, line-to-line
	• Bypass input frequency

	• Load current
	• Load real power (kW), total and percentage
	• Load apparent power (kVA), total and percentage
	• Load percentage of capacity
	• Battery temperature, each battery string
	• Battery state of charge
	• Real time efficiency curve
	D. Power Flow Indications
	A power flow diagram shall graphically depict whether the load is being supplied from the inverter, bypass or battery and shall provide, on the same screen, the status of the following components:
	AC Input Circuit Breaker (optional)
	• Battery Circuit Breaker, each breaker connection of complete battery complement, complete disconnection and partial connection (one or more, but not all breakers open.)
	• Maintenance Bypass Status
	E. Main Display Screen
	The following UPS status messages shall be displayed:
	• Rectifier (Off / Soft Start / Main Input On / Battery Input On)
	• Input Supply (Normal Mode / Battery Mode / All Off)
	• Battery Self Test (True / False)
	• Input Disconnect (Open / Closed)
	• EPO (True / False)
	• Charger (On / Off)
	• Output Disconnect (Open / Closed)
	• Maint. Disconnect (Open / Closed)
	• Bypass Disconnect (Open / Closed)
	• Inverter (Off / Soft Start / On)
	• Bypass (Normal / Unable To Trace / Abnormal)
	• Output Supply (All Off / Bypass Mode / Inverter Mode / Output Disable)
	• Inverter On (Enable / Disable)
	F. HMI Control Buttons

	Buttons shall be provided to start and stop the inverter. A pop-up message requesting confirmation shall be displayed whenever a command is initiated that will change the status of the UPS.
	Other buttons shall be provided to reset faults and silence the alarm buzzer.
	G. Event Log
	This menu item shall display the list of events that have occurred recently while the UPS was in operation. The Event Log shall store up to 1000 events, with the oldest events being overwritten first if the log's capacity is reached.
	H. Measures Menu
	A "measures menu" shall provide access to the full set of measurements for each functional block (rectifier, bypass, booster/charger, batteries, inverter and load).
	A. Battery Status Indicator
	A battery status indicator shall display DC alarm conditions, temperature, battery state of charge, the present battery voltage, total discharge time, status of last battery test and battery time remaining during discharge.
	The UPS shall provide the operator with controls to perform the following functions:
	• Configure and manage manual battery test.
	• Modify test duration and minimum voltage
	• Start battery test
	• Monitor test status and progression
	• Stop battery test
	• Battery test status
	J. Alarms
	The following alarm messages shall be displayed:
	• Mains Voltage Abnormal
	• Mains Under voltage
	• Mains Freq. Abnormal
	• Charger Fault
	• Battery Reversed
	• No Battery
	• Parallel Comm. Fail
	• Bypass Unable To Track

	• Bypass Abnormal
	• Inverter Asynchronous
	• Fan Fault
	• Control Power Fail
	• Unit Over Load
	• System Over Load
	• Bypass Phase Reversed
	• Transfer Time-Out
	• Load Sharing Fault
	• Bypass Over Current.
	K. Controls
	System-level control functions shall be:
	• Start Inverter (and transfer to inverter)
	• Stop Inverter (after transferring to bypass)
	• Startup Screen
	• Battery Test Set point Adjustment
	• Configure Manual Battery Test
	• Initiate Manual Battery Test
	• System Settings (Time, Date, Language, LCD Brightness, Password, Audio Level)
	• Alarm Silence Command
	• Fault Reset Command
	• ECO mode
	A. Manual Procedures
	Load Transfers
	Two buttons (START INVERTER, STOP INVERTER) shall provide the means for the user to transfer the load to Bypass and back on UPS. A Sync-scope shall be provided to display the phasing between Bypass and Output in graphical representation.
	Shutdown
	Two buttons (UPS, SYSTEM) shall provide the means for the user to shut down the inverter and transfer the load to bypass or shut down the entire system.
	2.2.3 Self-Diagnostics
	A. Event Log File

	Event Log File The control system shall maintain a log of the event conditions that have occurred during system operation. Each log contains the event name, event time/date stamp, and a set/clear indicator.
	2.2.3 Remote Monitoring Capability
	A. Communication Cards
	The UPS shall be equipped with slots for optional communication card.
	· Optional additional dry contacts
	· Optional SNMP Web Cards, providing SNMP, Telnet and Web-management capability
	· Optional 485 Cards, for Modbus interfacing.
	B. Output Alarm Contacts: Dry contact outputs shall be provided for Summary Alarm, Bypass Active, Low Battery and AC Input Failure.
	C. Customer Input Contacts: The UPS shall have four discrete input contacts available for the input and display of customer-provided alarm points or to initiate a pre-assigned UPS operation. Each input can be signaled by an isolated, external, normally open contact.
	When an assembly is selected as a pre-assigned UPS operation, the following actions shall be initiated:
	• On Generator—Provides selectable choices to enable or disable battery charging, and enable or disable ECO Mode operation while on generator.
	• Transfer to Bypass—Manual command to transfer from inverter operation to static bypass operation.
	• Fast Power Off—Emergency Module Off (EPO) command to stop UPS operation.
	• Acknowledge Fault—Acknowledge a UPS alarm condition and present faults will be reset.
	• Bypass/Inverter Off—Emergency Power Off (EPO) command to stop UPS operation.
	• External Maintenance Bypass Breaker (MBB) status (open or closed)
	2.3.10 Battery Disconnect Breaker
	The battery cabinet shall have a properly rated circuit breaker to isolate it from the UPS. This breaker shall be in a separate enclosure or in a matching battery cabinet. When this breaker is open, there shall be no battery voltage in the UPS enclosure. The UPS shall be automatically disconnected from the battery by a shunt trip of the battery cabinet breaker when signaled by other control functions.

	3.0 EXECUTION
	3.1 FIELD QUALITY CONTROL
	The following inspections and test procedures shall be performed by factory-trained field service personnel during the UPS startup.
	A. Visual Inspection
	• Inspect equipment for signs of damage.
	• Verify installation per drawings supplied with installation manuals or submittal package.
	• Inspect cabinets for foreign objects.
	• Verify that neutral and ground conductors are properly sized and configured per Emerson Network Power® requirements as noted in Emerson drawings supplied with installation manuals or submittal package.
	• Inspect each battery jar for proper polarity.
	• Verify that all printed circuit boards are configured properly.
	B. Mechanical Inspection
	• Check all control wiring connections for tightness.
	• Check all power wiring connections for tightness.
	• Check all terminal screws, nuts and/or spade lugs for tightness.
	C. Electrical Inspection
	• Check all fuses for continuity.
	• Confirm input and bypass voltage and phase rotation are correct.
	• Verify control transformer connections are correct for voltages being used.
	• Ensure connection and voltage of the battery string(s).
	3.2 UNIT STARTUP
	1. Energize control power.
	2. Perform control/logic checks and adjust to meet Emerson specification.
	3. Verify DC float and equalize voltage levels.
	4. Verify DC voltage clamp and overvoltage shutdown levels.
	5. Verify battery discharge, low battery warning and low battery shutdown levels.
	6. Verify fuse monitor alarms and system shutdown.
	7. Verify inverter voltages and regulation circuits.
	8. Verify inverter/bypass sync circuits and set overlap time.

	9. Perform manual transfers and returns.
	10. Simulate utility outage at no load.
	11. Verify proper recharge.
	Input Characteristics
	Nominal Voltage
	Tolerance on voltage
	Nominal frequency(60Hz selectable)
	Tolerance on frequency
	Input Power factor @nominal voltage
	Total harmonic distortion (THDi) @ full load
	INVERTER OUTPUT CHARACTERISTICS
	Nominal voltage (380/415 selectable)
	Nominal frequency(60Hz selectable)
	Nominal Power @ 40 Deg C (kVA)
	Output Voltage Stability in steady state condition
	Stability in dynamic conditions for 100% load step variations
	Load crest factor without derating
	Output voltage distortion with 100% linear load
	Output voltage distortion with 100% non-linear load as

7.3.19 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	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. 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 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. 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.
4	**Temperature requirements** The environment inside the CCC DC shall need to be continuously maintained at 22o ± 2o 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.

5	**Relative Humidity (RH) requirements** Ambient RH levels shall need to be maintained at 50% ± 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.
6	**Temperature & Relative Humidity Recorders** 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.
7	**Air quality levels** 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.
8	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.
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	In case of aisle containment, the following points need to be adhered to: 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.

7.4 INTELLIGENT INTEGRATED INFRASTRUCTURE

7.4.1 Water Leak Detection

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 3Lines
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

viii. Water leak sensing cable shall be mechanically strong, resistant to corrosionand abrasion.

ix. It shall be constructed with two sensing wires, an alarm signalling wire and a continuity wire constructed by fluoropolymer carrier.

x. It shall have end circuit to detect open circuit fault.

c) Hooter

7.4.2 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

7.4.3 Fire Suppression System

1. Gas Based Fire Suppression System (GBFSS)

- The MSI 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 solenoid or pneumatic actuator) as the case may be, discharge pipe, non-return valveand 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 MSI 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 atotal 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 than5 days
- be efficient, effective and does not require excessive space and high pressurefor storage
- commercially available
- *Key components are valves and its accessories, actuators, flexible dischargeand 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 dischargeof the agent in less than 10 seconds into the affected zone.
- The software calculation shall be approved VdS or FM / UL. The discharge timeshall 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 forunder 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 concentrationof 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 theagent'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 areashall

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 possibleto re-fill the cylinders in India itself.
- The MSI 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 tofacilitate 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 of5m 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 orVds approved.

- The detection of smoke by such detectors shall immediately set of 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 notbe 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 hydraulicflow calculation generated by using the agent's design software. Thecalculations shall validate the fill density assumed by the MSI.
- The MSI shall submit copies of the datasheets of the hardware used in the system.
- The MSI shall also submit copy of CCE approval letter for the cylinderproposed to be used.
- The MSI shall also submit calculations to evidence the quantity of agentconsidered for the system.
- The successful vendor must submit, along with the supply invoice, a certificateof authenticity, for the agent from the system engineering company dulychecked and verified by distributor.
- The system engineering company should provide, as part of the handing over, the As built drawings and operation & maintenance manual.

7.4.4 Fire Alarm System

S. No	Minimum Required Specifications
1.	**MAIN FIRE ALARM CONTROL PANEL (FACP)** 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.

	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.
2.	**Panel Components & functions** 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. The control panel shall include the following capacities: • Support up to minimum 90 detectors & 90 devices • Support up to minimum 180 addressable points. • Support multiple digital dialers and modems The control panels shall include the following features: • Provide electronic addressing of analog/addressable devices. • Provide an operator interface control/display that shall annunciate command and control system functions. • Provide an internal audible signal with different programmable patters to distinguish between alarm, supervisory, trouble and monitor conditions. • Provide a discreet system control switch provided for reset, alarm silence, panel silence, drill switch, previous message switch, next message switch and details switch. • Provide system reports that provide detailed description of the status of system parameters for corrective action or for preventative maintenance programs. • Provide an authorized operator to perform test functions within the installed system.
3.	**Power Supply** 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. 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. 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. **Power supply for all input & output devices to be driven from main Fire Alarm Panel.**
4.	**Field Mounted System Components**
5.	**Multi-sensor Photo Thermal Detector:** 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 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: • 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. • 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. • Activate automatic smoke control sequences. • All automatic events programmed to the alarm point shall be executed and the associated outputs activated. • All stairwell/exit doors shall unlock throughout the building. • All self-closing fire/smoke doors held open shall be released.
13.	Installation: All conduiting / wiring /Trays /channels /trenches /pipes etc. for completion of Job
14.	Warranty: 5 Years Comprehensive onsite OEM Warranty

7.4.5 Diesel Genset

S. No	Specifications
1.	**Scope of Supply** The scope covers supply of Diesel Generator set of stationary type having rated capacity of 125 KVA each at CCC specified site conditions of 40^{o} C ambient temperature and 100% relative humidity on FOR site basis. 2 No's of 125 KVA DG set shall be connected in N+1 Configuration to support the Command & Control Centre IT load and cooling units. In case primary DG set unable to start in power fail condition other DG set shall be automatically start in stipulated time. The engine should comply with the latest CPCB Norms of the country and equipped with: - Diesel engine complete with all accessories - An alternator directly coupled to the engine through coupling, complete with all accessories. - Automatic voltage regulator - Complete starting arrangement, including two nos. batteries & chargers - Base frame, foundation bolts etc - Engine Cooling and lubrication system - Engine air filtering system. - Exhaust silencer package with insulation and Aluminium cladding with all structural requirements to install - Set of GI pipes, valves, trainers, unloading hose pipes as required for fuel transfer system from storage area to fuel tank including electrically driven fuel pump as

	per site requirement - All lubricants, consumable, touch up paints etc. for first filing, testing & commissioning at site. The fuel oil for initial commissioning will also be provided by the contractor for continuous running on full load for 8 hours - AMF panel for control, metering and alarm - Enclosure for silent type D.G. Set
2.	**SCOPE OF SERVICE**. The Contractor shall provide following services: 1. Design manufacture, shop testing including assembly test 2. Dispatch, transportation to site 3. Erection, testing & commissioning with all equipment's/material required for the purpose 4. Drawings, data, design calculations and printed erection, operation & maintenance manual. **5.** Certification and compliance for meeting noise level & emission parameters and other requirements in accordance with latest Notification of MOEF.
3.	**TECHNICAL REQUIREMENT**: The rating of DG sets is as follows: DG set net output after considering duration for engine and alternator separately due to temperature rise in side the enclosure and on account of power reduction due to auxiliaries shall be 125 kVA, 1500RPM, 0.8Pf, 415V, 3 Phase, 50Hz. The above rating is the minimum requirements. DG sets shall also be rated for 130% of full load for 1 hour in every twelve hours of continuous running. The output voltage, frequency and limits of variation from open circuit to full load shall be as follows: Voltage variation ± 5% of the test value. Frequency 50Hz ± 2% The Diesel Generator and other auxiliary motor shall be of H class with temperature rise limited to Class-F for temperature rise consideration.
4.	Noise Level & Emission Parameters: These shall be as per latest Notification of MOEF.
5.	PLANT DESIGN Diesel Engine The engine shall comply with the IS 10002/BS 5514/ISO 3046: latest edition. a. Diesel engine shall be turbo charged multi cylinder V-type/in line type with mechanical fuel injection system. b. The engine with all accessories shall be enclosed in an enclosure to make it work silently (with permissible noise level) without any degradation in its performance. c. The fuel used shall be High Speed Diesel oil (HSD) or Light Diesel Oil (LDO) as

	per IS: 1460.
6.	Air Suction & Filtration Suction of air shall be from in-door for ventilation and exhaust flue gasses will be let out to outside atmosphere, Condensate traps shall be provided on the exhaust pipe. Filter shall be dry type air filter with replaceable elements. Fuel tank capacity should be sufficient to run for 12 hrs. Continuous with full load as specified.
7.	**AVM PADS:** One set of AVM pads are included and built along with the base frame - Mounts are spring type and 99% efficient, suitable for gen set application. These mounts are placed between the engine - alternator and the base frame
8.	**FUEL AND LUBRICATING OIL SYSTEM.** The engine shall have closed loop lubricating system. No moving parts shall require lubrication by hand prior to the start of engine or while it is in operation.
9.	**ENGINE STARTING SYSTEM.** Automatic electric starting by DC starter motor shall be provided.
10.	**FUEL INJECTION AND REGULATOR** The engine shall be fitted with electronic/mechanical governor suitable for class A- 1 as per IS 10000. The engine shall be fitted with a heavy, dynamically balanced fly wheel suitable for constant speed governor duty.
11.	**ALTERNATOR:** The alternator shall be of continuously rated duty, suitable for 415 V, 3 phases, 50Hz, 125 KVA for full block load power development having brush-less, synchronous, self-excited, self-regulating system. The alternator shall be drip-proof, screen protected as per IP-23 degree of protection. The rotor shall be dynamically balanced to minimize vibration. The alternator shall be fitted with shaft mounted centrifugal fan. It shall have the winding of class H but limited to Class-F for temperature rise consideration. The Alternator regulatory shall be directly coupled to the engine and shall be complete with the excitation system, automatic voltage regulation of +/- 1%, voltage adjusting potentiometer and under/ over speed protection.
12.	**Terminal Box:** Terminals shall be suitable for two runs of 3½ Core 185 mm2 Aluminium cable for 125 KVA DG set. The neutral shall be formed in AMF panel. The generator terminal box shall be suitable to house necessary cables. Minimum two (2) no's of earthing terminals are to be provided for neutral in the terminal box in addition to the regular earthing points of the generator body. The alternator with all accessories shall be enclosed in an enclosure to make it work silently (within permissible noise level).

13.	**COUPLING:** The engine and alternator shall be directly coupled by means of self- alignment flexible flange coupling to avoid misalignment. The coupling shall be provided with a protecting guard to avoid accidental contact.
14.	**MOUNTING ARRANGEMENT**: The engine and alternator shall be mounted on a common heavy duty, rigid fabricated steel base frame constructed from ISMC of suitable sections. Adequate number of anti-vibration mounting pads shall be fixed on the common base frame on which the engine and the alternator shall be mounted to isolate the vibration from passing on to the common base frame or the foundation of the D.G. Set.
15.	PERIPHERALS **BATTERY AND BATTERY CHARGER**: Two nos. 12/24V batteries or as required for starting, complete with all leads, terminals and stand shall be provided. Each battery shall have sufficient capacity to give min. 6 nos. successive starting impulse to the diesel engine. Each battery shall have its own charger unit. The battery charger shall be complete with transfer, suitable rating (415 V, 3 Ph., 50 Hz. / 230V, 1 Ph., 50Hz) rectifier circuit, charge rate selector switch for "trickle" / boost' charge, D.C. ammeter & voltmeter, annunciation panel for batter charge indication/ loading/ failure. The charger shall float and Boost Charge the battery as per recommendation of manufacturer of battery. The charger shall be able to charge a fully discharged battery to a state of full charge in 8 Hrs. with 25% spare capacity. Manual control for coarse and fine voltage variation shall be provided. Float charger shall have built-in load limiting feature. Ripple shall not be more than 1% (r m s) to get smooth DC voltage. Charger shall be provided with out-put Voltmeter & Ammeter. Changeover scheme for selecting battery and battery charger by changeover switch should be provided.
16.	CONTROL AND INSTRUMENTATION: Each D.G. Set shall be provided with suitable instruments, interlock and protection arrangement, suitable annunciation and indications etc. for proper start up, control, monitoring and safe operation of the unit. One local AMF control panel along with each D.C. set shall be provided by the Supplier to accommodate these instruments, protective relays, indication lamps etc. The AMF Panel shall have IP-52 degree of Protection as per IS: 12063. The D.G. sets shall be provided with automatic start facility to make it possible to take full load within 30 seconds of Power Supply failure. Testing facility for automatic operation of D.G. Set shall be provided in AMF panel. A three attempt starting facility using two impulse timers and summation timer for engine shall be provided and if the voltage fails to develop within 40 sec., from receiving the first impulse, the set shall block and alarm to this effect shall be provided in the AMF

	panel. Following instruments shall be provided with Diesel Engine. a. Lube oil pressure gauge b. Water temperature thermometers. c. Engine tachometer/HR d. Any other instruments necessary for DG set operation shall be provided. DG Set in N+1 configuration shall be capable of being started/ stopped manually from remote as well as local. (Remote START/STOP push button shall be provided in 415V ACDB). However, interlock shall be provided to prevent shutting down operation as long as D.G. Circuit breaker is closed. The diesel generator shall commence a shutdown sequence whenever any of the following conditions appear in the system. a) Over-speed b) Over load c) High temperature of engine and cooling water. d) High temperature inside enclosure. e) Low lube oil pressure f) Generator differential protection. g) Short circuit protection. h) Under voltage i) Over voltage. Following indication lamps for purposes mentioned as under shall be provided in AMF panel. Pilot indicating lamp for the following: a) Mains ON b) Alternator ON c) Charger ON/OFF d) Breaker ON/OFF e) Main LT Supply ON/OFF Thermostatically controlled space heaters and cubicle illumination operated by Door Switch shall be provided in AMF panel. Necessary isolating switches and fuses shall also be provided. AMF panel shall have facility for adjustment of speed and voltage including fine adjustments in remote as well as in local mode.
17.	**D.G. SET Enclosure** **General requirement** Diesel engine, alternator, AMF panel, Batteries and Chargers shall be installed outdoor in a suitable weather-proof enclosure which shall be provided for protection from rain,

	sun, dust etc. Further, in addition to the weather proofing, acoustic enclosures shall also be provided such that the noise level of acoustic enclosure DG set shall meet the requirement of MOEF. The diesel generator sets should also conform to Environment (Protection) Rules 1986 as amended. An exhaust fan with louvers shall be installed in the enclosure for temperature control inside the enclosure. The enclosure shall allow sufficient ventilation to the enclosed D.G. Set so that the body temperature is limited to 58^{O}C during maximum ambient temperature of 50^{O}C & full load. The air flow of the exhaust fan shall be from inside to the outside the shelter. The exhaust fan shall be powered from the DG set supply output so that it starts with the starting of the DG set and stops with the stopping of the DG set. The enclosure shall have suitable viewing glass to view the local parameters on the engine. Fresh air intake for the Engine shall be available abundantly; without making the Engine to gasp for air intake. A chicken mesh shall be provided for air inlet at suitable location in the enclosure. The Enclosure shall be designed and the layout of the equipment in side it shall be such that there is easy access to all the serviceable parts. Engine and Alternator used inside the Enclosure shall carry their manufacturer's Warranty for their respective Models and this shall not degrade their performance. Exhaust from the Engine shall be let off through silencer arrangement to keep the noise level within desired limits. Interconnection between silencer and engine should be through stainless steel pipe. All the Controls for Operation of the D.G. Set shall be easily accessible. There should be provision for emergency shutdown from outside the enclosure. Arrangement shall be made for housing the Battery set in a tray inside the Enclosure.
18.	**Constructional Features:** The enclosure shall be fabricated from at least 14 Gauge CRCA sheet steel and of Modular construction for easy assembling and dismantling. The sheet metal components shall be pre-treated by Seven Tank Process and Powder coated (PURO Polyester based) both-inside and outside for long life. The hard-ware and accessories shall be high tensile grade. Enclosure shall be given a lasting anti-rust treatment and finished with pleasant environment friendly paint. All the hardware and fixtures shall

	be rust proof and able to withstand the weather conditions. Doors shall be large sized for easy access and provided with long lasting gasket to make the enclosure sound proof. All the door handles shall be lockable type. There should be provision for separate additional locking facility with the normal door lock. The Enclosure shall be provided with anti-vibration pads (suitable for the loads and vibration they are required to carry) with minimum vibration transmitted to the surface the set is resting on. High quality Acoustic foam/rock wool of required density and thickness shall be used with fire retardant thermo-setting resin to make the Enclosure sound proof. Provision for Neutral / Body Earthing at two (2) points. Points shall be available at two side of the enclosure with the help of flexible copper wires from alternator neutral, and electrical panel body respectively. The earthing point shall be isolated through insulator mounted on enclosure.
19.	**INTALLATION ARRANGEMENT** DG set enclosed in enclosure shall be installed on Concrete Pedestal 300 mm above FGL. The construction of required platform with GI angle iron on cornice of platform as required according to the weight of DG set is in the scope of bidder.
20.	**DOCUMENTS** Following drawings and data sheet shall be submitted for approval during implementation phase: (i) DG Set test certificate (ii) GA drawing of DG set (iii) Layout of DG set in the enclosure along with sections. (iv) GA and SLD of AMF panel. (v) Arrangement of inclined roof and pedestal. (vi) The detailed construction drawing of DG set Platform The DG Set shall be supplied with (i) DG Set test certificate (ii) Engine Operation & maintenance Manual. (iii) Engine PARTS Catalogue. (iv) Alternator Operation, maintenance & Spare parts Manual. (v) Alternator test certificate.
21.	**TESTS:** The Diesel generator sets shall be tested for routing and acceptance tests as per the relevant IS/IEC standards.

	The type test report for diesel engine and alternator are required to be submitted as per relevant standard shall be submitted for purchaser's approval.
22.	Warranty: 5 Years Comprehensive onsite OEM Warranty
23.	**Preferred Engine make:** Cummins /Kirloskar /Volvo **Preferred Alternator make:** Stamford/ Kirloskar/Parkinson

7.4.6 Link Load Balancer

Sr No.	Minimum Technical Specification
1	The proposed dedicated Hardware device should support minimum 20 WAN links for inbound/outbound traffic load balancing & redundancy. WAN Links must support IPv4 or IPv6 addressing or both simultaneously. Proposed device should be next generation Hyperconverged multi- tenanted Network Function Appliance with support upto 16 virtual instances. Should have internal redundant Power supply with 2 TB usable hard disk, 64 GB RAM and have capability to host 3rd party and open source virtual network Functions like WAN Optimization, DNS etc.on the same appliance
2	Appliance should support minimum 4 x 10GB SFP+ ports
3	The solution should support Static NAT, port based NAT and advanced NAT for transparent use of multiple WAN/ Internet links. Should support inbound load balancing and persistency features including RTS (return to sender) and IPFlow persistency.
4	Should support minimum 2 Million concurrent connections & 500,000 Connections per second
5	Traffic load balancing using e-Policies should support algorithms including round robin, least connections, shortest response, persistence ip, hash ip, hash ip and port, consistent hash IP and SNMP
6	The solution should support user-defined IP and Service Group functions for configuring firewall, bandwidth management and routing policies.
7	Should support XML-RPC for integration with 3rd party management and monitoring. Should also support SAA, SAML, Hardware binding and AAA support along with SSO. Solution must support machine authentication based on combination of HDD ID, CPU info and OS related parameters i.e. mac address to provide secure access to corporate resources.

8	The solution should support Multi-homing function for inbound IPv4 and/or IPv6 traffic Load Balancing and fault tolerance across up to 20 WAN links by enabling DNS relay or DNS authoritative server function.
9	Should have IPV6 support with IPv6 to IP4 and IPv4 to IPv6 translation and full IPv6 support. Also should have IPV6 support with DNS 6 to DNS 4 & DNS 4 to DNS 6 translation based health check for intelligent traffic routing and failover
10	The solution should support DHCP and DHCPv6 server function
11	The Should provide comprehensive and reliable support for high availability with Active- active & active standby unit redundancy mode. Should support both device level and VA level High availability
12	The proposed solution should have capability to support data deplucation and byte level caching on the same appliance for better WAN optimization
13	The solution should provide comprehensive and reliable support for high availability and N+1 clustering through standard VRRP on Per VIP based Active-active & active standby unit redundancy mode.
14	OEM should have direct presence in India since last 5 years and have 24 x 7 TAC in India

7.4.7 Backup Appliance with Backup Software

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 and VTL backup simultaneously via NFS v3, CIFS, FC , OST and 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 150 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 availbility 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 and min. one hot spare disk as well.
9	Proposed appliance should support different retentions for primary and DR backup storage and should support instant copy creation on remote site for better DR readiness with support for transmittimg only deduplicated unique data in encrypted format to remote sites.
10	Proposed appliance should support retention lock (WORM) feature which ensures that no data is deleted accidently 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 256 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.

7.4.8 DLP (Data Leakage Prevention)

S. No.	DLP design and architecture

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.

6.5 ICT SOFTWARE COMPONENTS FOR DATA CENTER

7.4.9 HIPS

S.No.	Minimum Specifications
	Make
	Model
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
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

S.No.	Minimum Specifications
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

7.4.10 Facial Recognition System

Sr. No	Key	ITEM DESCRIPTION
1.	**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, UAV/Drones etc.
2.	**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 application for various purposes for non- voluntary face detection & recognition in the open crowded scenarios.
3.	**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.
4.	**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.

5.	**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. FRS shall be able to process uploaded pre-recorded video feeds with a speed of up to X20, depending on the proposed hosting hardware and the video quality
6.	**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, scars, tattoos etc. for future searches.
7.	**Support for cameras/video formats**	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 and PTZ Cameras with IR Illuminators without any special configurations required
8.	**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.
9.	**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.
10.	**Image Format support**	The system shall be able to utilize any of the file formats like JPEG, PNG, BMP, TIFF etc. format for enrolment.
11.	**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 2 sec.

12.	**Enrolment of faces**	The system shall have option to automatically enroll face images from CCTV cameras/video source. This functionality should also be provided through the Video Intelligence platform in addition to the FRS application. 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.
13.	**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.
14.	**Full HD Support**	The system shall be able to work on full HD Camera video with maximum performance.
15.	**Implementation**	The system shall be able to be implemented on IT hardware like Server or Workstation.
16.	**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
17.	**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.
18.	**Algorithm Benchmarking**	The Vendor should have any performance benchmarking certificate. NIST certificate will be preferred.
19.	**Performance**	The system must perform a full 1: N search of the probe image in under 5 seconds against a database of up to 50 mn face records.

20.	**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.
21.	**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
22.	**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 2 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
23.	**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
24.	**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.

25.	**OEM owned algorithm**	The FRS OEM should have ownership of Face Recognition Engine /Algorithm for any custom specific development as required by client
26.	**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.
27.	**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.
28.	**Video Alert**	FRS shall be able to play a short video clip of the moment of face detection without dependency on VMS which can be downloaded/exported/saved for evidence proof
29.	**Timeline of detections**	FRS shall provide timeline sequence of all detections of subject with date, time & location.
30.	**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.
31.	**Minimum hardware support**	FRS Application Engine must be able to run a minimum of 20 FRS Camera Channels per Server. (Server with 128 GB RAM, 3 NVIDIA Tesla T4 card with 40 cores.) Other optimized and better sizing shall be accepted.
32.	**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.

Face Recognition System KPI Criteria/Evaluation Parameters:

Sr. No.	Aspect
1	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 recorded video 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.
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

7.4.11 Virtualization Software

SL No	Feature	Specifications
1	**Bare Metal Solution**	Sits directly on the bare metal server hardware with no dependence on a general-purpose OS for greater reliability & security and should be Leaders in the Gartner's Magic Quadrant latest available.
2	**Guest OS Support**	Windows client, Windows Server, Linux (at least Red Hat, SUSE, Ubuntu and CentOS, Solaris x86) etc. OS vendor should provide certification and support for hypervisor.
3	**Live Migration**	Live Virtual Machine migration between different generations of CPUs in the same cluster and without the need for shared storage option and long distances from one site to another with no disruption to users or loss of services, eliminating the need to schedule application downtime or business downtime.
4		Live migration of VM disk from one storage array to another without any VM downtime. Support this migration from one storage protocol to another eg: FC, NFS, iSCSI, DAS.
5	**Availability**	Proactive High availability capability that utilizes server health information and migrates VMs from degraded hosts before problem occurs, should optimize power consumption by turning off hosts during the reduced demand
6		Migration of VMs in case one server fails all the Virtual machines running on that server shall be able to migrate to another physical server running same virtualization software.
7		It should support affinity and anti affinity rules to set constraints that restrict placement of a virtual machine to a subset of hosts in a cluster and to keep virtual machines paired or separated.
8		Zero downtime, Zero data loss and continuous availability for the applications running in virtual machines in the event of physical host failure, without the cost and complexity of traditional hardware or software clustering solutions.
9	**Performance**	Add CPU, Memory & devices to virtual machines on the fly when needed, without disruption or downtime of working VMs for both windows and Linux based VMs.

10		Create a cluster out of multiple storage datastores and automate load balancing by using storage characteristics to determine the best place for a virtual machine's data to reside, both when it is created and when it is used over time.
11		Support for persistent memory, exposing it as block storage or as memory, to enhance performance for new as well as existing apps
12		Should be able to dynamically allocate and balance computing capacity across collections of hardware resources aggregated into one unified resource pool with optional control over movement of virtual machines like restricting VMs to run on selected physical hosts.
		The Solution should offer virtual load balancers with L4–L7 load balancer with SSL offload and pass-through, server health checks .
13		Should support network and storage QoS to ensure perfromance on per VM basis
16	**Storage support**	Support boot from iSCSI, FCoE, and Fibre Channel SAN. Integration with Storage API's providing integration with supported third-party data protection, multi-pathing and disk array solutions. Solution software should allow common management across storage tiers and dynamic storage class of service automation via a policy-driven control plane
17	**Management**	The solution should offer converged visibility and analytics that tie together compute, network, storage and security and provide Physical to Virtual Correlation and troubleshooting, report the amount of East-West, North-South, Internet, virtual machine to virtual machine, virtual machine to physical traffic within the datacentre
		The solution should offer comprehensive flow assessment and analytics and security groups and firewall rules suggestion for the purpose of implementing a zero trust security within the data-center, provide a converged view of virtual and physical network, provide end to end topological view of path between two virtual machines. It should support leading hardware vendors as well.
17	**Virtual Switch**	Span across a virtual datacenter and multiple hosts should be able to connect to it. This will simplify and enhance virtual-machine networking in virtualized environments and enables those environments to use third-party distributed virtual switches.

		The solution should be capable to of multisite networking (Layer 2 extension) irrespective of underlying physical topology for active active DC & DR purposes, container network and security for container to container L3 networking and micro segmentation for microservices etc
		The solution should support reduction in Recovery Time Objective when the VMs are brought up from DC to DR, without the need to redo the IP-addresses, the default gateway router should be stretched across datacentres, also the firewall policy should also be applied across DC & DR automatically, so that when Virtual Machines move from DC to DR there is no need to reconfigure the firewall policies
18		In-built enhanced host-level packet capture tool which will provide functionalities like SPAN, RSPAN, ERSPAN and will capture traffic at uplink, virtual switch port and virtual NIC level. It should also be able to capture dropped packets and trace the path of a packet with time stamp details.
		The Solution should provide distributed routing (OSPF & BGP), VXLAN based logical virtual switching, NAT function, server load balancer, Software L2 bridging to physical environments, L2 & L3 VPN, , site-to-site IPSEC VPN services, distributed L2-L4 stateful firewall at vNIC level
19	**VM based Replication**	Efficient array-agnostic replication of virtual machine data over the LAN or WAN. This Replication should simplify management enabling replication at the virtual machine level and enabling RPOs as low as 15 minutes.
20	**Disaster Recovery Automation**	Solution should provide DR automation solution delivered from virtualization manager console for automated failover, failback and recovery of application VMs in proper sequence to other data center with single click
21		Solution should provide solution to perform non-disruptive DR drill/testing of recovery plan for full and selected applications every six months without impacting production applications running in primary environment.

7.4.12 Enterprise Management system/Help Desk Management

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: • 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.	The proposed solution must be featured in Gartner/IDC reports. Documentary proof must be provided at the time of submission.
4.	There should be a tight integration between infrastructure metrics and logs to have the single consolidated console of Infrastructure & security events.
5.	Consolidate IT event management activities into a single operations bridge that allows operator quickly identify the cause of the IT incident, reduces duplication of effort and decreases the time it takes to rectify IT issues.
6.	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.
7.	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

8.	The solution shall provide future scalability of the whole system without major architectural changes.
9.	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.
10.	All the required modules should be from same OEM and should be tightly integrated for single pane of glass view of enterprise monitoring
11.	The solution must provide single integrated dashboard to provide line of business views and drill down capabilities to navigate technical operators right from services to last infrastructure components
12.	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.
13.	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
14.	Proposed NMS solution must have deployment reference of monitoring & managing 2500+ network nodes in at least 3 deployments across Gov/PSU/Large Enterprise.
15.	The Solution should provide all the modules as a single monitoring engine to correlate events in real-time from Networks, Servers and Applications
16.	The solution should be virtual appliance and deployable on Linux operating systems to reduce the overall TCO
17.	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
18.	The solution should provide High Availability (HA) at datacenter site
19.	The solution should have inbuilt role-based access module to enable multiple users with different groups to create dashboards specific to their department
20.	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.
21.	Calculates availability for clients, servers and ANPR/access/video units for efficient SLA management
22.	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 collected 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 co-ordinated 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 ed 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 offend-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: • 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 events 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, problems 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 event 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 connectors 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 logs 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: • 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 VERIFY 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 stores 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 most 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 services 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.
	Infrastructure cabling and connection monitoring
1.	The solution should be capable of tracking device history for networked end devices including the following forensics details:
2.	When device was first connected to the network
3.	If and when it was removed from the network
4.	If and when it was moved from one physical location to another
5.	How long it has been active or inactive.
6.	Asset, configuration and change management
7.	The solution should be fully complying with ANSI/TIA 606-B (including B-1) and ISO/IEC 18598 standards.
8.	The solution should deliver physical connectivity information to the management software.
9.	The solution should be a complete Real Time Interconnect Solution and should provide alerts for:
10.	Patch cord connections or disconnections from the patch panel.
11.	Patch cord connections or disconnections from the switch.
12.	Inter-changing of patch cords at the switch side.
13.	Inter-changing of patch cords at the panel side.
14.	There should use of DAC/ Multi-mode cables to ensure maximum possible reduction in latency parameters.
15.	These alerts should be patching connection or disconnection alerts. These should show exact information about the panel port or switch port which got disconnected or connected and end to end link information.
16.	The Physical Layer Management solution should be strictly based on the physical detection of patch cord connectivity.
17.	The solution should provide the capability of electronically tagging any network equipment such as network printer, servers, IP Camera, desktop, switches, modems, etc.
18.	The system should be robust and should report the patching connectivity information as complete ONLY when the two ends of the same patch cords are connected and should not get confused by any subsequent insertion of any other patch cord.

19.	The solution should provide the technician an easy method of patching with- out imposing any specific sequence rules/order for the patching, thus allowing the technician to carry patching work orders as in the case of a non-intelligent solution.
20.	Patch cord removal from Panel / Switch side should be monitored and alerts like email/SMS should be sent if any end of the patch cord is removed.
21.	The solution should provide the capability to automatically connecting to a remote database sites as well as to a local database.
22.	The solution shall be able to maintain a record of the rack capacity and utilization including:
23.	Total rack space and occupied rack space
24.	Total number of available intelligent panel ports
25.	Total number of non-intelligent panel ports
26.	Total number of switch ports and “switch utilization”
27.	Total number of PDU power outlets (if installed at site)
28.	Total number of environmental sensors (if installed at site)
29.	The solution should be able to monitor on-line of patch cord removal from either side:
30.	Between intelligent panels
31.	Between intelligent panel to active device like Switch.
32.	The solution should have the following visual indications:
33.	LED above each port - indicating patching, patching work order pending and correcting bilking mode in case of patching mistake.
34.	LED per each patching frame – indicating panel status.
35.	Sound – in case of patching or removal of a cord between either intelligent panels or between intelligent panels to a switch.
36.	All Changes of the telecommunications infrastructure facilities and networked devices should be maintained within the intelligent infrastructure management system to keep track of current activities and completed activities including:
37.	Real time tracking of authorized and unauthorized patching activities
38.	Generation of move, add, change work orders
39.	Providing means for retrieval of work orders at racks with intelligent equipment using port LEDs, tablet, etc.
40.	Automated tracking of work order completion
41.	Scheduled work order and work order history
42.	Monitoring and alerting on connected information

43.	The Intelligent Physical Layer Management Solution should have guidance lights per port. The light guidance is mandatory for tracing the two ends of any patch cord, executing planned work orders and for remote management.
44.	The lights per port on the panels should be powered from the scanning devices and should not require a separate power supply.
45.	The intelligent panels should have the necessary intelligent hardware and light indicators integrated within the panels. Retrofits are not an option.
46.	The panels should be passive and the panels should not require any power for operation of the intelligent management solution.
47.	The Intelligent Physical Layer Management solution should be scalable and the design should enable maximum usage of its components e.g. scanning devices, by sharing of same components over multiple racks when required.
48.	The solution should be simple, effective and as automated as possible requiring minimum human intervention. For e.g. for executing work orders the solution should depend on light guidance only without need for reading instructions from any media/display.
49.	The solution should provide patching information based only on physical connectivity information and not thorough any other way.
50.	The solution should be web based and not require any clients to be installed on end devices. All features should be available through this web explorer only.
51.	All scanning devices monitoring the intelligent panels should be 1U only to allow maximum usage of rack space. Also they should have the capability to be shared among more racks.
52.	The scanning devices should automatically detect the panel type; the scanning devices are connected to, and should also automatically detect the connectivity between the scanning devices. This is necessary for automatic & error free real time detection & installation of hardware components in the software.
53.	The solution should offer flexibility to extend the panel scanning capability to distances more than 100 feet (one rack) in order to cover multiple racks.
54.	Since all the upper & center units of the rack (critical real estate space in rack) will be required to mount panels or switches to provide a hassle free environment for their control and installation, the scanning devices would be mounted either at the top or bottom of the rack. Hence it is important that the scanning devices should carry a design such that they require minimum interaction during any work order execution and do not force any change in the rack design to enable their functioning.

55.	The solution should be efficient and should not require use of multiple media for providing or verifying of the same information or carrying out a work order. Any work order execution should be achieved by means of lights without requiring any other interface. This is essential to ensure easy usage of the system.
56.	The solution should provide an easy way for tracing panel port connectivity information even at the rack level without directly interacting with any panel port / software. This is important to provide information during network outage.
57.	The implementation of the intelligent solution should not hamper or should not be hampered by the progress in the other cabling, patching & active installation. The solution should be capable to be installed at any time during the network installation and testing.
58.	The solution should provide the capability of monitoring port availability status on network equipment including switches, patch panels and telecommunication outlets should be monitored in real time for the purpose of detecting unexpected or unauthorized activities.
59.	The intelligent management software should use standard database so that the solution should be able to communicate and exchange data with other systems using standard protocols and database formats. This is to provide easy integration and customised reporting to other systems. Integration can be done via: SDK, SNMP traps, XML, database sharing and web services.
60.	Server provisioning feature should be supported and built in the solution at the time of implementation. For this the solution should be ready and should not require to build integration module to integrate to IP power strips to get information of the power being consumed in the racks in real time.
61.	The solution should be ready to connect to devices which control various parameters in the Datacenter / Hub room environment (temperature sensors, humidity sensors, door access sensors, etc.) and provide this information to the software in real time and help in server provisioning.
62.	The system should provide Servers Health like the real time power being consumed by a server and information like ambient temperature inside the servers ,by an out of band access or network method without additional requirement of sensors or hardware.
63.	The solution should offer as a built in feature the possibility to report any unauthorized MAC outside the white list of MACs allowed on the site.

64.	The solution should be capable to block switch ports automatically on intrusion detection. This capability however should be selectable by the user depending on the critical nature of the location.
65.	The solution should provide visual representation of the datacenter environment for:
66.	Power consumption
67.	Space availability
68.	Temperature, humidity and other related environment sensor information.
69.	The solution should have inbuilt dashboard. The solution should offer users to customize their own dashboard like switch utilization, panel utilization etc.
70.	The solution should be provided with an unlimited user licenses. This is important to enable use by multiple users.
71.	The single scanning hardware unit should be able to connect to panels in multiple Racks.
72.	The work order execution should be achieved by LEDs on panel ports. No other interface should be required for execution of the work order.
73.	The solution connectivity, between the different scanning appliances, should be based on standard RJ-45.
74.	The solution should have built in reports for all physical layer monitoring, and also for data center operations like power consumption, temperatures, rack status and various other sensors information.
75.	The intelligent solution must offer all copper and fiber options (RJ-45, LC, and MPO/MTP)
76.	The solution should support tablet/smart phone in order to present the work orders.
77.	It should have the ability to connect and provide datacenter environment reports like power consumption in racks in real time, temperatures within racks, rack door closures, water level sensing etc.
78.	All Copper & Fiber components should be from the same OEM vendor.
79.	All Components Passive and active Components should be RoHS (Restriction of Certain Hazardous Substances) complied.
80.	Declaration –RoHS Compliant should clearly be mentioned on datasheets of each Passive Components (Copper & Fiber).
81.	FRLS cables to be used for power related connections.
82.	There should be 15-year performance warranty and Application Assurance

Helpdesk management

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

7.4.13 ICCC core application (HA)/ICCC Software

S. No	Technical Specification
A	**General**
1.	The Unified Command & Control Platform (UC&C) shall be an enterprise class IP-enabled Cloud ready application. 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 edge devices.
2.	The platform must be Cloud ready from day 1 and must have the ability to host either in total or some of the modules in a private cloud environment approved by Meity.
3.	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 blueprints, images, streaming camera 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):**
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	The GIS MAP shall offer a smart selection tool to access the video. By clicking the location, the user wants to see, the GIS MAP will automatically select the cameras that can see this location and move the PTZ towards that location. This smart selection tool shall take obstacles into consideration and not display cameras that cannot see the location because of a wall.
8	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.
9	The user shall be able to select and display the content of multiple UC&C entities on the map in popup windows.
10	The GIS MAP shall provide the following search capabilities:
11	Search within the map by entity name, street name, or point of interest.
12	Drag and drop entities from the UC&C to the map to center their location.
13	Map to support event-based response actions for decision making in case of any emergency / critical situation
15	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: 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	An incident shall be the holistic description of the situation and support the following attributes: Visual: • Colour • Icon. Incident management shall provide the ability to customize incident types using a set of imported icons. Sound Incident category. Incident category shall allow an operator to organize incident types in a logical tree The location can be an entity (camera, door, zone, area) or a geographical coordinate. A priority level A description States Standard operating procedures. History of activities. Attach Entities. Entities related to the source of events triggering the incident shall be automatically associated to the incident. Attached documents. Documents and URLs providing more information or guidance on the incident and its management.
12	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	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: 1. 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. 2. History of the incident including: a. All events related to the incident

	b. System workflow activities c. Operator actions for the incident d. Comments about the incident
16	Operators shall be able to perform the following actions: 1. Change the incident state. 2. Forward the incident. 3. Transfer the incident. 4. Edit the incident: a. Change the description b. Change the priority level c. Release the ownership 5. Attach additional entities to the incident. 6. Link related incidents. 7. 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: 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&Cfor 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: a. HTML b. PDF c. XML d. Custom format
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: 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	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) a. Crimes - Using historical crime data, determining when certain areas will be more vulnerable, identifying geographical features. b. Offenders - Criminal groups, Criminal profiles, juvenile offenders likely to become major criminals. c. Perpetrator identities - Patterns in crimes done by the offender, profiling the kind of weaponry he keeps d. Point in time Analysis on areas like resource invested Vs Crimes going down in specific areas / Police Area Offices, Railway Offices, SP-Officess. e. Crime victims - Identifying groups likely to be hurt (religious targets), people at risk of domestic violence, etc. f. 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.
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.
5	Video-specific reports (archive, bookmark, motion, and more).
6	Configuration reports
7	ALPR-specific reports (mobile ALPR playback, hits, plate reads, reads/hits per day, reads/hits per ALPR zone, and more).
8	System Health activity and health statistics reports for proactive maintenance.
9	Generic Reports, Custom Reports and Report Templates

10	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.
	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.
H	**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.
H	**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:
	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.
	View audit trails that show a history of user/administrator changes to an entity.
6	Common entities such as users, schedules, alarms and many more, can be reused by all embedded systems in platform.
7	The application must have single user unified interface for configurations of all the systems of Video, ANPR and Emergency response.
8	There should not be any limitation on the number of end client licenses for the UC & C application.
I	**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.
J	**Mobile app Functionalities:**

1	Ability to logon/logoff the UPS using an authorized use profile of the system. Ability to change the picture or the password of the user of the mobile app. 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. Ability to view below minimum edge devices Unified with the UC&C platform: Cameras ii. ALPR cameras GIS and Offline Maps Iv. Ability to navigate the system hierarchical view of the edge devices & entities with ability to search entities in the system.
2	It shall be possible to download the mobile apps from the Central application store (Apple iTunes App Store,/Google Play,/Windows Store).
K	**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- ailures.
3	Health events shall be accessible via the SDK (can be used to create SNMP traps with external EMS / NMS systems).
L	**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.

M	**Third Party System Unification:**
1	Directory service like MS – AD 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: Software Development Kits (SDKs), Driver Development Kits (DDKs), REST-based Web Service SDK and RTSP Service SDKs.
3	A UC&C SDK shall be available to support custom development for the platform.
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 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.
N	**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.

7.4.14 Automatic Vehicle Location System (AVLS)

Sr. No.	Technical Specification
1.	The AVL shall be seamlessly embedded with ICCC.
2.	The AVL shall be able to receive GPS information from NEMA compliant GPS systems and have the flexibility to add manufacturer-specific protocols.
3.	The AVL shall be able to receive real-time or historical information and perform data fusion to build a complete time-accurate location database of each unit.
4.	The AVL shall associate the GPS unit to an AVL entity, such as a vehicle, that can have a multitude of other associated systems and datasets, such as video cameras, map of assets, License Plate Recognition cameras, operators, telematics and analytics.
5.	The AVL shall display the last known location of its parent entity on dynamic maps.
6.	The AVL shall display the last known direction of travel on dynamic maps.
7.	The AVL location data shall be synchronized with video feeds associated with the unit.
8.	The AVL shall display alarms from the devices.
9.	The AVL shall display events from monitored devices.
10.	The AVL shall enable the user to place any AVL device online and offline.
11.	The AVL shall enable the user to poll any AVL device at any desired time.
12.	The AVL shall enable the user to place any AVL device in Maintenance Mode.
13.	The AVL shall let the user setup geofenced areas.
14.	The AVL shall let the user select which geofenced areas are of interest to each AVL unit.
15.	The AVL shall raise events when an AVL unit enters or exits a geofenced area. The event shall contain meta data such as the name of the AVL unit and geofenced area and a time stamp.
16.	The AVL shall let the user associate the AVL unit to a schedule (GTFS or other).
17.	The AVL shall periodically compare the current location of the AVL unit to its associated schedule and raise an event when the vehicle is behind schedule

	based on configurable thresholds.
18.	The AVL shall give the user a way to find which vehicles were inside a dynamic user-defined geofence within a specified time span.
19.	The AVL shall give the user a way to schedule a transfer of the video files from a selection of vehicles and from a specified time span to the centralized system.
20.	The AVL shall have a route playback ability to display the vehicle location and direction of travel as well as all other associated data, such as video and telematics, from a specific time and start playback.
21.	The AVL solution provider must have 24/7 support with a proper online / telephonic / chat-based support escalation portal
22.	The user interface must be the existing command and control user interface for configurations, operations and monitoring

7.4.15 Computer Aided Dispatch Software (CAD)

Sr. No.	Technical Specification
1.	Chronological display of events dispatched by call takers
2.	Allows agents to update existing event details
3.	GIS based caller location display on maps
4.	Integrated interface to handle emergency and non-emergency signals
5.	Logging and playback of voice calls with event tagging option
6.	Logging of all voice calls and SMS related to an event
7.	Click-to-call facility to callback the caller/victim
8.	Messaging facility to send case number, acknowledgment, complaint details, to the caller/victim, as SMS
9.	Phone book feature to provide one-click calling facility to hospitals, police stations emergency helplines, etc.
10.	Dispatching of events to Emergency Response Units (ERU) nearest to the caller location
11.	Dispatching multiple ERUs for an event based on demand
12.	Multiple events can be assigned to a single ERU, ERU can decide whether accept/reject the assignments, based on situation.
13.	Support to add or withdraw ERUs assigned to a mission
14.	Live update of event handling by ERU
15.	Click-to-call and messaging facility to ERUs
16.	Facility to receive live updates from ERUs in the form of text, image and video
17.	Real time location tracking of ERUs
18.	Facility to schedule future events like, VIP visit, rallies, festivals, etc. Allows the agent to set date and time for the particular case, automatic case is generated on

	that date.
19.	Allows agents to make conference call with other agents (CRM, CAD or CCS) or other dialed number by the agent.
20.	Supports messaging between agents
21.	Facility to generate report for a particular event with all details
22.	Comprehensive report generation for all events
23.	Statistical report generation
24.	Dynamic update of GIS map
25.	Searching facility based on various options, like case status, case ID, phone number, date & time, case type etc.

7.4.16 Video Management Software

Sr. No.	Technical Specification
1	VMS **General Requirements**
	The VMS application must seamlessly Integrate with the ICCC platform including the sub modules like Incident management and Big data tools for all the functionalities outlined.
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 at least 50 + brands of Cameras 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 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 – Active 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 UDP streams, the application shall redirect audio/video streams to active viewing clients on the network using multicast UDP 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).
1.16	The application shall support edge recording capabilities with ability to playback the video recorded at different speeds and ability to offload the video recorded on the application server on schedule, on event, or manually to store it on the recording server.
1.17	The proposed software shall be scalable 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. The proposed application must provide a single interface to monitor, collaborate and action for both on premises and cloud devices like cameras, ANPR devices etc.
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, ALPR, and other system events and alarms, as well as view live and recorded video.
2.2	VMS shall enable seamless integration with video analytics systems like face recognition, intrusion detection, crowd monitoring; Automated Number Plate Recognition (ANPR) system, other traffic management applications; and other typical video analytics applications
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, Incident Management System, etc.
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, including custom 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:
2.26	The ability to display all cameras attached to the system both Public, Collaborative monitoring and Cloud based entities.
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.
2.33	The ability to start/stop recording on any camera in the system that is configured to allow manual recording by clicking on a single button.
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
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	**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.
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 248-bit RSA public/private key cryptography.
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.
3.12	The application must support encryptions 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.
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 and fingerprint based biometric devices 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	Functionalities: Core 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. b. Ability to display a geographic map with VMS entities geo-located on the map. c. Ability to view any camera configured on the map. d. Ability to search cameras or location on the map. e. Ability to view live and recorded video from the cameras of the central recording server. f. Ability to display live and recorded video side-by-side for a specific camera. g. Ability to perform digital zoom on cameras. 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. i. Ability to use the camera of the smartphone and stream a live video feed to a video recorder in the system. 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.
4.4	It shall be possible to extend to the widgets of a dashboard using the SDK. This will provide the ability to develop custom widgets to the system.
4.5	The VMS shall support the following actions on a dashboard: print dashboard, export dashboard to PNG file, and automatically email a report based on a schedule and a list of one or more recipients.
4.6	The VMS shall support the following operations: • Adding an IP device • Updating an IP device • Updating basic device parameters • Adding/removing channels • Adding/removing output signals • Updating an IP channel • 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	Architecture overview: 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 though the UC&C platform. 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. 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 – 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. ii. Community surveillance camera connected via Public cloud network and further connected to the Command center UC & C platform and VMS module. iii. An Edge based intelligent IoT gateway solution with ability to sniff the CCTV feeds, which can be installed by community owners and streamed in to the Police Area Offices, Railway Offices, SP-Offices police stations or directly to the Command Center UC & C and VMS module. Such gateways streaming to either local Police Area Offices, Railway Offices, SP-Offices police stations or Central command center would be based on the availability of LAN / WAN connectivity and the architecture must be flexible enough to support both design possibilities.
5.2	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.

7.4.17 Video Analytics Software

AI based Video Analytics - Overall System Specifications		
Sr. No	**Key**	**Description**
2	**Dynamic Deployment**	Each of the video analytics use-case shall be structured as an independent module that can be deployed on any camera using a simple user interface utility, providing a complete visibility of the use cases and which cameras they are running

		on. The platform should have utility of scheduling each use case on individual camera. The user should be able to easily select the camera by tag, groups or locations and schedule applications on any camera.
3	**Advanced AI compatible**	The Video Analytics system shall be compatible with the latest technological advancements in the domain of computer vision and AI. Hence, it shall be able to quickly adapt to newer libraries and AI advancements. All the analytics and use-cases shall be based on advanced AI technology, and shall not depend on traditional algorithms.
4	**Libraries and frameworks**	The system shall be fully compatible with popular Computer Vision and Artificial Intelligence frameworks including but not limited to such as OpenCV, OpenVINO, Tensorflow, CAFFE, Pytorch, MXNet, TensorRT, Keras and Darknet. from day one
5	**Training new models**	The system shall allow seamless training by labelling any objects within the images and providing them suitable attributes of multiple types such as class, subclass, colour, type etc. The system shall allow training to happen continuously, on demand or on periodic intervals, which shall be configurable.
6	**Annotation**	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. 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.

		The annotation tool should have a comprehensive project management feature, including assigning annotation jobs on a set of images to individual users. The system should also have support for higher privileged users who can approve/disapprove the annotations done by the annotators. The user should be able to train new deep-learning models from the annotated data using the Annotation UI itself. The user-interface should allow to plug-in the trained model in any of the relevant Video Analytics use-cases dynamically at each camera. 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
7	**Model Comparison**	The System shall have a library of standardized AI models developed by the OEM of the Video Analytics System, academic institutions and members of the developer community. 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.
8	**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.
9	**Unsupervised deep learning methods**	The system shall be able to use algorithms and unsupervised deep learning methods to provide alerts and useful actionable insights from live streaming video feed data. System shall have capability to automatically analyse hours of video data for defining own rule.
10	**Self-learning Capabilities**	The system shall be capable of fully self-learning with no initial programming input by the end user. The solution shall learn what normal behaviour is for people, vehicles, machines, etc. and the environment based on its own observation of patterns of various characteristics such as size, speed, reflectivity, colour, grouping, vertical or horizontal orientation and so forth.
11	**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.
		Picture Intelligence Unit – UI Interface and Functional requirements: Video Intelligence platform should have inbuilt intelligence capabilities to deliver the analytics requirement of the PIU. This is envisaged to be a video forensic unit/ R&D Setup for Video Content Analysis. It will use live camera feeds, criminal and crime scene photographs/ videos etc. as evidence. It will ensure video analytics, continuous time stamp and non-tampering of electronic evidence as per laws.
		Video Synopsys UI- The Video Intelligence shall provide an intuitive UI for Vide Synopsys. Able to

		analyse all the recorded video files and provide the operator with synopsis video for quick review and investigation thereby reducing viewing time considerably. The video files from all the 3rd Party Video Management Software (VMS) shall be supported.
12	**Common UI for all the use-cases**	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.
13	**Web based Interface**	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.
14	**Live Video Interface**	The User interface shall allow a user to view the live video stream from any camera with overlaid information of regions, objects, people and vehicles based on each of the use-case
15	**Configuration per-use-case per-camera level**	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.
		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.
		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.

16	**Camera Calibration Tool**	The Video Analytics system UI should have an in-build camera-calibration tool that can take user inputs such as reference-heights, reference depths and floor landmarks to calibrate the camera. The calibration tool should have an option to use the GPS coordinates of the camera location. Once the camera is calibrated, each detected object should also be assigned real-world coordinates with respect to the Camera GPS coordinates. This functionality should be available for each camera added in the VA system The OEM should ensure that there should not be any geometric distortions on the deployed cameras.
17	**Key configuration parameters**	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.
		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.
18	**Filtering and Retrieval**	The system shall allow a user to filter and retrieve all the events based on any combination of the following parameters: Time of the event Objects in the event Type of the use-case Camera Location etc.
19	**Transparent and Open Architecture**	The architecture shall clearly demonstrate the technology stack with layers of the core platform, data governance and interface to different software applications.

20	**Highly parallel and distributed**	The algorithms powering the video intelligence system shall possess capability to operate parallel and distributed manner across a cluster of machines. Both training of AI algorithms and inference shall be distributed.
21	**User Management**	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.
22	**Deployment of use-case across any camera**	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.
23	**Video Compatibility**	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.
24	**Centralized Deployment Support**	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.
25	**Support for third-party use-cases**	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.
		If a new use-case needs to be developed based on Video Intelligence, the system shall provide a developer Software Development Kit (SDK) for this purpose. The SDK shall be provided along with detailed documentation for building end-to-end use-cases on the system.
		The system shall also allow the user to plug different AI models in the individual running of the video analytics use-case.
26	**Flexible Technology Stack**	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.
		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.
27	**General VA specifications**	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.
		It shall be possible to run the analytic as per hourly/daily/weekly schedule. There should be a provision to define multiple such schedules. It should be possible to set the schedule to any analytic use case. It should be possible to assign multiple analytics on the same camera.
		It is possible to generate email or a text message to the designated recipients in case critical alerts are generated. The application shall escalate the alert to the designated users through email or a text message in case the alert is not acknowledged by the operator in a specified period of time.
		It shall enable common configuration settings in a batch mode on multiple cameras.
		The application shall allow searching the analytics events based on priority, date and time (from and to) and camera. It should be possible to generate statistical analysis of various use cases across the time of the day.
		The analytics shall enable the operator to define an unlimited number of detection regions per camera. The system shall allow setting each region independently to be 'Active for Analytics' for any given period of time of the day.
		The analytics events shall be stored in the

		database. In case the events are purged, the purged events stored to external files for later reference.
		For Vehicular and ANPR Analytics, it is possible to deploy the analytics in centralized architecture where all the feeds from the cameras are available in the Data Centre and analyzed centrally.
		The system shall have a single client application for setting analytics, live viewing, archived viewing and the administrator functions.
28	**VA output Accuracy Parameter**	Accuracy may be evaluated using following KPIs: a. Detection Rate (> 99%) b. True Positive Rate + True Negative Rate (>95%) c. False Positive Rate (<5%) d. False Negative Rate (<5%)
		There should have feature to improve the accuracy overtime with further continuous learning and also based on the input received from the field officer's incident reports (**captured by the system and matrix generated through the system rather than the manual exercise**) and improvement of AI models. The OEM should take this feedback and upgrade the algorithm to show accuracy improvement quarterly basis.

Video Analytics Use Case Specifications:

AI based Crowd Estimation and Management		
S. No.	**Key**	**Description**
1.	**Introduction**	Crowd Estimation and Management (CEM) Video Intelligence system shall allow estimation of crowd density within the camera view. This is an important tool for understanding the crowd movement and management for the security and facilities management agencies. System shall raise an alert if the crowd density within a camera view

		is above a certain threshold.
2.	**Deployment**	The CEM System shall be a purely computer vision and artificial intelligence-based system that be deployed on all the existing and new CCTV cameras, including box cameras and PTZ cameras.
3.	**Camera compatibility**	The system shall be completely independent of the make/model of the cameras and be compatible with ONVIF compliant cameras. The CEM system shall support H264, H264+, H265 and MJPEG video streaming from cameras.
4.	**Accuracy on datasets**	The CEM system shall have 85% average accuracy in estimation of crowd on public databases and/or real time situation to be given during proof of concept time
5.	**Ability to define regions**	The CEM system shall have an ability to annotate multiple regions within the camera view and the user shall be able to specify crowd thresholds for each of the regions separately. If within any region the crowd density estimation if above the user defined threshold, the system shall raise an alert.
6.	**Alerts**	The system shall raise alerts in case of the following: - The CEM system shall raise an alert if the density of crowd is above a user-defined threshold. - The system shall raise an alert in case of erratic movement detected within the crowd - The system shall raise an alert if there is any chance of stampede or overcrowding due to increase in flow rate and erratic movement - The system shall trigger alarm if more than desired density is observed near specified regions of interest.
7.	**Crowd flow estimation data**	The CEM system shall also provide a data of crowd flow from one user-defined region to the other, in case of two regions selected by the user.
8.	**Data representation**	The CEM system shall have an MIS system with a detailed report and dashboard on crowding events and data at a minimum of hourly granularity. The system shall report Crowd Density and direction to load-balance various gates. The system shall provide detailed counts of total visitors in hourly/daily/weekly/monthly and overall. The system shall also provide IN and OUT counters for all the visitors

9.	**Heat Maps**	The CEM system shall have an option of generating real time heat maps of crowd density.

AI Based Camera Health Monitoring		
Sr. No.	**Key**	**Description**
1.	**Camera Status**	The Camera Health Monitoring app should be able to monitor the status of the camera and report an alert in case the camera is not functional or tampered with intentionally or unintentionally.
2.	**View Obstruction**	It should detect and raise an alert if the camera view is obstructed by any foreign object. The user should be able to adjust the threshold parameters of extent of obstruction in terms of percentage of camera view
3.	**Bright Light Shown**	The app should be able to detect and raise an alert if the camera view is tampered with bright lights. The system should specifically identify it as a camera tampering event with light shining.
4.	**Camera View Changed**	It should raise an alert if the camera view is changed/moved suddenly.
5.	**Illumination Too Low**	It should raise an alert if the camera scenes gets too dark below a threshold.
6.	**Camera Connectivity**	It should raise an alert if the camera is turned off or connectivity is lost.
7.	**Notification with Health Type**	The health monitoring app should notify the user with the type of camera health issue, namely: View Obstruction, Bright Light Shown, Camera View Changed, Low Illumination and loss of connectivity
8.	**Sensitivity Management**	It should have provision to adjust the sensitivity of detection on each camera

App Specification - Abandoned Object		
S. No.	**Key**	**Description**
1.	**Detections**	The system shall be capable of detecting left objects that have remained stationary for a period of time that is considered suspicious by the user.
		The system shall be capable of performing the left object detection despite drastic light changes and the casting of shadows in front of the left objects.
2.	**Multiple object**	The system shall have the ability to detect multiple objects that are left stationary in a scene.

	detection	The system shall be able to detect multiple objects each with its own timer as per the defined detection time. If multiple objects are abandoned in the scene one after the other and alarm shall be raised for each object (one after the other) once that object has been left in the scene for longer than the detection time.
3.	**Configuration of detection time**	The user shall have the ability to configure the detection time to suit the environment.
4.	**Event Review**	The system shall be able to immediately review the event (with a click of a single jump- to-event button) to recognize the person who has left the object.

App Specification – Person Collapsing		
Sr. No.	**Key**	**Description**
1.	**App detection**	The app should detect if a person walking upright has collapsed or fallen on the ground.
2.	**Configurable parameters**	The user should be able to configure the amount of time beyond which if the person is on the ground, the system should raise an alert.
3.	**App Reporting**	This app should raise an alert if any pedestrian is Jay walking. The app should provide zone wise data of both the pedestrian movements at zebra crossings and jay walking with a minimum of hourly granularity.

Specification – AI Based Advance Intrusion Detection		
S. No.	**Key**	**Description**
1.	**App detection**	The app should be able to detect an act of intrusion. Intrusion herein refers to the instance of an individual crossing a pre-defined virtual fence defined by the user.
2.	**Configurable parameters**	The user should be able to configure the length and orientation of the virtual fence. She should also be able to define the direction in which crossing the line would be considered as intrusion.

Other than this; The Use Cases are mentioned above; Please incorporate those while quoting the product

7.4.18 Enterprise GIS for Web GIS with Geo Analytics (Only for adding layers)

Sr. No	**Description**

1.	Should be capable of maintaining data history, version management and conflict detection.
2.	Should support database check in – check out / replication functionalities hence maintaining the parent child relationship of Master Database.
3.	Software should have inbuilt utility for checking availability of server software updates/patches
4.	Software should support Geodata service and Geometry service
5.	Software should support Cloud Environments like Amazon Web Services (AWS) or Microsoft Azure
6.	Software should support deployment on-premises on physical hardware, in a private cloud using Vmware or other virtualization technologies, or in the cloud using an Infrastructure as a Service provider (IaaS) such as e.g. Amazon Web Services, Microsoft Azure, IBM SoftLayer, etc.
7.	The software should support feature data (Point, line, polygon) as input data type and tabular data
8.	GIS system should be capable to manage maps, satellite images, GIS data of various point of interest information, infrastructure and assets etc.
9.	It should provide access to free Online 2D, 3D, Street, Basemap, imagery Services for location reference.
10.	GIS system should have a portal for administration that lets administrators to add, update, manage and maintain city GIS data and user management, Content Sharing and capability to build various GIS applications
11.	Software should have the feature to create web sites using template or wizard. It should support adding widgets which can easily be configured minimizing customization.
12.	The application should provide an out-of-the-box, configurable mobile application that allows dynamic query and update server data remotely. The mobile application should be able to integrate with GPS devices.
13.	The software should be able to seamlessly visualize and share data, maps, apps, 3D scenes with other members in organization
14.	The software should be able to share map and layer packages to be used in desktop GIS application.
15.	The software should provide a map viewer to create, save, share maps and provide analysis tools for clustering, aggregation, proximity analysis, data enrichment, etc.

16.	The software should record various usage statistics for items, users and groups, and reports this in activity dashboards and access / usage reports to administrators and or select users.
17.	The software should provide an embedded interactive app for designing and building web responsive applications with no requirement of programming.
18.	The software should support user-friendly applications for map centric field data collection, form-based surveys and maintaining field crew workforce, etc.
19.	Should be capable of Content Management (like, Manages content locations and marks relevant content as Authoritative) and Organization User Management (e.g. User can manage all aspects of inviting and managing User, including adding to groups and resetting passwords) for Managing content for different projects and role based-access management.
20.	Software allows Users to sign in with built-in accounts and accounts managed in multiple SAML-compliant identity providers configured to trust one another to manage users that may reside within or outside your organization
21.	The GIS server should be highly scalable
22.	Software should support deployment in clustered environments: Active-Active, Active-Passive.
23.	The software should provide open API to visualize the published Services
24.	Should support multiple number of Editing and viewing by desktop, web browser and mobile clients.
25.	Server application should record various service statistics, such as total requests, average response time, and timeouts, and reports this information in Manager console for better monitoring and performance optimization of services
26.	Should have Web Editing Application Functionalities like simultaneous Feature editing, isolated editing in separate versions, Undo/Redo operations, snapping by layer, snapping to new geometry, settable snapping, modify, merge, split operations, specify an Exact X,Y location, modify and create attribute values, maintain attribute values through defined rules (Domain) etc.
27.	Should support server-side geoprocessing tasks
28.	The software should provide open API to visualize the published Services
29.	The software should provide open API to visualize the published Services
30.	Should support multiple number of Editing and viewing by desktop, web browser and mobile clients.
31.	Server application should record various service statistics, such as total requests,

	average response time, and timeouts, and reports this information in Manager console for better monitoring and performance optimization of services
32.	Should have Web Editing Application Functionalities like simultaneous Feature editing, isolated editing in separate versions, Undo/Redo operations, snapping by layer, snapping to new geometry, settable snapping, modify, merge, split operations, specify an Exact X,Y location, modify and create attribute values, maintain attribute values through defined rules (Domain) etc.
33.	Should support server-side geoprocessing tasks
34.	The software should provide open API to visualize the published Services
35.	Should support multiple number of Editing and viewing by desktop, web browser and mobile clients.
36.	The Server software should support Replication across multiple commercial databases in connected and disconnected environments
37.	Server should be able to support read-only site mode. (This is intended to disable publishing new services and blocks most administrative operations during production.)
38.	Software should support a Service Oriented Architecture (SOA) (GIS on the enterprise service bus).
39.	It should have ready to use apps for Field, Office, and community and Application developers.
40.	The software should provide SDKs to build and deploy native applications on a variety of popular platforms and devices including Android, IOS, Java, .NET, QT etc.
41.	The application server and database servers must be supported on both Windows & Linux platform.
42.	Should support standard Web server / application server like IIS, Apache, Tomcat, Web Sphere, Web logic etc.
43.	Server based GIS Software should offer server-based analysis and geoprocessing. This should include vector, scripts, and tools; and synchronous processing.
44.	Server Software should run as a native 64-bit application and should support Windows 64-bit and Linux operating systems 64-bit.
45.	Should support Open Geospatial Consortium (OGC) and open web services: including Map, WMS, WFS, WCS, KML and GeoJSON
46.	Should have out of the box Web Application Functionalities like pan, zoom,

	identifying features on a map, measure distance, interactive north arrow, magnification window, overview window, find place, query attribute, search attribute, editing, geo-processing tasks, adding base maps etc.
47.	Should support browser-based access for viewing, editing and analysing of Geo-Spatial Data
48.	Software should allow character-by-character auto-complete suggestions to be generated as a user types an address in a client application for Geocoding of addresses
49.	Server Software should support rapid encoding and decoding for any pixel type for image service caches.
50.	Server administrator should be able to prevent unauthorized users from accessing cached pages by disabling of caching of service-related information by the web browser
51.	Software should allow to export data from the feature service to a file geo spatial database or SQLite database using custom clients.
52.	software should support to automatically generate diagrams and manage physical and logical network, Access, create, update, and edit Schematic Diagrams
53.	System tools can analyze patterns and aggregate data in the context of both space and time -Space-time (spatiotemporal) analysis
54.	Server Software should support Dynamic map service
55.	Server Software should support Cached service – Map, Image
56.	Server Software should support print and Schematic services
57.	Server Software should support Geocoding service
58.	Server Software should support Geoprocessing service and run custom geoprocessing models
59.	Support for geo spatial databases and Query layers – o Amazon RDS for Microsoft SQL Server or Amazon RDS for PostgreSQL o IBM DB2 or Informix o Microsoft Azure SQL Database or Microsoft SQL Server o Oracle o PostgreSQL
60.	Server Software should support Big Data File Shares like Apache Hadoop HDFS, Apache Hive, Local File Shares (CSV, Shapefile)
61.	Server Software should support Raster File Share like – AWS S3, Microsoft Azure

	Storage, Local File Shares
62.	Server Software should support for Query Layers: ALTIBASE, Dameng, IBM Netezza, SAP HANA, SQLite and Teradata
63.	Software should support simple scripting syntax to control feature rendering, label text etc. that can be used across the platform
64.	Software should support Token model authentication and the built-in User Store
65.	Should have built in user management along with Active Directory and LDAP
66.	Should support Web-tier authentication by the web server such as Integrated Windows Authentication or even leverage an organization's existing Public Key Infrastructure (PKI)
67.	Should support the option to use Enterprise Logins -
68.	Integrate with a SAML 2.0 Identity Provider (IdP) to provide Web Single Sign On
69.	Software should support to encrypt data-in-transit by enabling HTTPS
70.	Log events of interest such as who is publishing services for the Logging and Auditing purposes. Should support to enable spatial database in SAP HANA
71.	Server Software should be capable of running advanced geoprocessing tools
72.	Should have an inbuilt web gateway option to be configured and option to use different gateways like HTTP load balancer and network router devices
73.	Should have geoprocessing framework, geoprocessing tools, core analysis functionalities

7.5 SOW FOR INTEGRATED TRAFFIC MANAGEMENT SYSTEM (ITMS)

7.5.1 Key Components of Adaptive Traffic Control System (ATCS)

6.6.1.1 Traffic Signal Controller

1. 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.
2. The Traffic Signal Controller will be adaptive so that it can be controlled through thecentral 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
3. Site specific configuration data shall be stored in a non-volatile memory device (FLASH memory) easily programmable at the site through keypad or laptop. Aminimum 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.
4. 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.
5. The controller shall provide a real time clock (RTC) with battery backup that set andupdate 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.
6. The controller shall have the facility to update the RTC time from ATCS server, GPS and through manual entry.
7. The traffic signal system including controller shall have provision audio output tonesand should be disabled friendly for.
8. 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

vii. 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.

viii. 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.

ix. Special Day Plans – The controller shall have facility to configure a minimum of 20 days as special days in a calendar year.

x. 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.

xi. 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.

xii. 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.

xiii. 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.

xiv. Signal lamps monitoring – The controller shall have inbuilt circuitry to monitor the lamp status

xv. 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.

xvi. 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.

xvii. Fixed Time mode with fixed offsets

xviii. Vehicle Actuated mode with fixed offsets

- ***Input and Output facilities***

1. 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.
2. Detector Interface: A minimum of 16 vehicle detector inputs shall be available in thecontroller. All detector inputs shall be optically isolated and provided with LED indication for detection of vehicle.
3. Communication Interface: The traffic signal controller shall support Ethernet interface to communicate with the ATCS server
4. 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.
5. Real-time Clock (RTC): The GPS receiver for updating time, date and day of the weekinformation of the traffic signal controller should be an integral part of the traffic signal controller.
6. The traffic signal controller shall update the date, time and day of the week automatically from GPS during power ON and at scheduled intervals.
7. Manual entry for date, time and day of week shall be provisioned for setting the traffic signal controller RTC (Real Time Clock).
8. It shall be possible to set the RTC from the Central Server when networked
9. 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
10. Operator Display (optional): The traffic signal controller shall optionally have a LED backlit Liquid Crystal Display (LCD) as the operator interface.

6.6.1.2 Countdown Timer:

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

9. Count Down Timer to be configured in Vehicular Mode.
10. The Vehicular countdown timer should be dual
11. Color,; Red for Stop or STP and Green color for Go
12. There should be alternate Red and Balance phase time for STOP or STP in Flashing
13. 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 LEDViewing Angle 30° LED Wave Length 630-640nm (Red), 505nm - 520nm (Blue-Green)LED Dice Material AlInGaP (Red), InGaN (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 yellowAsian 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)

6.6.1.3 Communication Network:

14. 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 ICCC. Central Computer running the ATCS application shall calculate and send optimum signal timings to all intersections in the corridor. MSIshall clearly specify the bandwidth requirements and the type of network recommended for the ATCS.
15. The contractor shall specify the networking hardware requirements at the ICCC and remote intersections for establishing the communication network.

6.6.1.4 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 foruse with the box.
- Each box shall be equipped with certified cable glands/plug and with earthingbar.

Technical requirements 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	IP66 / NEMA 4X
6.	Mounting	On Camera Pole / Ground mounted on concrete base
7.	Form Factor	Rack Mount/DIN Rail
8.	Other Features	Rain Canopy, Cable entry with glands and Fans/any other accessories as required for operation of equipment's within junction box.

Cable continuity shall be through junction box dedicated terminals

6.6.1.5 ATCS Software Application

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 Computer based on the data and information gathered by vehicle detectors atstrategic locations at the intersections controlled by the system.

ATCS application software requirement:

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 corridorcycle 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 thecorridor 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 secondsmaximum.
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 simulationsoftware 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, delaysand emergency response time to events via simulation and planning tools liked 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,
S.No.	Description
	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: a. Intersection based reports i. 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). ii. 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. iii. 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. iv. 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. v. Mode switching report – The report shall give details of the mode switching taken place on a day. vi. Event Report - The report shall show events generated by the controller with date and time of event.
	vii. Power on & down: The report shall show time when the master is switched on, and last working time of the master controller. viii. 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. ix. Plan Change – The report shall show the time of change of plan either through keypad or remotely through a PC or Server. x. RTC Failure – The report shall show the time when RTC battery level goes below the threshold value. xi. 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. xii. 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. xiii. Lamp Status Report – The report shall show lamp failure report with date and time of failure, color of the lamp and associated phase. xiv. Loop Failure Report – The report shall show the date and time of detector failure with detector number and associated phase. xv. Conflict – The report shall show the conflict between lamps (RED, AMBER, GREEN) in the same phase or conflict between lamps with other phase. b. 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 c. 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.
37.	Graphical User Interface - The application software shall have the following Graphical User Interface (GUI) for user friendliness. i. User login – Operator authentication shall be verified at this screen with login name and password ii. 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. iii. 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. iv. Saturation Snapshot – This display shall show the current saturation levels of all intersections in a corridor. v. Reports Printing / Viewing – This link shall allow selection, viewing and printing of vi. different reports available under ATCS vii. Time-Space Diagram – The time-space diagram shall display the current stages being executed at every intersection in a corridor with immediate previous history. viii. Junctions shall be plotted proportional to their distance on Y-axis and time

	elapsed for the stage in seconds on X-axis. ix. Junction names shall be identified with each plot. x. Facility shall be available to plot the time-space diagram from history.
S.No.	**Description**
	xi. Currently running stage and completed stages shall be identified with differentcolors. xii. Stages identified for synchronization shall be shown in a different color. xiii. Speed lines shall be plotter for stages identified for synchronization to the nearestintersection in both directions. xiv. It should be possible to freeze and resume online plotting of Time-Space diagram. xv. The system shall have other graphical interfaces for configuring the ATCS, as appropriate.

6.6.1.6 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 preciseinformation 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 capabilityin 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, no matter 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-calibration functions throughout the entire design life.
12.	It should have flexibility of installation on the roadside, at the corner of an intersection, at themedian of a highway or on a gantry, with best results, not like side-firing technology, needing set-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.

7.5.2 SCOPE OF WORK

6.6.2.1 Automatic Number Plate Recognition (ANPR) System

Overview

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 statusand category as specified by the database. The system usage shall be privilege driven using passwordauthentication. 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 recognitionof 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 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.

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. Local Server at Intersection: The system must run on a Commercial Off the Shelf Server (COTS). Outdoor IP 66 Quad core processor based server should be able to cover at least 8 lanes. Temperature rating of the server should be at least 60 degree.

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 tothe command control and communication centre 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. Minimum 2(two) USB Port to support the latest external mass storage devices and Ethernet (10/100) Port for possible networking. However all logs of data transfer through the ports shall be maintained by the system.

xxi. System should be capable of working in ambient temperature range of 0 Degree Celsiusto 60 Degree Celsius.

xxii. Lightening arrester shall be installed for safety of system (As per BIS standard IS 2309 of 1989).

xxiii. The housing(s) should be capable of withstanding vandalism and harsh weather conditions and should meet IP66, IK10 standards (certified).

xxiv. Encrypted data, images and video pertaining to Violations at the Onsite processing station should be transmitted to the ICCC electronically.

xxv. Advanced Encryption Standard (AES) shall be followed for data encryption on site and ICCC, and its access will protected by a password.

xxvi. Ability to video recording in base station for 7 days. Automatically overwrite the data after 7 days.

xxvii. Direct extraction through any physical device like USB flash drive, Portable Hard disk etc. shall be possible.

xxviii. Network Connectivity: Wired/GPRS based wireless technology with 4G and upgradableor batter to be provided.

xxix. Vehicle number detection is to be made possible on the ANPR cameras.

xxx. ANPR cameras should also have capability to detect Red Light Violation.

xxxi. The complete tracking of the vehicle is to be made possible on the GIS map to locate any suspicious / identified vehicle.

xxxii. 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.

6.6.2.2 Red Light Violation Detection (RLVD) System

Overview

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 LightViolation, 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 ofViolation, 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 stateof signal (Red/Green/Amber) by which the system should clearly show nature of violationand 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 trafficsignal 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.

Scope of Work

Over all solution should be able to provide features and capable to fulfil the following requirements:

a. Speed Violations :

i. 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.
ii. The system shall have the provision of setting different speed thresholds for different class of vehicles.
iii. The speed violations system should be installed on mid-blocks or designated areas as identified during design stage.

b. Wrong Direction Vehicle Movement

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.

c. Recording & display information

The recording and display of information should be detailed on the snapshot of the infractingvehicle 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

- The system should start automatically after power failure. The system should have secureaccess mechanism for validation of authorised personnel.
- A log of all user activities should be maintained in the system.
- Roles and Rights of users should be defined in the system as per the requirements of theclient
- In the event that the connectivity to the ICCC is not established due to network/connectivity failures, then all data pertaining to the infraction shall be stored onsite and will be transferred once the connectivity is re- established automatically. Ability of physical transfer of data on portable device whenever required. There should be a provision to store minimum one week of data at each site on a 24x7 basis. System shouldbe mounted as per appropriate deign by MSI.

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 whichinclude a wider view covering the violating vehicle with its surrounding and a closer viewindicating readable registration number plate patch of the violating vehicle or its web linkon notices for court evidence.

c) All outstation units should be configurable using the software at the Central Location.

d) 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.

e) 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).

f) 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.

g) 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

suchcases the printing should be possible along with the magnified image.

h) 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, thesystems need to be configured to mask and recover with minimum outage.

i) The evidence of Infraction should be encrypted and protected so that any tampering canbe detected.

j) The user interface should be user friendly and provide facility to user for viewing, sortingand 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.
- On site-out station processing unit communication & Electrical Interface (Junction Box).
- The system should be equipped with appropriate storage capacity for 7days 24X7 recording, with over writing capability. The images should be stored in tamper proof format only.
- Wired/GPRS based wireless technology with 4G and upgradable.
- Minimum 2(two) USB Port to support the latest external mass storage devices and Ethernet (10/100) Port for possible networking.
- System should be capable of working in ambient temperature range of 0 degrees C to 60 degrees C.
- Lightening arrester shall be installed for safety of system (As per BIS standard IS 2309 of 1989).
- The housing(s) should be capable of withstanding vandalism and harsh weather conditions and should meet IP66, IK10 standards (certified).
- Encrypted data, images and video pertaining to Violations at the Onsite processing station should be transmitted to the ICCC.
- Advanced Encryption Standard (AES) shall be followed for data encryption on site and ICCC, and its access will protected by a password.
- Ability of continuous video recording in base station for 7 days. The system shall automatically overwrite the data after 7 days. It should be noted that at any point of time the local storage at the base station should have the data of previous 7 days.

- Direct extraction through any physical device like USB flash drive , Portable Hard disk etc. shall be possible

6.6.2.3 Automated e- Challan System

a. 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 /Fakeaddressed
ix. Vehicles/Theft Vehicles/Authorized complaints/Multiple owners)
x. Identification of Police Stations, Junctions, Courts, Police Staff for theTraffic 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

6.6.2.4 Speed Violation Detection (SVD) System

Overview

a) The Speed Violations should be automatically detected by the system by using appropriate sensors technology.

b) The system should be capable of capturing multiple infracting vehicles simultaneously in defined lanes at any point of time simultaneously with relevant infraction data like:

   i. Type of Violation
   ii. Speed of violating vehicle
   iii. Notified speed limit
   iv. Date, time, Site Name and Location of the Infraction
   v. 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 or video frames of the violation, covering the violating vehicle with its surrounding.

d) The system shall provide the No. of vehicles infracting simultaneously in each lane. The vehicles will be clearly identifiable and demarcated in the image produced by the camera system.

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.

f) Speed measurement may be made by using non-intrusive technology such as Image based or any other appropriate certified technology. CE and homologation certificate from Ministry of Traffic or equivalent department from respective country of origin, document authenticated by Indian Embassy (to authenticate that systems are legalized and tested for infractions to avoid legal issues) or Certificate from internationally accredited metrology laboratories (approved for speed calibration) is acceptable.

g) The system should automatically reset in the event of a program hang up and restart after power failure.

h) Ability to define role based access.

i) The data shall be transferred to the ICCC in real time for verification of the infraction and processing of challan.

j) In the event that the connectivity to the ICCC is not established then all data pertaining to the infraction shall be stored on site and will be transferred once the connectivity is re-

established automatically.

Speed Violation Application

a) It should be capable of importing violation data for the Operator for viewing and retrieving the violation images and data for further processing. The programme should provide for sort, transfer & print command.

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) All outstation units should be configurable using the software at the Central Location.

d) Violation retrieval could be sorted by date, time, location and vehicle registration number and data structure should be compatible with PSCL Traffic Police database and PSCL Transport department database structure.

e) The operator at the back office should be able to get an alarm of any possible fault(s) at the camera site (outstand) (e.g. sensor failure, camera failure, failure of linkage with traffic signal, connectivity failure, Camera tampering , sensor tampering).

f) The automatic number plate recognition Software may be part of the supplied system, or can be provided separately as add on module to be integrated with violation detection. a.) Success rate of ANPR will be taken as 80% or better during the day time and 60% or better during the night time on standard number plates.

g) Image zoom function for number plate and images should be provided. Any updates of the software available, shall be updated free of cost during the contract period by the vendor and will integrate the same with existing application and database of PSCL TrafficPolice and PSCL Transport department.

h) The application software should be integrated with the notice branch software for tracing the ownership details of the violating vehicle and issuing/printing notices.

i) Various users should be access the system using single sign on and should be role based. Different roles which could be defined (to be finalized at the stage if SRS) could be Administrator, Supervisor, Officer, Operator, etc.

j) Apart from role based access, the system should also be able to define access based on location.

k) Rights to different modules / Sub-Modules / Functionalities should be role based and proper log report should be maintained by the system for such access.

l) Important technical components of the architecture must support scalability to provide continuous growth to meet the growing demand of PSCL Police. The system shall support

vertical 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. Main technological components requiring scalability are Storage, Bandwidth, Computing Performance (IT Infrastructure), Software / Application performance and advancement in proposed system features.

m) The system shall also support horizontal scalability so that depending on changing requirements from time to time, the system may be scaled horizontally.

n) 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 shall be in such a way as to be resilient to technological sabotage. To take care of remote failure, the systems need to be configured to mask and recover with minimum outage.

o) 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 endeavour to make use of the SSL/VPN technologies to have secured communication between Applications and its end users. Furthermore, all the system logsshall be properly stored & archived for future analysis and forensics whenever desired.

p) 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.

q) System shall use open standards and protocols to the extent possible.

r) The user interface should be user friendly and provide facility to user for viewing, sorting and printing violations. The software should also be capable of generating query based statistical reports on the violation data.

s) The data provided for authentication of violations should be in an easy to use format as per the requirements of user unit.

t) User should be provided with means of listing the invalid violations along with the reason(s) of invalidation without deleting the record(s).

u) Basic image manipulation tools (zoom etc.) should be provided for the displayed image but the actual recorded image should never change.

v) Log of user actions be maintained in read only mode. User should be provided with the

password and ID to access the system along with user type (admin, user).

w) Image should have a header and footer depicting the information about the site IP and violation details like viz. date, time, equipment ID, location ID, Unique ID of each violation, lane number, Registration Number of violating vehicle and actual violation of violating vehicle etc. so that the complete lane wise junction behaviour is recorded viz. (Speed of violating vehicle, notified speed limit, Speed Violation with Registration Number Plate Recognition facility. Number plate of cars, buses/HTVs should be readable automatically by the software/interface. There should be user interface for simultaneous manual authentication / correction and saving as well.

x) Interface for taking prints of the violations (including image and above details).

Scope of Work

a) Traffic violations of over speeding vehicles in fixed locations as well as predefined stretchof road shall be automatically detected by the certified and homologated system which isin use with various agencies worldwide.

b) All over speeding vehicles not following traffic rules and driving unsafe with risk to themselves and others will be fines. Vehicles crossing any dangerous spot will be booked with SPOT SPEED ENFORCEMENT SYSTEMS. At the same time Point to point speed will also be installed in some strategic arterial (urban/highway road to prosecute commuterswho try to slow down just in front of the spot speed systems and then over speed. Vehiclespassing through the control section at a Speed greater than a determined speed limit (values to be made configurable via software) shall be detected as violation and System shall produce a sequence of relative images (or a movie) with value of speed detected andexecuting ANPR process to automatically extract number plate of vehicle in infraction.

c) The photograph generated by the system at both locations shall be stitched together and ANPR shall be performed.

d) Specifications for Instant Speed System.

S.No.	Specifications
1	Traffic violations should be automatically detected by the system. The System should provide image of over speeding vehicle with proper proof of speed violation in terms of Video and photographs of vehicle with required data printed on it.
2	Following data for each infraction should be provided: date, time, location, speed, number plate with the help of automatic number plate detection mechanism(using ANPR camera or similar means).

3	System should generate automatically color image (day time) of the number plate of the Vehicle. In case of traffic violations, the system shall generate challan as per pre-defined formats with relevant images of violation. The system should provide control image to verify speed.
4	The Speed system should use a speed sensor which has means to cross confirmation through simulators. The speed sensor should have possibility of proper working without actual vehicle transit.
5	System should be in the form of a 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. Preferred systems should be installed at a minimum height of 5.5 meters or above.
6	System should work in day and night condition and in bad weather conditions
8	Camera Unit: Cameras must be Day night and must have CMOS with 1/2.8" sensor (or greater), shutter speed 1/1000 sec or better, resolution 2Megapixel or better, temp range -5 to +55°C, Megapixel auto iris lens.
9	Integrated external Infrared capable to take images in night time and detect automatically number plate for minimum 25 meters.
10	Control: speed setup Km/hr, up to 150km/h ± 3%
11	Working temperature 0°C to +60°C 80% and above humidity.
12	Processor: Industrial processor for local site with minimum 7 days recording. LPU/system should send data automatically to the CCR and should be able to auto start in case of power failure.
13	BACK office: the system should provide data decryption and storage, Issuing of automatic challan with automatic number plate detection with multiple images. No deletion or addition of data without proper authorization & proper password protection
14	Possibility to import data files and infractions should be provided as per city police requirement. Violation retrieval should be available for selected location, time and number series (DL 07,UP 07...etc.). (one-time configuration of software as per Traffic police requirement should be considered)
15	System should be able to recognize automatically the number plate of cars in involved in violation. The accuracy should be more than 80% in day and 60 % night condition. ANPR system should be capable to work with Indian number plates and should preferably have been used for Indian plates for a considerable period of time.

16	Communication: -The system should have proper communication with control room and should be able to provide online infraction reports and live infraction. Automatic number plate detection should be part of the system
17	Back office: Server Intel Xeon (8M Cache, 2.30 GHz or better) with 16GB (2 X 8GB) RAM and 6TB SATA Hard Disk Server based back office will be preferred to single pc software
18	Stability of product and after sale services: MSI should have local support for technical assistance and system should be repairable or replaceable. MSI should show spares availability for minimum 2 such systems.
19	Third party (authorized company to do so) speed test reports can be submitted to client. On field detailed speed test reports for more than 120-200 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 post implementation but before FAT.
20	Test reports for IP 66 for cameras should be provided. This is to support harsh rainy season and dusty environment.

e) Specification for Average Speed System

S.No.	Specification	Minimum User Requirement
1	General	Technology to be used is non-intrusive.
		The measure of vehicle speed shall be the Average Speed in a control section.
		The system may also be used for measuring Instant Speed at any point
		All vehicles passing through the control section at a Speed greater than a determined speed limit (values to be made configurable via software) shall be detected as violation and System shall produce a sequence of relative images (or a movie) with value of speed detected and executing ANPR process to automatically extract number plate of vehicle in infraction. The system should not be solely ANPR depended for speed ticket generation. System shall have provision for setting different speed thresholds for minimum of two vehicles categories (light, commercial).
		Minimum User Requirement

		System shall work in day and night conditions and should be
		The system should have option to add instant speed in case if client decided to add instant speed in future.
		Cameras fitted in the equipment shall record a digitized image or video frames of the violation covering defined lanes on each approach arm at any point of time simultaneously with relevant data about the offence, i.e. date, time, fixed location and speed etc.
		The photograph generated by the system at both locations shall be stitched together and ANPR be performed.
		The results are independent of number plate recognition at individual points.
		Make: Certified Camera for the Purpose as per certificate Resolution: 2 Megapixels or better(see camera details in Camera part)
		External IR (no flash)
		Distance: 25 meters with 20 degrees beam
		The mounting(s) shall house all the required connections including the electricity and network connectivity. It also houses the microprocessor unit and electronic interface with the sensors, camera(s) etc. and an UPS
		The housing(s) confirms to IP 66
		(security class LASER (IEC/EN 60825)/Image based System in cases were instant speed is installed with average speed
		Speed limits to be measured 150km/hr.
		Maximum error permissible ±3 %
		Speed measurement to be made by non-invasive
		system through approved technologies and for systems already in use used by authorities worldwide.
		System should provide specific lane of the vehicle when speeding
		System should provide clear megapixel image with automatic ANPR data with speed in image
		The vendor shall calibrate the cameras from time to time and ensure that the calibration certificates are provided to the client to ensure

		accuracy of system.
		Violations should be available for selection from a displayed list corresponding to each location separately. The retrieval could be sorted by date, time, location and by vehicle registration number.
		Various automated reports should be available for hourly data, infraction per hour/day week etc.
		The user interface broadly falls into the categories of viewing, sorting and printing violations and system configuration/housekeeping.
		The violation viewer shall be provided with a means of listing the invalid violations along with the reason(s) of invalidation without deleting the original record(s).
		Complete database management and E fine issuance
		Software shall provide interface for taking printouts of violations .
		There shall be a password access system along with user type (admin,user). It permits role based permission system for accessing the data base and printouts.
13	Communication	The system shall have appropriate means of communication viz.3G/leased lines or any other better means of network with the Control Room.
14	Local Processing	The industrial processor used should be provided with each camera.Should be minimum multiple core , RAM 2 GB, with SD storage and USB storage options, temp -40 to 60 degrees and should be part of system.
	Unit	(LPU specifications are minimum and OEM should provide industrial LPU as required for applications supplied)
15	Integration with Third Part VMS	The system should be integrated with the proposed Video Management System.

f) Violation Transmission and Security

i. Encrypted data, images and video pertaining to Violations at the Onsite processing station should be transmitted to the ICCC electronically through GPRS based wireless technology with 3G upgradable to 4G or wired connectivity, in JPEG format.

ii. Advanced Encryption Standard (AES) shall be followed for data encryption on site and ICCC, and its access will protected by a password.
iii. The vendor shall ensure that the data from the onsite processing unit shall be transferred to ICCC within one day.

g) Video Recording

iv. The system should be capable of continuous video recording in base station for 7 days. The system shall automatically overwrite the data after 7 days. It should be noted that at any point of time the local storage at the base station should have the data of previous 7 days.
v. Direct extraction through any physical device like USB, Hard disk shall be possible.

6.6.2.5 Traffic Accident Reporting System (TARS)

a) TARS solution should provide:

i. Accident reporting system
ii. Accident recording system
iii. Analysis of accidents
iv. 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 Road Accident 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:

i. how the accident happened,
ii. detailed information about the vehicle(s) involved
iii. type and extent of human impact
iv. human factors involved (inebriation, etc.)
v. nature of any injuries,
vi. type and extent of property damage,
vii. socio-economic data of the people involved,
viii. primary & secondary causes of the accident

ix. incident photos
x. drawing of accident analysis
xi. information on analysing agency and personnel

6.6.2.6 Traffic Sensors Lights and Signals

a) 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.

b) 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

c) Traffic Lights: Key Features:

i. lowest power consumption for all colors
ii. Meets or exceeds intensity, color and uniformity specifications
iii. Temperature compensated power supplies for longer LED life
iv. Uniform appearance light diffusing
v. Should be Intertek/ETL/EN certified
vi. LED shall be single source narrow beam type with clear lens & Luminance uniformityof 1:15
vii. Pedestrian traffic lights should be
viii. provided with clearly audible signals for the benefit of pedestrians with visual impairments
ix. Phantom Class 5 or equivalent. IP Rating: IP65
x. LED aspects:
xi. Red, Amber, Green-Full (300 mm diameter) : Hi Flux
xii. Green-arrow (300 mm diameter): Hi flux
xiii. Animated Pedestrian-Red and Green Animated c/w countdown (300 mm) Hi Brite withdiffusions
xiv. LED Retrofit Specifications:
xv. Power supply: Redundant
xvi. Standards: EN 12368 certified
xvii. Convex Tinted Lens: Available

xviii. Fuse and Transients: Available

xix. Operating Temperature Range: 0 degree Celsius to 55 degree Celsius Turn Off/Turn OnTime: 75 milliseconds max

xx. Total Harmonic Distortion: <20%

xxi. Electromagnetic interference: Meets FCC Title 47,Subpart B, Section 15 Regulation orequivalent EN/IRC standard

xxii. Blowing Rain/Dust Spec: MIL 810F or Equivalent EN/IRC standard complaint

xxiii. Minimum Luminous Intensity (measured at intensity point)(cd):

- Red 400
- Amber 400
- Green 400
- Dominant Wavelength (nm):
- Red 630
- Amber 590
- Green 490

d) Lamp conflict compatibility system: Compatible with lamp failure and conflict detection

6.7 CCTV SURVEILLANCE SYSTEM

6.7.2.1 Outdoor Fixed Box Camera

S.No	Features	Specifications
1.	Form Factor	Box Type / Bullet Camera
2.	Image Sensor	1/2.8" Progressive CMOS
3.	Day/NightvOperation	ICR with IR range of 100m or better
4.	Minimum Illumination	Color 0.005 lux , B/W 0.0005 lux
5.	Lens	External Lens (5 mm to 50 mm)
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
21	Edge Video Content Analytics	Camera should have in-built Edge Based Analytics, Abandoned Object, Intrusion Detection, Tampering, Line Crossing, Loitering Detection, Object Removal
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 though 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	,30% ~ 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

6.7.2.2 Outdoor PTZ Camera

S. No.	Parameters	Specifications
1.	Certifications	UL /BIS ,CE,FCC, IP66
2.	Compatibility	ONVIF profile S , G and Q
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	4-6mm to 120-180mm
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
19.	Edge Video Content Analytics	Camera should have in-built Edge Based Analytics, Abandoned Object, Intrusion Detection, Tampering, Line Crossing , Loitering Detection, ObjectRemoval
	Storage backup on network	Camera should support network failure detection , Camera should have thecapability to start the recording automatically on SD card in

20.	failure	case of connectivity between camera and NVR/Storage device goes down
21.	Edge 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	Min8 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
S. No.	**Parameters**	**Specifications**
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 ± 20% / DC 12V
43.	Power Consumption	45W or less (with IR & Heater on)

6.7.2.3 ANPR Camera

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 ICCC platform.
3.	The automatic number plate recognition Software will be part of the supplied system, Success rate of ANPR will be taken as 95% or better for both day and night time.
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 ICCC.
33.	ANPR should have at least 1 Deployment in India in any Law Enforcement Project. Necessary Document evidence to be provided
34.	Vehicle Search: Shall have an option to search vehicles by a. vehicle colour b. vehicle colour +license plate c. vehicle make and type d. date & time e. location f. type of Vehicle
35.	Number plate missing detection: a. 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. b. The system should have capability to let the user search for all such vehicle through a UI based filtering system The user should be able to search and track any such vehicle using various vehicle search criteria as mentioned in the point above.

6.7.2.4 RLVD:

S.No.	Features	Specifications
1	General	System should be totally digital
2	Vehicle	The system shall detect and capture vehicle details when:

	violation criterion at Intersection	(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 instantspeed 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 allevidences 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 withoutintrusive 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 theIP65 box OR comprised of camera or other units mounted onpoles 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, Imageof 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 of 0 to 200 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 more than 120-200 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	Challan	
	Integration	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.

6.7.2.5 Infrared Illuminators

The infrared illuminators are to be used in conjunction with the cameras specified above (as required) to enhance the night vision, in case, MSI 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 forthe application
5	Casing	Aluminium and Polycarbonate
6	LED Indicators	Required
7	Environmental Protection	IP66, IK09 Rated
8	Mount Options	Wall, Ceiling, Camera Housing Mount
9	Operating Temperature	0 °C to 55 °C or better
10	Standards/Certification	UL,CE,FCC
11	Approved Makes	Same as Camera OEM

6.8 Public Address System

Overview

a) The Public Address System (PA) shall be capable of addressing citizens at specific locations from the ICCC.
b) The proposed system shall contain an IP-based announcing control connected tothe ICCC.
c) Public Address system shall be used at intersections, public places, market placesor those critical locations as identified by PSCL to make important announcementsfor 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 shallbe 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) MSI shall install IP based Public Address System as part of the informationdissemination 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 ICCC

c) MSI, 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. MSI 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 toestablish 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. CasingIP-55 rated for housing

6.9 Variable Messaging System

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 contentfor VMSB display.
c) The system shall have capability to divide VMSB screen into multi parts to displaydiverse form of information like video, text, still images, advertisements, weatherinfo, 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 authenticationbased 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 basedon 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 thereare 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 andthe infrastructure from malicious attacks, theft, natural disasters etc. provisions for security of field equipment as well as protection of the software system fromhackers and other threats shall be a part of the proposed system. Using Firewallsand 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 makeuse of the SSL/VPN technologies to have secured communication between Applications and its end users. Furthermore, all the system logs shall be properlystored & 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 thegrowth 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 communicationbetween 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, butis 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 locationswith 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, VMBS 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 ICCC.

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 ICCC 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 ICCC.

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 startsand 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.

- ***Variable Message Sign Board application***

a) Central Control and Communication Software should allow controlling multiple VMS from oneconsole.

b) Capable of programming to display all types of Message/ advertisement having alphanumericcharacter in English, Hindi, and combination of text with pictograms signs. The system shouldhave 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 messageto any VMS unit.

n) Various users should access the system using single sign on and should be role based. Differentroles 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 singlepoints 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 securitypolicy. 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.

- ***Remote Monitoring***

All VMSB shall be connected / configured to ICCC for remote monitoring through network fortwo 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 200mmapprox.)
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 Diming
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 automaticcontrol)

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/EN12966 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: 2.88mX1.2m 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/EN12966 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 charactersize 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 whendiodes are not illuminated.
   iii. All periodic self-test results shall be relayed to the ICCC in real time to update thestatus of the VMS

6.10 Emergency Call Box

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 ICCC 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) MSI shall also install Emergency Call Box/Panic buttons at 50 locations (the final no. might vary based on field survey by MSI) in the city. These systems shall be deployed at identified junction for ease of access by citizens of PSCL city.

b) MSI, 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. MSI 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

6.11 Environmental Sensors

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 outdoorenclosure. 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 followingintegrated sensors inside one station: ▪ 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.
.	The sensor management platform shall allow the configuration of the sensor to the network and also location details etc.

0	▪ 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 AAQMSand 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 aperiod 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 thecentral 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 andgraphs either locally or from a remote client. ▪ 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	▪ 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** ▪ 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 ±30%.
2.	**Ozone (O3) Sensor** ▪ 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 ±30%
3.	**Nitrogen Dioxide (NO2) Sensor** ▪ 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 ±30%

4.	**Sulfur Dioxide (SO2) Sensor** ▪ 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 ±30%
5.	**Carbon Dioxide (CO2) Sensor** ▪ 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 CO2sensor shall be 0°C to 60°C ▪ Operating pressure of CO2 sensor shall be ±30%
6.	**Particulate Profile Sensor** ▪ Particulate profile sensor shall provide simultaneous and continuous measurement of PM10,PM2.5, SPM and TSP (measurement of nuisance dust) in ambient air ▪ Range of PM2.5 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 ±30%
7.	**Temperature Sensor** ▪ 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** ▪ 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** ▪ 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** ▪ 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** ▪ 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** ▪ 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** ▪ 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 to120 dBA ▪ Noise sensor shall have resolution of 0.1 dBA
14.	Integration with ICCC solution, VMSB, Portal and Mobile applications
15.	Conditions-Ruggedized enough to be deployed in open air areas on streets and park

8. CONCEPT DESIGN & LAYOUTS

8.1 Data Center (DC) at Patna Smart City Office

DC will occupy around racks of capacity as per given space, as smart city requirements are concern 20 racks of space including all servers, storage and Network components in centralized architecture framework will be required.

DC will occupy BMC room along with common NOC and SOC room for maintenance of Data Center IT Equipment's, whereas 300 KVA UPS for Power to IT load with HA will be used. Power requirement for given infrastructure is around 260 KVA.

Racks and Power are extended looking towards future expansion in Data Center at single point of time.

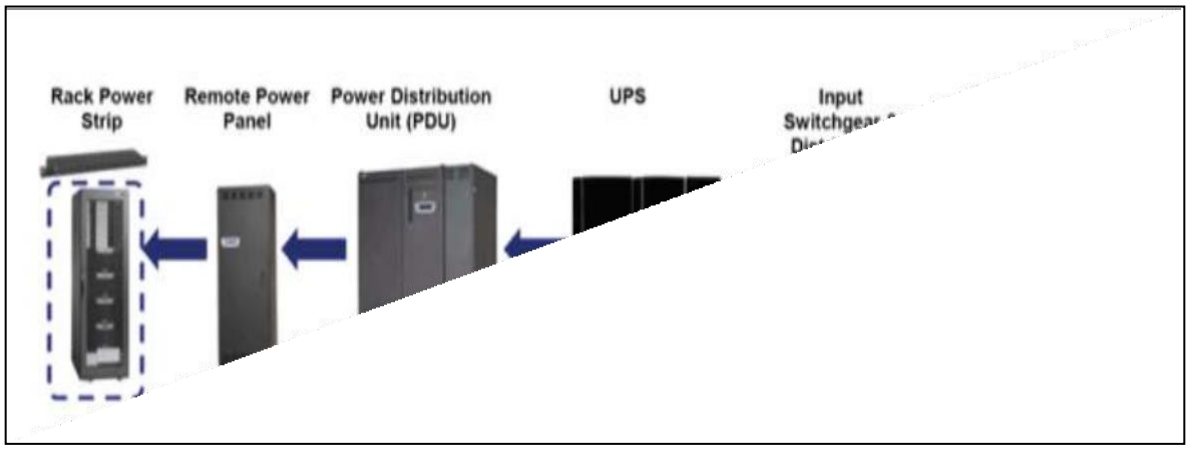


Figure: DC at PATNA SMART CITY OFFICE

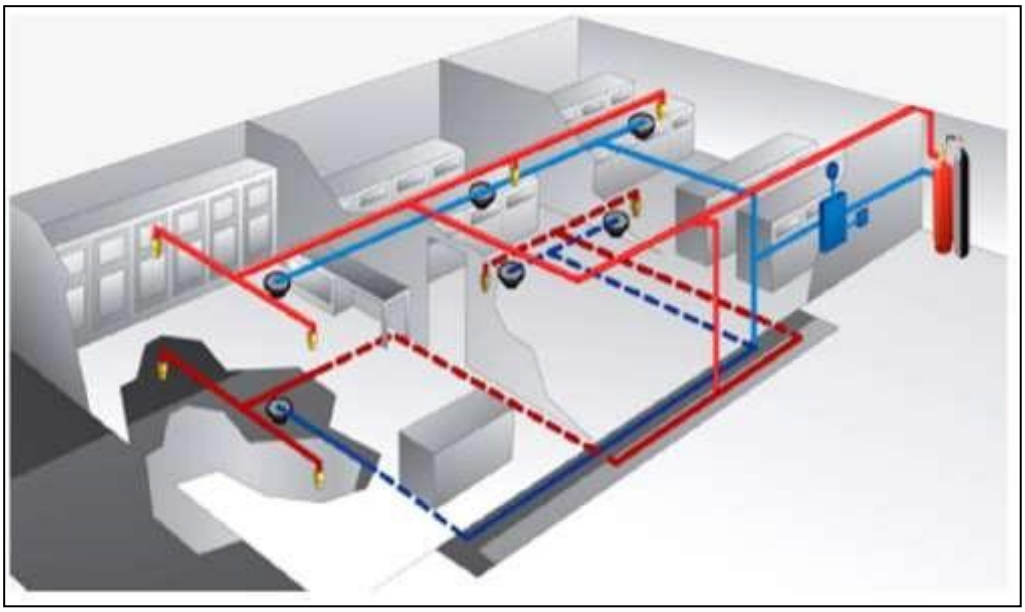
Data Center will be equipped with Access Control- Biometric Entry/ Exit protocols for ensuring authorized access.

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

Date Center will be provisioned with leading NOVEC Fire Protection System.

NOVEC 1230 fluid is a sustainable fire extinguishing clean agent that helps protect continuity of operations and high value assets. It will be non-conductive and will leave no residue, putting out fires while preserving both assets and operations. NOVEC Gas Fire Suppression system for the UPS room will be provisioned separately.

Figure: Fire Protection Layout



Raised Flooring and other essential components of DC

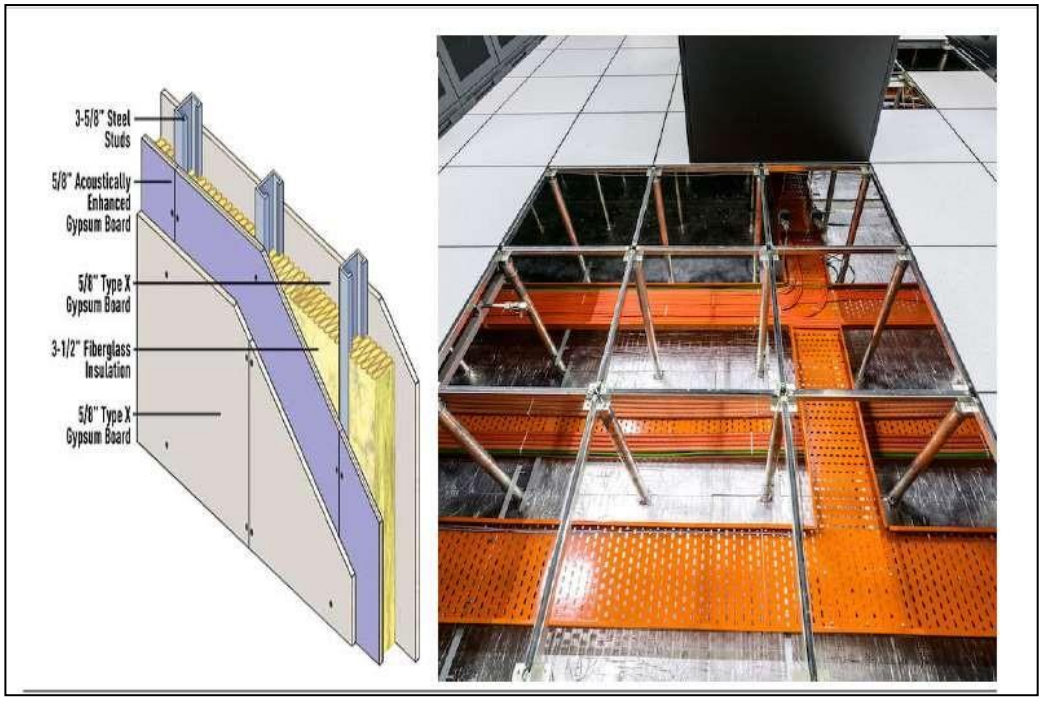


Figure: DC raised flooring

Functional specification of field devices:

A. Cameras and sensors

a) The camera & sensors layer will help the city administration gather information about the city conditions and capture information from the edge level devices.

b) The cameras need to work on 24 Hours throughout the year during all weather conditions and shall also provide continuous feeds from the installed locations with field of View to capture all coverage in the Data Center.

c) Each camera will work on high bandwidth (average 3/5 Mbps per camera approximately with H.265 compression) with robust infrastructure to provide stable and sharp streaming at the video wall layer.

d) The field cameras will pull the entire feeds on a MPLS cloud and broadcast the streams at Police Area Offices, SP-Offices, Railway Offices and Smart City Offices based upon the respective jurisdictions defined in an operational rule-based network engine.

e) All cameras must be equipped with capabilities to monitor and provide alert

during instances of vandalism, theft, etc. The housing should be vandal-proof with IP-66 weather-proof and IK 10 enclosure.

f) The cameras will be equipped with embedded cyber security measures and should not be classified with GB28181, GB/T28181-2011 standards which primarily facilitate the OEM to access the camera from anywhere globally and ingest outside videos in the network.

g) The camera should be capable to manage smart of the moving objects to minimize the effective bandwidth requirement and reduce storage space requirement.

h) Smart city Logo will be embossed/etching (in colour) in each camera

B. Civil and Hardware

Supply & Installation of Camera Infrastructure:

Based on detailed field survey as mentioned above, installation and commissioning the surveillance and monitoring systems at the identified locations and also undertake necessary work towards its testing. MSI will ensure the industry leading practices during the implementation phase w.r.t positioning and mounting the cameras, poles and junction boxes.

a) Ensure that surveillance and monitoring objective is met while positioning the camera such that the required field of view is being captured as finalized in field survey

b) Ensure that camera is protected from on field challenges of weather, physical damage and theft.

c) Make proper adjustments so as to have the best possible image / video captured.

d) Ensure that the pole is well placed for vibration resistance adhering to the road safety norms.

e) Deployment of Collisions preventive barriers around the junction box & pole foundation in case it's installed in collision prone place.

f) Appropriate unique code is to be given to each pole, which will be painted on respective pole.

C. Installation of Poles/Cantilevers

a) All installations are done as per standards with final check & satisfaction of the

Patna Smart City. For installation of CCTV Cameras, PTZ Cameras, Public Address System, etc.

b) It will be ensured that the poles erected to mount cameras are good, both qualitatively and aesthetically (the drawings have to be pre-approved by the Patna Smart City Officials).

c) The poles shall be installed with base plate, pole door, pole distributor block and cover.

d) Structural calculations and drawings for the approval of Competent Authority wiol be provided.

e) The OEM will be required to provide Manufacturing Authorization Form/ Certificate with the Country of Origin details for every product being provided as a part of Project requirement.

f) MSI will ensure that OEM will submit Factory Acceptance Certification for all its products.

g) The certification of the field equipment like poles for successful installation in terms of seismic strength, durability, etc. and the building floor strength a third-party inspection can be conducted through Government/PSUAuthorizedInstitutions/agencies

h) Coordination with concerned authorities / municipalities for installation to expedite the work.

i) Poles and cabinet shall be so designed that all elements of the field equipment could be easily installed and removed.

j) The physical look of the installation area returns to neat & tidy conditions after installation of poles, cantilevers etc. The placement shall be designed keeping in mind the normal flow of vehicular traffic and pedestrian movement is not disturbed.

k) The indicative drawing of pole and cantilever with foundation work is provided below:

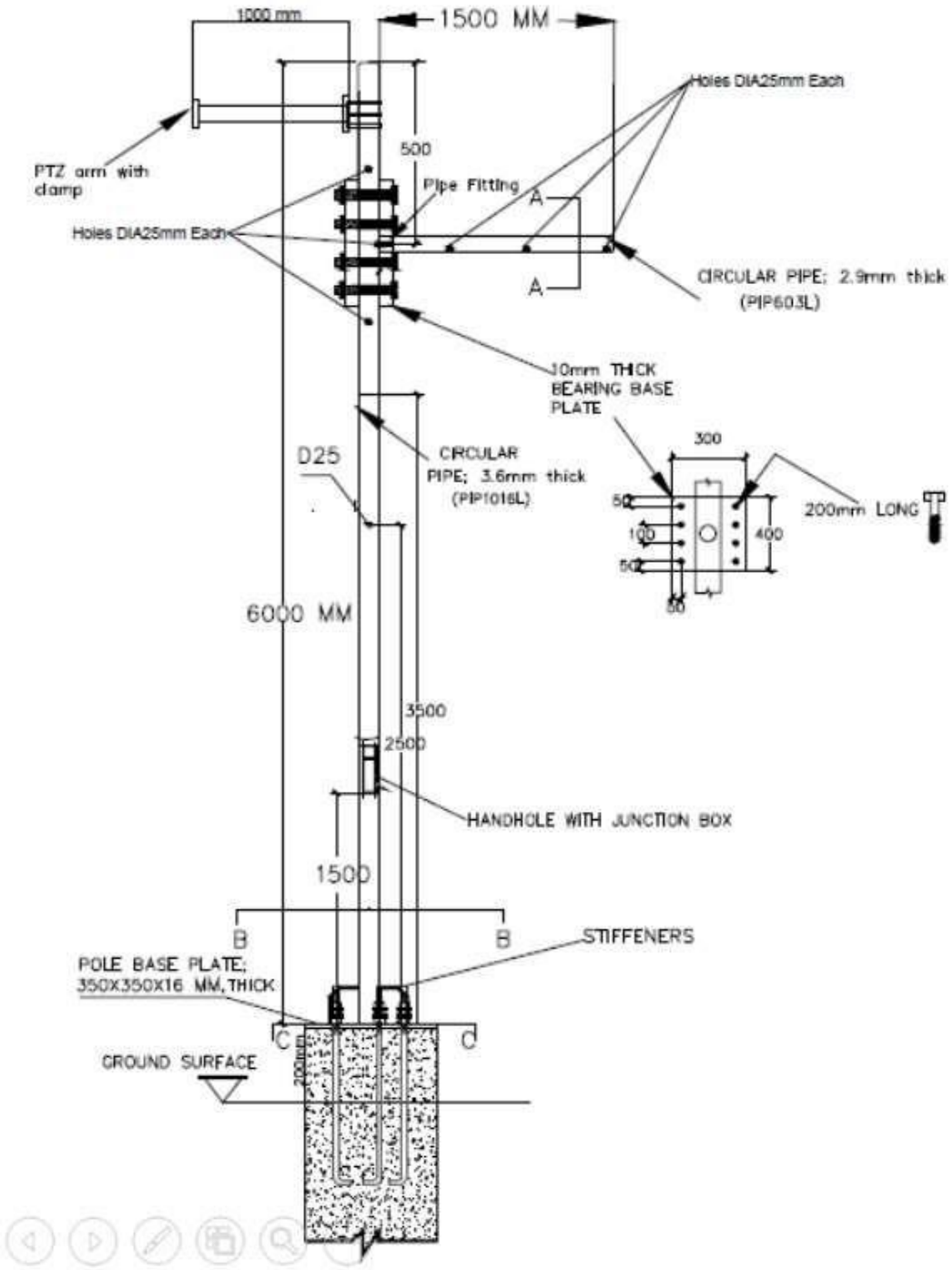
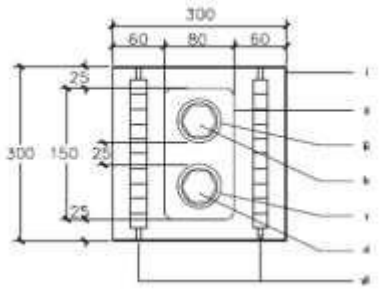
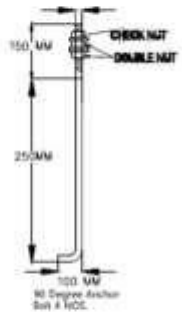


Figure: Indicative drawing of pole and cantilever

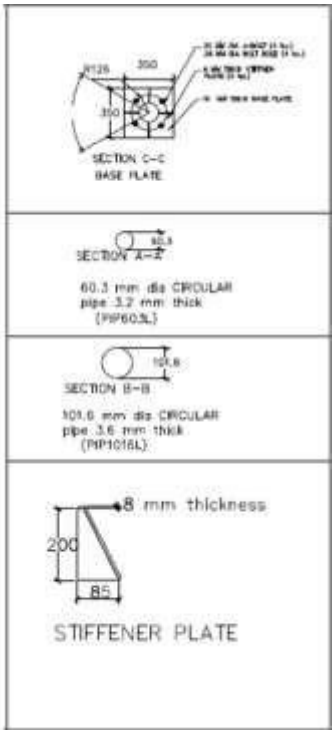


i	300 mm x 300 mm x 150 mm sized junction box of 1.5 mm material thickness
ii	Hand-hole on the pole
iii	50 mm diameter holes for exit cables
iv	Cable gland with earthing tag
v	50 mm diameter holes for entry cables
vi	Cable gland with earthing tag
vii	Terminal blocks-2 x 10 terminals mounted on DIN rail or fixed at both ends to the junction box

HANDHOLE WITH JUNCTION BOX



ALL DIMENSIONS IN MM.



D. Outdoor Cabinets or Junction Boxes specification in detail

a) Each location shall be fitted with outdoor cabinets dimensioned to host all equipment necessary to operate surveillance systems in this project.

b) Additional room in the location controller cabinet to accommodate the future system requirements.

- The size of outdoor cabinet / Junction Boxes shall be sufficient to house all the system components, which may be installed at the location or nearby. Ingress Protection should be Outdoor – IP55 or better for Junction Box to be dustproof and impermeable to splash-water. It shall be suitable for Patna's environmental conditions and it shall have provision for two types of cabinet as follows:

- **Power cabinet:** This cabinet shall have the provision to house the electricity meter and the redundant power supply system
- **Control cabinet:** This cabinet shall house the controllers for all the field components at that particular location e.g. ANPR, PTZ, Fixed cameras etc

c) Internal cabinet cabling shall be designed for an easy connection and disconnection of the equipment and power

d) The cabinets shall be of robust construction and shall include 3-point spring loaded locking mechanism with Pad lock and protective cover (Allen key) to prevent unauthorized access to the field equipment

e) Temperature and Humidity Control: All enclosure compartments shall be equipped with a natural convection air circulation system via provision of air circulation filters that shall not require maintenance and shall allow free circulation of air inside the enclosures to prevent overheating as well as the build-up and effects of humidity and heat, without permitting the entry of elements that might endanger system operation

f) MSI will ensure to place all the hardware inside the junction boxes that could withstand temperatures prevalent in Patna throughout the year

g) MSI will ensure security of Junction Box from vandalism & theft by using complete welded structure with fixed rear and side panels.

E. Civil and Electrical Works

a) Aall the civil & Electrical work executed and setting up all the field components of the system including:

- Preparation of concrete foundation for MS-Poles & cantilevers
- Laying of GI Pipes (B Class) complete with GI fitting
- Hard soil deep digging and backfilling after cabling
- Soft soil deep digging and backfilling after cabling with added rocks/ coarsen
- Chambers with metal cover at every junction box, pole and at road crossings
- Concrete foundation from the Ground for outdoor racks, if required

b) MSI will carry out all the electrical work required for powering all the components of the system

c) Electrical installation and wiring shall be under standard guidelines to the electrical codes of India

d) MSI will make provisions for providing electricity to the cameras (ANPR, PTZ, and Fixed) via SJB (Surveillance Junction Box), housing the UPS/SMPS power supply, with minimum backup in coordination with Patna Smart City Officials and the Electrical Department. The power will be fetched from the nearby transformer as guided by the Electrical Department.

e) For the Fixed Box cameras, MSI will provision for drawing power through PoE+ (Power over Ethernet) and for the ANPR cameras MSI will provision for drawing power through POE, POE+, while PTZ cameras shall be powered through dedicated power cable laid separately along with STP/SFTP cable if additional power is required.

f) Registration of electrical connections at all field sites shall be done in the name of the Patna Police.

g) Electricity meters will reside inside the power cabinet as per Bihar Electricity guidelines guidelines.

F. Earthing and Lightning Proof Measures

a) Technical Specifications taking into account lightning- proof and anti-interference measures for system structure, equipment type selection, equipment earthing, power and signal cable laying.

b) Corresponding lightning arrester shall be erected for the entrance cables of power line, video line, data transmission cables

c) All interface board and function board, interfaces of equipment shall adopt high speed photoelectric isolation to reduce the damage to integrated circuit CMOS (Complementary metal–oxide–semiconductor chip due to the surge suppression)

d) Install the earthing devices for the equipment, including lightning earthing,

protection earthing and shielded earthing. All earthing shall meet the related industry standards

e) The earthing cable shall be installed in a secure manner to prevent theft and shall be rust proof. Earthing down lead and the earthing electrode shall be galvanized.

G. UPS for field devices

a) As an acute necessity of the power backup arrangement for uninterrupted operations of field devices such as switches, cameras Gun-shot detection sensors, etc. the provision of adequate capacity UPS is recommended.
b) The UPS should be capable to provide 60 min. of power backup in field which will be placed inside the Junction Box with the set of batteries.
c) A UPS of 500 KVA, 1 KVA load for every pole mounted and floor mounted Junction Box respectively is considered.

Capacity /Training for Officers/Employees

The MSI will ensure that the concerned officials learns to operate all the services and SOPs of Smart City Project to deliver the desired outputs.

Based on the needs and the objectives of the project, training programs would be organized by the MSI with qualifying criterion under the following themes:

a. Creating awareness about the benefits of Smart City Project and operation on application skills.
b. Role-based training for people at different levels of monitoring and control.
c. "Train the Trainer" programs, where members of the staff would be trained to enable them to conduct further training programs, thus helping build up scalability in the training program and also reducing the dependency on external vendors for training.
d. System Administrator training: a few members of the staff with high aptitude shall be trained to act as system administrators and trouble-shooters for smart city officials. The training will be for around 2000 Government employees assigned by Smart City officers.

Warranty Services included after Go-Live:

a. Comprehensive warranty towards entire implemented system including IT hardware, Non-IT hardware, software and services etc. The warranty shall commence from the date

of acceptance of respective system/post Go- Live of the entire project and shall be operational for a period of minimum 05 years'

b. Technical Support for Software applications shall be provided by the respective OEMs for the period of warranty. The Technical Support should include all upgrades, updates and patches to the respective Software applications.

c. Goods supplied under the Contract are new, non- refurbished, unused and recently manufactured at the time of delivery; the End of sale / End of support of any product should not prevail before 18 months of the commissioning; and shall be supported by the MSI and respective OEM along with service and spares support to ensure its efficient and effective operation for the entire duration of the contract.

d. Goods supplied under this Contract shall be of the highest grade and quality and consisted with the established and generally accepted standards for materials of this type. The goods shall be in full conformity with the specifications and shall operate properly and safely. All recent design improvements in goods, unless provided otherwise in the Contract, shall also be made available.

e. Guarantee/Warranty for all Stores, Equipment, Services supplied at least for a period of 60 months (05 years i.e. 03 Years warranty+02 Years extended warranty) from the date of commissioning of the Systems at the Sites/Locations and that the

said system would continue to conform to the description and quality for all equipment's/system. If any deviation or deterioration in description and quality, design, workmanship and performance as per the agreed specifications is noticed or discovered during the period of warranty.

f. Replacement the faulty equipment, systems or portions thereof will be within a period of 48 hours. In such event the remaining warranty period shall apply to the equipment, systems or portions thereof so replaced from the date of replacement.

g. Service will be for 24x7 support with 4 hours response time and 48 hours of resolution time from the date and time of reporting of an error, during the warranty and extended warranty period.

Operation & Maintenance service which will run in parallel with Warranty Services:

The MSI shall provide complete Operations and Maintenance support for the integrated solution deployed from the date of Go-Live and shall be operational for a period of minimum 05 years' post Go-Live of the entire project.

During the Warranty and O&M period, the MSI shall provide all product(s) and documentation updates, patches/fixes, and version upgrades within 15 days of their availability/release and should carry out installation and make operational the same at no additional cost to C-DAC.

In this phase, MSI would be responsible for operations and maintenance of the entire solution.

The following services should be provided by MSI:

a. O&M phase planning and monitoring
b. Ongoing Administration and Maintenance requirements
c. Operation of Monitoring Centre (including Help Desk)
d. VAPT Execution
e. Facility Management Services at Command & Control Centre
f. MIS Reports and Incident Reporting
g. Assistance in Integration with other integrations as and when required by adding more use-cases
h. Continuous Learning to the system on new alerts and VA systems
i. SLA reporting
j. The MSI is required to ensure that all the required hardware and software proposed should be capable and meet the required performance as per the RFP.
k. MSI should ensure while execution and operation &maintenance phase, the industry best practices has to be followed. MSI should adhered to industry standard checkpoints while execution and after starting the operation phase while replacement/ re-installing / re-commissioning

The Cost of Operation & Maintenance shall be deemed to cover all costs for performing the maintenance services including the cost of providing all labour, tools, equipment, facilities, spare parts, replacement of faulty parts, consumables (excluding diesel/oil and batteries) and other related materials, documentation, staff training, test equipment and all other necessary items.

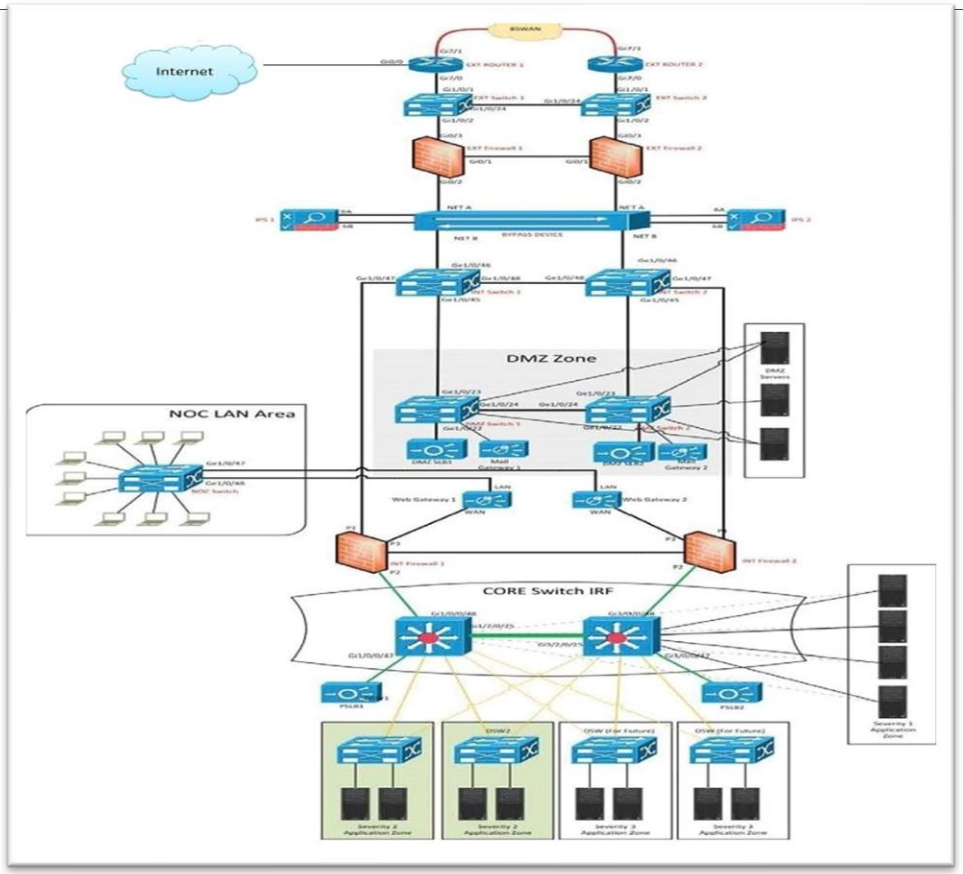
Sufficient technical maintenance staff will be deployed to carry out the m aintenance works.

Operation Power charges

Operational power charges for the field electrical meter will be paid by the system integrator after readiness & final acceptance of the site. MSI will be responsible of arranging the power for installation, implementation & testing of the site till final acceptance by Patna Smart City. Field Electrical Meters will be issued in the name of Patna Smart City. One time electrical meter connection installation & implementation, cabling charges and the operation & maintenance Incident management, complaint logging for any fault in meter or field electrical connections will be responsibility of MSI during the entire contract period. The power connections (electrical meters) charges will be paid by MSI and the recurring power charges will be borne by the MSI ; However MSI will submit the overall bill for the reimbursement; It will be effective from Go-Live phase. Appointed MSI will coordinate the execution of connections with Electrical Department. The DG gen set, UPS will be installed at Patna Smart City Office at approved site and the operational expenses of fuel consumed by DG gen set till the time of acceptance will be borne by MSI.

Implementation and Performance Audit

The project implementation upon completion will undergo a complete implementation audit in terms of contractual role and responsibilities of the MSI . The third party audit (TPA) will be conducted by CERT-In empanelled agency on behalf of Patna Smart City. The report will be submitted to Patna Smart City after completion of the process.


Internet
DMZ Zone
NOC LAN Area
CORE Switch IRF